Plan de Contingencias y Recuperación de Desastres.

Acciones generales en caso de desastre.

Rescatar las operaciones en el lugar del desastre.- Esfuerzos inmediatos a la ocurrencia del desastre para proteger y preservar el equipo de computo, en particular cualquier medio magnético y óptico de almacenamiento de datos deberá ser identificado y protegido o movido a un lugar limpio y seco lejos del lugar del desastre.

Determinar el sitio de recuperación.- Al mismo tiempo, una exploración de la escena del desastre se realiza por personal calificado para estimar el tiempo requerido para reestablecer el orden de trabajo de los sistemas afectados. Se efectúa la decisión de utilizar un sitio alterno, que deberá ser un sitio lejano a la escena del desastre donde pueden reestablecerse temporalmente las capacidades computacionales y de redes hasta que el sitio primario este listo. El trabajo comienza inmediatamente en lo que respecta a la reparación o recontracción del sitio primario, que puede tardar algunos días o meses.

Compra de equipo nuevo.- El proceso de recuperación se apoya fuertemente en los proveedores y su respuesta a la adquisición de repuestos para los recursos que no pudieron ser rescatados del desastre. El CIMAV se apoyara en los procedimientos gubernamentales de emergencia que apliquen para la adquisición para rápidamente aprobar ordenes de compra para las necesidades.

Iniciar el reensamblaje en el sitio de recuperación.- Los componentes rescatados y nuevos son reensamblados en el sitio de recuperación de acuerdo a instrucciones contenidas en este plan, debido a que todos los planes de este tipo inherentemente están expuesto a cambios constantes de la industria de la computación, puede ser necesario desviarse del plan, especialmente si el plan no ha sido actualizado con frecuencia. Si los proveedores no pueden proveer un cierto componente en los tiempos requeridos, puede ser necesario efectuar sustituciones de ultimo minuto. Después de que la fase de reensamblaje se ha completado, el trabajo se turna a los procedimientos de recuperación de datos.

Restauración de datos a partir de respaldos.- La recuperación de datos recae enteramente en el uso de respaldos guardados en ubicaciones fuera de sitio, los respaldos se pueden tomar de medios magnéticos, ópticos u otro medio de almacenamiento. Los esfuerzos primarios es el reestablecimiento de los sistemas operativos de cada sistema de computo, seguido de la recuperación de las aplicaciones y datos de usuario a partir de los respaldos, los usuarios que poseen aplicaciones espaciales deberán de involucrarse en la recuperación de sus aplicaciones con el fin de que esta se satisfaga.

Restauración de datos de aplicación.- En este punto los planes de recuperación de desastres para usuarios y departamentos deben unirse a la recuperación completa de los servicios, debido al periodo de tiempo en que se llevo a cabo el respaldo fuera de sitio con respecto a la fecha del desastre, los usuarios deberán de tener medios para recuperar los datos de bases de datos hasta el punto del desastre, y deberán ser capaces de introducir los datos generados en el sitio alterno para actualizar al día los datos de las bases de datos.

Reubicarse en el sitio principal y permanente.- Al termino del proceso de restauración de los servicios en el sitio principal, se desmantela el equipo instalado en el sitio alterno y se llevan al sitio permanente.

Riesgos de desastre y prevención.

El tomar medidas para la prevención de desastres mitiga los efectos de antemano lo cual es de suma importancia, por lo que se listan amenazas naturales y cerradas por el hombre:

- Fuego.
- Inundación.
- Tolvaneras y vientos fuertes.
- Crimen cibernético.
- Acciones terroristas y sabotaje.

Fuego.

La amenaza de fuego en el sitio principal de telecomunicaciones y sistemas del CIMAV es real y posee el mayor índice de riesgo de todos los desastres contemplados, el edificio esta lleno de dispositivos eléctricos y conexiones que pueden sobrecalentarse o hacer corto y causar un incendio.

Medidas preventivas.

Alarma de incendio.- CIMAV posee sistema de alarma contra incendio, con actuadores manuales, sirenas y señalamiento visual instalado en puntos estratégicos.

Extinguidores.- Se encuentran ubicados en lugares visibles y estratégicos.

Construcción del edificio.- Los edificios de CIMAV están construidos primariamente de materiales no inherentemente inflamables, el riesgo de incendio se reduce dada la presencia de productos resistentes a la flama.

Entrenamiento y documentación.- Instrucciones detalladas de el manejo de incendios con proporcionadas por la comisión de seguridad e higiene así como la operación de los extinguidores y procedimientos de simulacro de incendio.

Recomendación.

Revisión regular de los procedimientos deberá efectuarse para asegurar que se encuentren al día. Simulacros no programados deberán efectuarse por un administrador imparcial y una evaluación por escrito deberá efectuarse y entregarse a los jefes de departamento.

Inspecciones regulares de los equipos de prevención de incendio deberán realizarse a intervalos programados, los extinguidores deberán ser inspeccionados periódicamente como política estandarizada.

Inundación.

El edificio de investigación dentro del cual se albergan la mayor parte de los recursos y servicios de la unidad de telecomunicaciones y sistemas del CIMAV, esta ubicado en un área cuyo nivel es mas bajo que el de los edificios circundantes, ese factor acoplado a la posibilidad de que una tormenta deposite grandes cantidades de lluvia en el área norte de la ciudad de Chihuahua presentan la amenaza de inundación. Las aguas de inundación que penetraran en el MDF pueden causar un daño severo, no solo pueden existir fallos de energía debido al agua, las aguas de inundación pueden acarrear lodos y materiales que pueden dañar las conexiones y equipos electrónicos, aparte de presentar una amenaza para la seguridad del personal debido a la presencia de energía eléctrica en las instalaciones.

Medidas preventivas.

Se llevó a cabo la construcción y modificaciones de los drenajes principales en CIMAV después de la ocurrencia de un evento de inundación ocurrido tiempo atrás, con lo cual se reduce dramáticamente el riesgo de inundación severa.

Recomendaciones.

Inspección periódica a los sistemas de drenaje verificando que estén libres de obstrucciones, verificar fugas de agua especialmente el drenaje de aguas de lluvia proveniente del techo del edificio que pasa por el cuarto de telecomunicaciones especialmente en los eventos de lluvia, se pueden colocar sensores de agua en lugares estratégicos para detectar niveles de inundación en el cuarto de telecomunicaciones. Efectuar entrenamiento y simulacro de procedimientos de apagado regularmente así como entrenamiento al personal para respuesta ante victimas de electrocución.

Tolvaneras y vientos fuertes.

Debido a la zona geográfica en que esta ubicado el CIMAV no existen grandes posibilidades de vientos de intensidad suficiente como para provocar desastres mayores, sin embargo se deben tomar medidas en al eventualidad de que una ráfaga de viento produzca un daño mayor a las instalaciones.

Medidas preventivas.

Dada la construcción de las edificaciones de CIMAV, existen riesgos asociados a la eventualidad de vientos de magnitud considerable que pudieran fracturar o desprender los vidrios de los domos, ventanas y puertas, lo que provocaría la entrada de grandes cantidades de polvo o lluvia, en lo respectivo al cuarto de comunicaciones estos elementos pueden producir daños a los equipos.

Recomendaciones.

El personal de CIMAV debe de conocer los riesgos de quebradura o desprendimiento de ventanales en el evento de presencia de vientos fuertes y los lugares adecuados para protegerse en caso de desastre. El personal de telecomunicaciones y sistemas deberá contar con lonas y cubiertas grandes en el cuarto de telecomunicaciones listos para cubrir el equipo electrónico en caso de existir daños en las ventanas, el personal deberá estar capacitado para cubrir correctamente el equipo.

Crimen cibernético.

El crimen cibernético se la vuelto mas común y mas peligroso a medida que los sistemas se vuelven mas complejos y el acceso se encuentra mas ampliamente distribuido, con las nuevas tecnologías de red, se presentan fugas de acceso potenciales.

El crimen cibernético usualmente no afecta los dispositivos de hardware en una forma destructiva. Tal vez sea mas insidioso, y puede seguido venir del interior. Un empleado o estudiante disgustado puede infiltrar virus o bombas de tiempo en aplicaciones y código de sistemas. Un empleado bien intencionado también puede cometer errores de codificación que afecten al integridad de datos (esto no se considera crimen a menos que el empleado deliberadamente sabotee programas y datos).

Medidas preventivas.

Todos los sistemas y equipos deberán contar con productos de seguridad que protejan contra accesos no autorizados. Todos los sistemas deberán estar protegidos por contraseñas, especialmente

aquellos que permiten actualizaciones a los datos. Todos los usuarios se les deberá pedir cambiar su contraseña en periodos regulares. Todos los sistemas de seguridad deberán registrar los intentos inválidos de acceder a datos y los administradores de seguridad deberán revisar estos registros en periodos regulares.

Todos los sistemas deberán ser respaldados periódicamente. Estos respaldos deberán guardarse en un área separada a la de los datos originales. La seguridad física de el área de respaldos y almacenamiento de datos deberá implementarse. Deberán establecerse estándares en cuanto al numero de ciclos de respaldo que se retendrán y la duración de su retención.

Recomendaciones.

Mejora continua a las funciones de seguridad de cada plataforma. Políticas coercivas y procedimientos espaciales cado se detecten violaciones a la seguridad. Regularmente dar a conocer a los usuarios la importancia de mantener sus contraseñas en secreto. Hacerles conocer a los usuarios como establecer una contraseña segura difícil de adivinar.

Mejorar la seguridad de red. Algunos sistemas de red son susceptibles a ser intervenidos , en los que usuarios sin escrúpulos pueden buscar contraseñas, implementar mecanismos de seguridad mas robustos en la red, tales como contraseñas de un solo uso, encriptación de datos y medios de transmisión de datos mas seguros.

Acciones terroristas y sabotaje.

Los sistemas de telecomunicaciones son siempre blancos potenciales para acciones terroristas y de sabotaje tales como bombas y eliminación de información, así como la posibilidad de secuestro de personal clave.

Medidas preventivas.

Seguridad del sitio es de extrema importancia. De cualquier modo, la acciones terroristas pueden ocurrir independientemente de la seguridad del edificio y pueden ser muy destructivas. Una bomba puesta enseguida de la pared exterior del cuarto de telecomunicaciones puede causar severos daños al interior del cuarto.

Dada la libertad que se goza en el país, y las instalaciones de CIMAV, casi nadie aceptara una planeación de seguridad a gran escala, las restricciones y costos que serian necesarios para la protección de los edificios en si ante un atentado. De cualquier modo pueden aplicarse algunos principios de sentido común.

Los edificios deberán ser iluminados en cada cara durante las noches, las puertas del cuarto de telecomunicaciones deben ser fuertes y con buenos cerrojos. Las entradas al cuarto de telecomunicaciones deberán estar cerradas en todo momento. Solamente las personas autorizadas deberá de permitírseles la entrada al cuarto. las personas sospechosas deberán ser reportadas.

Recomendaciones.

Mantener buena seguridad en el edificio. Las puertas del cuarto de telecomunicaciones deberán mantenerse cerradas en todo momento, todos los visitantes al cuarto de telecomunicaciones deberán recibir autorización con anticipación así como registro de entrada y salida.

Preparación para desastres.

Para facilitar la recuperación a partir de un desastre que destruye todo o parte de el cuarto de telecomunicaciones en el CIMAV, ciertas preparaciones deberán de haberse hecho de antemano. A continuación se describe lo que debe de hacerse para establecer un camino rápido y ordenado para la restauración de los servicios que operan en el CIMAV, los cuales son:

- Planeación de recuperación de desastres.
- Ubicación temporal de recuperación.
- Equipo de reemplazo.
- Respaldos
- Cajas fuertes de desastres.

Planeación de recuperación de desastres.

La primer y mas obvia cosa por hacer es tener un plan. El plan en general del que este documento es parte es lo que utilizara el departamento de sistemas para responder a un desastre. Las condiciones bajo las que este plan puede ser efectivo, dependen de los planes de recuperación de desastres establecidos por otros departamentos de CIMAV.

Por ejemplo, en un desastre que afecte todos los edificios de CIMAV, los departamentos de administración y finanzas, contabilidad, adquisiciones, etc … se verían severamente afectados al no tener acceso a los procedimientos apropiados, documentos, listas de proveedores y procedimientos de aprobación, el proceso de recuperación iniciado por el departamento de sistemas puede ser retrasado mientras los procedimientos de compra se reestablecen.

Todos los demás departamento de CIMAV deberán de desarrollar planes de cómo efectuaran sus actividades en caso de desastre tanto en su lugar de trabajo, como por la suspensión de acceso a los servicios mantenidos por le departamento de sistemas por un largo periodo de tiempo debido a un desastre.

Estos departamentos necesitan manera de trabajar mientras las computadoras y redes están caídas, además necesitan un plan para sincronizar los datos que son restaurados en los servidores y computadoras centrales con el estado actual de los movimientos. Por ejemplo, el pago de nomina de trabajadores, controlado por el departamento de recursos humanos, puede efectuar el pago a trabajadores, sin embargo los datos de pagos realizados deberán de ser introducidos al sistema cuando se encuentre de nuevo en servicio, por lo tanto llevar un registro de todos los movimientos tales como pago de nomina, mientras las computadoras centrales están caídas es de extrema importancia.

Lugar de recuperación.

Si el lugar donde residen los servicios de telecomunicaciones y sistemas es destruido en un desastre, la reparación o reconstrucción de ese lugar puede tomar mucho tiempo y en el inter será necesario restaurar los servicios de computo y red en un lugar alternativo.

El CIMAV posee un listado de opciones de sitios alternativos, cada uno en dependencia de los costos.

Sitio de recuperación en caliente.

Es una opción muy cara para estar preparado para un desastre, consistente de un lugar de telecomunicaciones separado preparado con equipo de computo, ubicado en otra ciudad listo para entrar en funcionamiento en le momento en que se notifique que el sitio principal esta caído. Ambos lugares deben estar interconectados con líneas de alta velocidad de manera que los usuarios de CIMAV puedan seguir teniendo acceso a las computadoras y aplicaciones desde sus oficinas.

Compañía de recuperación de desastres.

Algunas compañías poseen las capacidades de bajo un costo determinado proveer un espacio y equipo para la recuperación de los servicios bajo una condición de desastre, el equipo de telecomunicaciones deberá de llevar físicamente los respaldos realizados a la ubicación.

Existe la posibilidad de que algunas instituciones ubicadas en la ciudad de Chihuahua, que poseen recursos computacionales suficientes puedan apoyar el proceso de recuperación mediante el préstamo de instalaciones y personal calificado para el apoyo al proceso de recuperación del desastre, algunas de ellas son la UACH, el Tecnológico de Chihuahua, Gobierno de Estado, `por nombrar algunas.

Sitio de recuperación en frío.

Este es un área separada físicamente del sitio principal, donde se ha identificado un espacio para usarse temporalmente para albergar el equipo de computo y sistemas de red mientras el sitio primario es reparado. Existen varios niveles de preparación de este tipo de sitio, que van desde un cuarto sin terminar, donde existen las instalaciones eléctricas, de soportería y de climatización en correcto funcionamiento para la instalación de los equipos.

Para una situación de desastre en CIMAV se ha definido como sitio de recuperación en frío un área del edificio administrativo, desde donde se pueden puentear la mayoría de los servicios de telecomunicaciones, aunque el control de las condiciones de climatización aun no se encuentran completamente soportadas.

Mas detalles en lo que respecta a las preparaciones que se han llevado a cabo, además de el trabajo que se requiere realizar para renovar el espacio y prepararlo para recibir el equipo de computo esta disponible en el capitulo *“Recuperación en el sitio de recuperación en frío”* .

Reemplazo de equipo.

Este plan contiene un inventario completo de los componentes de cada computadora y sistemas de red así como su software que debe de res restaurado después de un desastre. Los cambios inevitables que ocurren en los sistemas a través del tiempo requieren que el plan sea actualizado periódicamente a la configuración mas cercana a la actual. Toda vez que sea posible, se deberán de efectuar convenios con los proveedores para obtener reemplazos en una citación de emergencia. Para evitar problemas y retrasos en la recuperación, se deberá intentar en todo caso replicar la configuración actual de los sistemas. Sin embargo, existirán casos en donde los componentes no estén disponibles o su entrega considere tiempos excesivamente largos. El equipo de recuperación tendrá que tener la experiencia y recursos para resolver estos problemas tal y como se presenten en su momento. Algunos procedimientos de este plan deberán cambiarse, usando diferentes modelos de equipo de diferente proveedor o marca que sean equivalentes para el proceso de recuperación.

Respaldos.

El reemplazo de hardware, edificios y empleados es relativamente fácil de hacer, sin embargo al información almacenada en equipos viejos no se puede comprar con nada. Debe de ser restaurada a partir de una copia de respaldo que no fuese afectada por el desastre. Existen algunas opciones disponibles para ayudar a asegurar que las copias de respaldo de los datos sobrevivan a un desastre en el sitio principal de telecomunicaciones y sistemas.

Copia doble remota.

Esta opción aplica para un subsistema de discos ubicado en un sitio lejano del sitio principal de telecomunicaciones, los datos escritos a disco en el sitio principal se replican al disco remoto en el momento en que se lleva a cabo un cambio en la estructura del disco principal, esto asegura tener la información mas al segundo de las bases de datos del sitio principal en caso de que sea destruido. Se puede simplificar el proceso de recuperación colocando el subsistema de disco remoto en el sitio de recuperación remoto. Esta opción es algo cara, pero no prohibitiva. No requiere que todo un sistema de servidores sea construido en un sitio de recuperación en caliente, solamente requiere de un subsistema de discos, típicamente se limita únicamente a sistema de discos principales y no de todos los servidores.

En el CIMAV realiza copias programadas de la información importante acerca de la configuraron, cuentas de usuario e información de que dependen los servicios de cada servidor, en un servidor de archivos dentro del sitio principal de distribución junto con los servidores, eventualmente se lleva acabo una copia de la información mas importante en discos ópticos para ser guardados en una ubicación distinta.

Cajas de seguridad para desastres.

Con el fin de asegurar que una copia actual del plan de recuperación de desastres este disponible en el momento en que ocurra un desastre, se han establecido procedimientos para el almacenamiento de este plan junto con otra información importante para llevar a cabo la recuperación en frío de los servicios.

La copia del plan estará guardada en dos lugares simultáneamente, uno es en el departamento de sistemas, y el otro en el sitio de recuperación en frío dentro del edificio administrativo, dentro de una caja que se encuentre identificada.

El contenido de las caja será el siguiente:

1. Copia física del plan de recuperación de desastres completa.
2. Copia digital del archivo del plan de recuperación de desastres en CD.
3. Sobre sellado con las contraseñas administrativas de cada uno de los sistemas, cada vez que el sello del sobre se encuentre roto se deberán cambiar todas las contraseñas para evitar problemas de seguridad.
4. Copia de cada uno de los sistemas operativos de cada sistema para efectuar una reinstalación.
5. Copia de los programas de instalación para las aplicaciones de cada uno de los sistemas.
6. Copia de los archivos de configuración y usuarios de cada uno de los sistemas en CD.
7. Copia en CD de la documentación del Hardware de los sistemas de CIMAV.
8. Documentación de inventarios de equipos, identificación de red de datos e información general de soporte de cada proveedor conocido.

Iniciación de los procedimientos de emergencia.

Notas acerca de la seguridad.

En prácticamente todo tipo de desastre existen peligros abundantes, mientras que en si la sobrevivencia al desastre puede ser una experiencia horrorosa, mas allá de los heridos y muertos seguidos por el mismo debidos a la negligencia y falta de precaución y cuidado.

Todo el personal deberá de ejercer un máximo de cuidado con le fin de asegurar evitar el daño físico o muerte mientras se trabaje alrededor del área de desastre. Nadie deberá de llevar a cabo tareas peligrosas sin antes haber tomado las medidas de seguridad apropiadas.

En este apartado del documento se hace referencia a las medidas de seguridad que deberá tomar el personal encargado de las labores de recuperación, estas notas estarán señaladas con el símbolo ∆, cada vez que se encuentre este símbolo se deberá prestar especial atención al riesgo existente y como prevenir el riesgo de lesiones.

Materiales Peligrosos.

Algunos de los materiales peligrosos presentes en las áreas administrativas y del departamento de sistemas son:

Productos de limpieza: Productos químicos peligrosos presentes en varios lugares dentro del departamento y en los closets del personal de limpieza.

Acido de baterías: El acido contenido dentro de las baterías de plomo dentro de las unidades de respaldo de energía que puede causar heridas cáusticas, ceguera y desordenes pulmonares si es inhalado, si se esta en contacto con el acido de baterías, lave la zona donde se expuso al acido con agua abundante hasta que se le pueda prestar atención medica.

Aceites, lubricantes y gases inflamables: en los alrededores de los sitios de distribución de red y del área de sistemas existen depósitos con lubricantes y aceites e incluso casetas de gases inflamables, los cuales tienen una alta peligrosidad en caso de incendio o fuga.

∆ Siempre aproxímese con cautela a cualquier conjunto de materiales peligrosos. Notifique al personal de seguridad mas próximo en caso de un derrame o fuga peligrosa. A menos de que tenga el entrenamiento apropiado, no intente limpiar un derrame peligroso por si mismo. Permita al personal calificado hacerse cargo del derrame.

Evasión del estrés.

La recuperación de un desastre será un momento muy estresante para el personal involucrado. Cada líder debe de monitorear cuidadosamente las horas de trabajo de su equipo para evitar una sobrecarga y agotamiento que puede ocurrir bajo estas condiciones. Una buna aproximación es dividir sus equipos en turnos y rotarlos en forma regular. Esto permitirá mantener al equipo descansado y proveerá tiempo para la familia del personal.

El riesgo de desorden de estrés postraumático es real y puede afectar a los sobrevivientes y trabajadores que atienden la recuperación en un desastre. Todos los lideres de recuperación y coordinadores deberán estar alerta a los síntomas de sus empleados que indiquen esta condición y deberán buscar ayuda adecuada para su tratamiento. Los síntomas como tales se manifiestan usualmente como:

Intrusiones: Las experiencias individuales vuelven a ser vividas en forma de pesadillas o recuerdos donde los eventos traumáticos son nuevamente experimentados.

Evasiones: Los individuos tratan de reducir la exposición a personas o cosas que pueden llevarlos a síntomas intrusivos.

Hiperarousales: Los individuos exhiben signos fisiológicos de estado de alerta incrementado, tales como hipervigilancia o un incremento en la respuesta inmediata.

Lista de notificación de desastres.

La lista de notificación de desastres del departamento de sistemas esta listada de forma que deberá de notificárseles tan rápido como sea posible en caso de desastre:

Personal de seguridad.

Servicios de emergencia según sea el caso (bomberos, ambulancia, policía, servicios de rescate, contención de riesgos y derrames peligrosos)

Teléfonos: 040, 060

Guardias de seguridad interna

Teléfono: 1198

Comité de seguridad e higiene

Coordinador: Mario Medina

Teléfono: 1181

Lista de notificación primaria del departamento de sistemas.

Jonathan Hernández Montes

Teléfono: 4869

Ivan Templeton Olivares

Telefono: 1193

Carmen Becerra Bencomo

Teléfono: 1150

Claudia López Domínguez

Teléfono: 1150

Equipos de Recuperación de Desastres.

Para funcionar eficientemente y permitir que todas las tareas se lleven a cabo simultáneamente, el proceso de recuperación será llevado a cabo por equipos.

Los equipos son:

- Equipo de Supervisión de la recuperación.
- Equipo de Evaluación de daños.
- Equipo de Recuperación de inmuebles.
- Equipo de recuperación de redes.
- Equipo de recuperación de plataformas.
- Equipo de recuperación de Aplicaciones.
- Equipo de Operaciones de Computo.
- Equipo de Soporte Administrativo.

El equipo de supervisión de recuperación se encarga de mantener el orden en las tareas de recuperación, este equipo posee un jefe de la recuperación, el tiene la autoridad final en las decisiones que deben hacerse durante la recuperación. El jefe de recuperación es el responsable de citar a los demás miembros del equipo de supervisión de la recuperación. A su vez cada miembro del equipo de supervisión de la recuperación ciara a los miembros de cada equipo de recuperación.

Selección del personal del equipo de supervisión de la recuperación.

Dado que cada desastre posee sus singularidades propias y es prácticamente imposible describir a los miembros necesarios para todo caso de desastre, se deberá tomar en cuenta la experiencia técnica necesaria y habilidades, una especificación general de cada miembro seria:

Jefe de coordinación de recuperación: Deberá de ser una persona con experiencia en administración y operación que este acostumbrado a trabajar en condiciones de presión, deberá de poseer amplio conocimiento del software y hardware en uso en el departamento de sistemas . Deberá de ser un solucionador de problemas debido a que existirán muchos problemas que no habrán sido anticipados.

Deberá de ser capaz de delegar responsabilidad a otros. También deberá tener autoridad para extender fondos como parte de la recuperación del desastre. El jefe de la Unidad de Telecomunicaciones y Sistemas es la primer opción como jefe de recuperación.

Coordinador de infraestructura: Deberá de compartir algunas de las habilidades del jefe de coordinación de recuperación, pero deberá de estar familiarizado con el proceso de hacer que los trabajos de construcción estén completados en tiempo y forma, deberá de entender y preveer la configuración eléctrica, acondicionamiento climático y requerimientos de comunicaciones.

Coordinador técnico: Deberá estar muy capacitado en varias áreas. Debe de tener un fuerte historial en la puesta a punto e interfaz de varias plataformas en uso tantas como sea posible. Necesita ser capaz de comunicarse fácilmente con el proveedor e ingenieros en cuestiones relativas a las opciones de instalación, desempeño, solución de problemas y algunas otras cosas, debe ser capaz de agendar y coordinar personal.

Coordinador administrativo: Debe de ser una persona hábil en la operaciones administrativas de CIMAV. Debe de estar bien acostumbrado a las operaciones día a día. También debe ser una persona de tacto, que pueda tratar con empleados y familiares de empleados durante tiempos difíciles, esta persona también debe de estar familiarizada con la compra de inmuebles, procedimientos y contratos.

Coordinador de redes: Debe de tener habilidades en el are a de mantenimiento y diseño de redes . debe estar entrenado para diagnosticar y corregir problemas en la red, conectar y depurar nuevas adiciones a una red existente.

Coordinador de aplicaciones: La primera opción para esta persona debe de ser alguien de soporte de aplicaciones. Esta persona debe de haber estado en contacto con las aplicaciones importantes, tales como nomina, contabilidad, etc … En caso de no estar disponible ninguna persona con estas características, se deberá optar por alguien con conocimiento de Oracle y restauración de bases de datos Oracle, sistemas Linux, Servicios SAMBA y permisos, ejecución de aplicaciones remotas, Active Directory y su restauración. La persona deberá de estar preparada para restaurar los sistemas a partir de respaldos anteriores. Deberá de funcionar de interfaz entre los usuarios para verificar el correcto funcionamiento de las aplicaciones así como analizar y desarrollar soluciones a los problemas que surjan.

Coordinador de operaciones de computo: Debe de ser hábil en las operaciones día a día de los sistemas principales de software así como conocimiento y habilidades para recrear (o implementar desde cero) itinerarios de producción para sistemas de aplicaciones. Esta persona también deberá de ser responsable de poner a punto una función de ayuda limitada que provea de información de la disponibilidad de los servicios y sistemas así como la forma de acceso a los sistemas que están en una configuración temporal o cualquier nuevo procedimiento que los usuarios requieran para accesar a los servicios.

Las personas que pueden ocupar cada uno de los puestos dentro del equipo de recuperación, para las posiciones correspondientes a la unidad de telecomunicaciones y sistemas se listan posibles candidatos a continuación:

Jefe de coordinación de recuperación: Jonathan Hernandez Montes

Coordinador de redes: Ivan Levi Templeton Olivares

Coordinador de aplicaciones: Claudia Lopez Dominguez y Carmen Becerra Bencomo

Coordinador de operaciones de computo: Jonathan Hernandez Montes

e Ivan Levi Templeton Olivares

Responsabilidades de cada equipo de recuperación de desastres.

El Jefe de la coordinación de la recuperación es el líder del equipo de administración de la recuperación y tiene la autoridad final en lo que respecta a las decisiones durante el proceso de recuperación. Cada uno de los demás individuos serán lideres de su equipo especializado que atenderán una porción de las tareas de recuperación. En la medida que el proceso de recuperación se lleva a cabo, existirán áreas que se traslapen entre los equipos y una comunicación estrecha será necesaria. El equipo de administración de la recuperación deberá de tener juntas regulares agendadas para proveer de comunicación entre los coordinadores de los equipos.

Cada coordinador deberá de agendar una junta con los miembros de su equipo adelantándose a las actividades planeadas que se tendrán que llevar a cabo, una agenda de la primer junta puede incluir:

1. Revisión del estado de la operación de recuperación.
2. Enfatizar las responsabilidades de cada equipo.
3. Asegurarse que los miembros están concientes de cualquier cambio al plan de recuperación original.
4. Asignación de tareas especificas a miembros individuales de cada equipo.
5. Determinar hora y lugar para futuras juntas.

Equipo de evaluación de daños.

Este equipo será liderado por el coordinador técnico. El será responsable de seleccionar a otros miembros de otros equipos, algunos pueden ser miembros de operaciones, servicios de red, telefonía, servicios técnicos y soporte. Este equipo no será responsable de una evaluación detallada para propósitos de reclamo de seguros, El enfoque primario de este equipo es dos tareas:

Proveer de información al equipo de coordinación de recuperación para que este sea capaz de tomar la decisión de recuperar el centro de distribución principal de telecomunicaciones y sistemas.

Proveer asesoramiento acerca del rescate de los componentes principales de hardware.

Basado en este asesoramiento el equipo de coordinación de recuperación puede iniciar el proceso de adquisición de equipo de reemplazo para la recuperación.

Equipo de recuperación de infraestructura.

Deberá de ser liderado por el coordinador de infraestructura. El será el responsable de seleccionar a los demás miembros de este equipo. Algunas opciones deberán ser miembros de operaciones, servicios de red, obra pública, representante del sitio de recuperación en frío y servicios de soporte.

Este equipo será responsable de los detalles de preparar el sitio de recuperación para dar cabida al hardware y personal necesario para la recuperación. La disposición e instrucciones para el sitio de recuperación en frío están incluidos en le plan de recuperación.

Este equipo también será responsable de supervisar las actividades de reparación o reconstrucción del sitio de distribución primario. Esta anticipado que la mayor responsabilidad en esto estará en el personal de mantenimiento y obra publica. Sin embargo, este equipo deberá de verificar la operaciones para asegurar que el sitio se repare para soportar adecuadamente la operación de los servidores y equipos de red y telefonía del sitio original.

Equipo de recuperación de redes.

Deberá de estar liderado por el coordinador de redes. El será responsable de la selección de los demás miembros del equipo, algunas opciones serían miembros de servicios de redes, soporte a usuario, obra pública y mantenimiento.

Este equipo será responsable de supervisar la restauración de la red de CIMAV y todas las conexiones de red necesarias para recuperar el sitio principal. Es completamente posible bajo ciertas condiciones de desastre que el equipo de recuperación de redes pueda ser el único involucrado como resultado de un desastre, por ejemplo debido a un incendio en un área que queme el cableado, este equipo deberá de encargarse de la recuperación inmediata.

Debido al gran grado de dependencia de las operaciones de CIMAV en cuanto a la red se refiere, se deberá de poner gran énfasis en la restauración de la red tan rápido como sea posible.

Equipo de recuperación de plataformas.

Deberá de Liderarse por el coordinador técnico, El será el responsable de seleccionar a los demás miembros de su equipo, Cada uno de los cuales será lider en cargo de la restauración de uno o más de las plataformas descritas en este plan.

Cada miembro del equipo puede reclutar a otros para asistir en forma técnica y detallada el trabajo de recuperación,. Ellos serán los responsables de comunicar las necesidades y estado a otros equipos de recuperación y coordinar las operaciones de restauración entre personal trabajando en diferentes plataformas.

Cada equipo de recuperación de plataforma deberá de seguir este plan general de acciones:

1. Revisar el daño causado.
2. Determinar que hardware, software y refacciones se necesitarán para iniciar la restauración de un sistema en particular.
3. Comunicar la lista de componentes que deberán comprarse y sus especificaciones al equipo de soporte administrativo.
4. Repasar los pasos de recuperación documentados en este plan para llevar a cabo cambios necesarios para ajustarse a las situaciones presentes en el momento.
5. Cuando el hardware comience a llegar, trabajar con el proveedor para instalar el equipo.
6. Cuando todos los componentes estén ensamblados, iniciar los pasos para restaurar los sistemas operativos y demás datos a partir de los respaldos existentes.
7. Intentar recrear el estado de todos los sistemas hasta momentos antes de que ocurriera el desastre de ser posible. Si no, el equipo es delegado al equipo de restauración de aplicaciones.

Equipo de recuperación de aplicaciones.

Deberá de ser liderado por el coordinador de aplicaciones, El será responsable de seleccionar a los demás miembros del equipo. Este equipo será responsable de llevar a cabo las actividades que siguen a la aprobación y aceptación de los sistemas de aplicación a su uso en ambiente de producción. En general las actividades de este equipo iniciaran después de que el equipo de recuperación de plataformas se haya completado. Algunos de los miembros serán de hecho miembros también del equipo de recuperación de plataformas.

Algunas tareas anticipadas pueden incluir:

1. Análisis de la necesidad de actividades de recuperación adicionales tales como recuperación de las bases de datos o de archivos individuales.
2. Desarrollar programas y procedimientos para atacar problemas específicos.
3. Hacer interfaces con aplicaciones de usuario para probar las aplicaciones.

Equipo de operaciones de computo.

Debe de ser liderado por el coordinador de operaciones de computo, el deberá de elegir a los demás miembros de su equipo, sus funciones principales serán:

1. Personificar el área de soporte para proveer asistencia telefónica e información de estado a los usuarios finales.
2. Proveer de apoyo al sitio de recuperación en frío.
3. Proveer funciones de control y producción para establecer agendas de trabajo de producción después de que los sistemas y aplicaciones son restaurados.

Equipo de soporte administrativo.

Deberá ser liderado por el coordinador administrativo, que será responsable de seleccionar a otros miembros del equipo, este equipo proveerá soporte a otros equipos de recuperación así como soporte a empleados y sus familias. Una de las mas importantes funciones que este equipo es proveer es hacerse

cargo de los detalles administrativos de tal forma que los ingenieros y técnicos que son responsables de la recuperación de los sistemas puedan concentrarse en su trabajo de recuperación.

Un miembro de este equipo debe ser designado como contacto familiar, esta persona estará disponible a lo largo del proceso de recuperación para proveer asistencia a los miembros de las familias de los empleados.

Un miembro de este equipo debe designarse como representante del departamento de adquisiciones de CIMAV. Esta persona será el enlace con la dirección de administración y finanzas para propósitos de autorizar las compras de emergencia y asegurar que la normativa del CIMAV y federal de reglamentos de compras bajo casos de emergencia se cumpla. El departamento de compras deberá tener su propio plan de contingencia a desastres que implementaran para ayudar a las necesidades de los departamentos en la restauración o reconstrucción de los edificios en el evento de un desastre.

Algunas tareas que se pueden adelantar pueden incluir:

1. Proveer de soporte al papeleo de ejecución de adquisiciones.
2. Asistir con información detallada de daños y procedimientos de reclamo de seguros.
3. Determinar el estado del personal que trabajaba en el momento del desastre.
4. Proveer servicios de conciliación para los empleados o sus familias que tengan problemas emocionales como resultado del desastre.
5. Coordinar arreglos para surtir de comida y alojamiento en caso de ser necesario a los empleados.
6. Proveer soporte para seguimiento de calendarios y costos relacionados al desastre.
7. Proveer servicios de transporte de equipo y materiales al sitio en frío como sea necesario.
8. Proveer soporte de relaciones publicas.
9. Asistir en el proceso de contrato de mano de obra externa que se requieran para completar el proceso de recuperación.

Activación del plan de recuperación de desastres.

Cita del coordinador de recuperación.

La primer orden del día es citar al coordinador de recuperación. La persona más apropiada para llenar este puesto es el jefe actual del departamento de sistemas. Si el director no esta disponible, la cita se deberá hacer al subdirector de administración y finanzas. La persona deberá de tener experiencia en la operación de datos de importancia en los sistemas y deberá de tener autoridad para llevar a cabo acciones expeditas durante el proceso de recuperación. El personal se describe en el tema “equipos de recuperación de desastres”.

Determinación del estado del personal.

Una de las primeras labores del coordinador de recuperación es determinar el estado del personal que se encontraba laborando en el momento del desastre. El personal de seguridad en el sitio después del desastre tendrá efecto en los rescates y primeros auxilios necesarios para las personas rescatadas del desastre. Sin embargo el coordinador de recuperación deberá realizar una lista de las personas saludables capaces de ayudar en el proceso de recuperación.

El coordinador de recuperación deberá ser rápido en citar al coordinador de soporte administrativo, de quien será la responsabilidad de identificar a cualquier herido o muerto en el desastre. El coordinador de soporte administrativo trabajara con las familias y empleados, atendiendo sus necesidades y obteniendo servicios de apoyo como sea necesario.

Rescate de Equipo y Protección de respaldos.

Un objetivo primario del proceso de recuperación es restaurar todas las operaciones de computo sin perdidas de cualquier dato. Es importante que el coordinador de recuperación cite al coordinador técnico rápidamente de tal forma que este pueda inmediatamente establecer las tareas para proteger y rescatar cualquier medio de almacenamiento donde se puedan guardar datos. Estos incluyen discos duros, discos flexibles, ZIP, CD-ROMS y unidades de lectura de discos. En la sección “Protección de equipo y rescate” contiene información valiosa acerca del rescate de medios magnéticos dañados.

Establecimiento del centro de control de recuperación.

El centro de control de recuperación es la ubicación desde donde el proceso de recuperación es coordinado. El coordinador de la recuperación debe designar donde se ubicara el centro de control de la recuperación. Si la ubicación no esta disponible el en edificio administrativo se tendrá que establecer otro lugar en otro edificio posiblemente un área en el edificio de postgrado o un edificio de oficinas externo al CIMAV.

Activación del plan de recuperación de desastres.

El coordinador de recuperación pone en marcha el plan, los primeros pasos son los siguientes:

1. El coordinador de la recuperación debe extraer la caja de seguridad de recuperación ubicada en el edificio administrativo y abrirla para obtener una copia actualizada del plan de recuperación de desastres. Este plan esta impreso dentro de la caja así como en forma de archivo digital en disco. Copias del plan deberán de obtenerse y repartirse a los miembros del equipo de recuperación en la primer junta. El coordinador de la recuperación es el responsable de los otros contenidos de la caja de seguridad, que deberá de ser posible ser resellada.
2. El coordinador de la recuperación deberá de citar a los miembros del equipo de recuperación. Esto deberá hacerse consultando a los miembros sobrevivientes del equipo de la unidad de telecomunicaciones y sistemas, mantenimiento y obra publica, y con aprobación del are administrativa de CIMAV, La decisión de quienes conforman el equipo de recuperación final es decisión del coordinador de la recuperación.
3. El coordinador de la recuperación deberá llamar a una junta del equipo de recuperación en el centro de control de recuperación o un sitio alterno designado. Se sugiere la siguiente agenda para esta junta:
    a. Cada miembro del equipo revisa el estado de sus áreas de responsabilidad.
    b. Después de la revisión, el coordinador de la recuperación hace la decisión final acerca de donde hacer la recuperación, si el sitio en frío será utilizado, el coordinador de la recuperación deberá declarar el uso del sitio de emergencia.
    c. Se hace una breve revisión del plan de recuperación de desastres junto con el equipo.
    d. Cualquier ajuste al plan de recuperación de desastres para acomodarse a circunstancias especiales deberán ser discutidos y tomarse decisiones acerca de ello.
    e. Cada mimbro del equipo esta bajo cargo de llevar a cabo a termino su rol de trabajo de recuperación respectivo e iniciar el trabajo según este agendado en el plan.
    f. Cada miembro del equipo deberá revisar la integración de sus propios equipos de recuperación, si existe un individuo clave que no este disponible para uno de los equipos de recuperación, el coordinador de la recuperación deberá brindar asistencia en la búsqueda de otros que tengan las habilidades y experiencia necesaria, incluyendo buscar ayuda de otras instituciones y centros de computo o proveedores.
    g. Se agenda la siguiente junta del equipo de recuperación, se sugiere que el equipo se junte por lo menos una vez cada día durante la primer semana del proceso de recuperación.

4. Los miembros del equipo de coordinación de recuperación deberán iniciar inmediatamente el proceso de contactar las personas que formaran sus respectivos equipos de recuperación y llamarlos a reuniones para poner en marcha su parte de la recuperación.
5. Se debe de despejar el área donde se ubicara el centro de control de la recuperación para que sea ocupara por el equipo de coordinación de la recuperación. Esto incluye la reubicación inmediata de cualquier personal que ocupe el cuarto, el coordinador administrativo deberá de ocuparse en conseguir los equipos básicos necesarios para el cuarto de recuperación, entre los que se incluyen:
    a. Mesas y sillas de oficina.
    b. Teléfonos.
    c. Computadoras personales compatible IBM (Pentium 4 o superior, 512MB RAM o mas, 80 GB disco duro o mas, tarjeta aceleradora de video, Monitores LCD 17´ o mayor, tarjetas Ethernet, quemador de DVD, disquetera 3 ½, teclado y Mouse)
    d. Impresora blanco y negro láser
6. La comunicación móvil será de importancia durante el proceso de recuperación, esta necesidad puede ser satisfecha mediante el uso de telefonía celular o radios.

Protección de equipos y rescate.

El procedimiento que se debe de usar inmediatamente después de un incidente para preservar y proteger los recursos en le área dañada se especifican a continuación.

Protección.

Es de extrema importancia que cualquier equipo, discos magnéticos u ópticos, papales importantes y otros elementos en el sitio dañado deben ser protegidos de ambiente hostil para prever daños mayores. Algunos de estos elementos podrán ser rescatados o reparables y ahorraran tiempo en las operaciones de restauración.

Recoger todos los discos duros y discos ópticos sueltos y llevarlos a un lugar seguro.

Recoger todos los equipos de computo y llevarlos a un lugar seguro.

Recoger todos los papeles importantes y cajas de papel nuevo y llevarlo a un lugar seguro.

Avisar a los guardias para evitar cualquier ingreso de personas a la zona de desastre.

Rescate de discos ópticos y magnéticos.

Los discos ópticos y magnéticos donde se encuentran guardados los datos son invaluables. A pesar de que se tiene un respaldo de los subsistemas de discos y aplicaciones primarias en un sitio alterno, existen discos duros que contienen información extremadamente valiosa que seria duro perder.

Después de proteger los discos de daños posteriores, la recuperación deberá de iniciar casi inmediatamente para evitar mas perdida. Un conjunto de compañías de recuperación a gran escala están identificadas en la sección “Servicios de recuperación de discos”

Si se requiere una atención mas inmediata que la que puede proveer un contratista, la sección “recuperación de discos ópticos y magnéticos dañados” describe el proceso de recuperación que puede seguirse en el sitio. También se puede encontrar información de cómo recuperar información contenida en disquetes en la sección ”recuperación de disquetes”.

Los siguientes son enlaces a sitios que proveen información adicional acerca de técnicas de rescate de discos magnéticos y de diversos tipos:

http://earth.library.pitt.edu/~webheads/ULS/policies/preserv/

http://www.nml.org/presentations/disaster_recovery/lc_disaster_recovery_slides_2.html/

Rescate de equipo.

Tan rápido como sea practico, todo equipo rescatable y consumibles se deberán mover a una ubicación segura. Si no se encuentra dañado, la transportación deberá de tramitarse a través del coordinador de la recuperación para mover el equipo al sitio de recuperación en frío, o a otra área protegida (como el almacén) mientras el sitio de recuperación en frío este listo.

Si el equipo ha sido dañado, pero puede ser reparado o reconstruido, el sitio de recuperación en frío puede no ser el mejor lugar para el equipo, especialmente si fue dañado por agua o fuego y necesita reparación. El taller de mantenimiento y prototipos puede proveer un lugar para secar repintar o enderezar el equipo.

Inventario.

Tan rápido como sea practico se deberá de efectuar un inventario completo de todo el equipo rescatable, junto con estimados del tiempo que tardara en estar listo para usarse de nuevo (en caso de reparación o reconstrucción). Este inventario debe de ser entregado al coordinador técnico y coordinador administrativo quien lo usara para determinar que hardware y consumibles recuperados del desastre deben de ser usados para levantar los sistemas recuperados.

Evaluación de daños.

La evaluación de daños es una evaluación preeliminar para establecer la extensión del daño al hardware critico y el lugar donde se encuentra. El objetivo principal es determinar donde se llevara a cabo la recuperación y que hardware debe de adquirirse inmediatamente.

Los miembros de equipo deberán estimar con tolerancia el tiempo requerido para reparar o reemplazar un recurso dañado. Tomando en consideración casos donde una reparación no puede empezar hasta que otros pasos sean completados. Los estimados del tiempo de reparación deben de incluir los tiempos de requisición, envío, surtido, instalación y prueba.

Considerando los elementos de hardware, considerar primero las listas de equipo que se proveen en las secciones de recuperación de cada plataforma. Estas listas serán construidas primariamente para la recuperación en el sitio en frío de tal forma que consistan de los componentes críticos necesarios para la recuperación. Se necesitara separar los elementos en dos grupos. Uno que estará formado por los equipos perdidos o destruidos y el segundo serán aquellos considerados rescatables que serán evaluados y reparados según sea necesario. Basado en reste estudio el equipo de coordinación de la recuperación puede iniciar el proceso de adquisición de refacciones.

Con respecto al edificio o cuarto, se deberá de llevar a cabo la evaluación al daño de la estructura, red eléctrica, sistemas de aire acondicionado e infraestructura de red. Si el estimado resultante de este proceso indica que la recuperación del sitio original requerirá mas de 14 días, la migración al sitio de reoperación en frío es recomendable.

Procedimientos de adquisiciones de emergencia.

El éxito o fracaso de la habilidad de este plan para asegurar la recuperación exitosa y en tiempo del equipo de computo y demás hardware asociado de red y telefonía estriba en la habilidad de adquirir bienes y servicios de forma inmediata.

Una política liberal para adquisiciones de emergencia en conjunto a un seguro de cobertura amplia, provee al coordinador de la recuperación de bases para tomar acciones de recuperación agresivas. Quizás solo se deban de citar precauciones, siempre existirá un día de reconocimiento seguido de cada evento extraordinario, cuando esas acciones se toman bajo condiciones de estrés del momento usualmente serán examinadas y evaluadas a la ligera a comparación de una situación normal, para reducir la ansiedad en la víspera de contabilización de los gastos, se recomienda seguir reglas preestablecidas a expensas de las circunstancias y mas importante, mantener registro de las transacciones y compras.

El coordinador administrativo de soporte es responsable de todas las adquisiciones de emergencia para la unidad de telecomunicaciones y sistemas, todos los coordinadores de equipos de recuperación deberán de efectuar sus peticiones al coordinador. El coordinador seguirá las reglas establecidas para adquisiciones en situaciones de emergencia y trabajara con el personal de compras electo por el departamento de compras para completar los procesos de adquisiciones. Si el departamento de compras ha sido afectado severamente por el desastre a grado de ser infuncional, el coordinador deberá de trabajar en conjunto a personal administrativo para apoyarse de los departamentos de compra del estado y otras instituciones con le fin de acelerar los procesos de adquisiciones.

El coordinador de soporte administrativo es también el responsable de dar seguimiento a todas las adquisiciones para asegurar que los registros financieros del proceso de recuperación del desastre se mantengan y que todos los procesos de adquisiciones pasen por una revisión de auditoria.

El coordinador de soporte administrativo debe estar conciente de la cobertura del seguro de CIMAV para saber que es y que no es permitido bajo las cláusulas de la póliza. En el caso de que la compra de un articulo no este permitida por la cobertura del seguro, o si los gastos exceden el monto limite de la cobertura del seguro, el coordinador debe consultar con el coordinador de la recuperación y otro personal responsables de CIMAV (dirección general).

Iniciación del proceso de recuperación.

Preparación del sitio en frío.

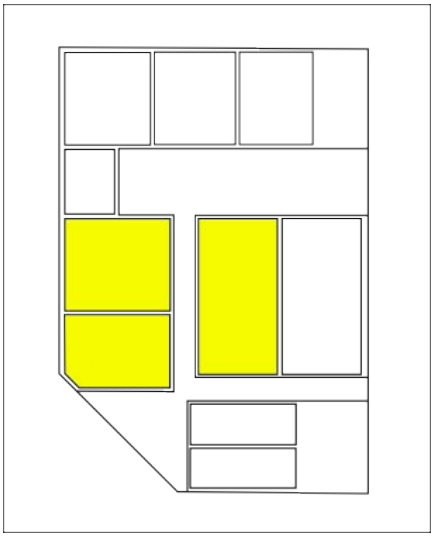
Esta sección se enfoca en la preparación del sitio de recuperación en frío designado para hacer de sitio primario de conexiones de red y computo después de ocurrido un desastre. Se ha elegido el cuarto de maquinas del edificio administrativo para albergar el equipo de red y servidores, el cual actualmente solamente alberga un sitio de distribución intermedia de red, y algunos documentos de archivo muerto así como viejas refacciones. Si el equipo de recuperación opta por usar este sitio después del desastre, habrá que llevar a cabo trabajos de adaptación para convertir este espacio de su actual uso a ser capaz de albergar los sistemas de computo, red y el personal de recuperación de desastre, el cual deberá de ubicarse en las oficinas contiguas, reubicando temporalmente al personal administrativo que las ocupa.

En caso de un desastre extremo donde el edificio administrativo también se haya vuelto inutilizable, deberá elegirse un sitio alterno. Dichos sitios requieren trabajo adicional para prepararse ara los requisitos especiales eléctricos y de enfriamiento del los equipos de computo. Otro sitio sugerido para la recuperación es la planta baja del edificio de posgrado, específicamente el área de biblioteca. Antes de considerar

efectuar la instalación de un sitio fuera de CIMAV, hay que asegurarse de considerar las necesidades de telecomunicaciones y redes hacia los edificios de CIMAV, incluyendo troncales.

Espacios del sitio de recuperación en frío.

El sitio de recuperación en frío esta ubicado en al esquina sur-oeste, en la primer planta del edificio de administración, el atea disponible para el uso de centro de recuperación de desastres es la descrita en la figura.



Las áreas consisten de dos oficinas y el cuarto de maquinas, en donde se concentran las conexiones de red y telefonía del edificio administrativo y a su vez se conecta la troncal telefónica y de red al sitio principal, Todas esta áreas deberán de ser desalojadas de personal y equipos innecesarios para el proceso de recuperación.

Revisión rápida a los trabajos de preparación del sitio.

El sitio en frío solo tiene preparaciones mínimas, existe muco trabajo por hacer en las primeras etapas del proceso de recuperación para que el sitio este listo. Aquí esta una rápida revisión de las instalaciones que deben realizarse:

- El equipo de computo, archivos y demás mobiliario de oficina propio para el desempeño de las labores del departamento de vinculación deberá de ser reubicado así como el material almacenado en el cuarto de maquinas, para hacer espacio para el personal de sistemas y coordinación de recuperación.
- Las instalaciones eléctricas ya existen en el cuarto de maquinas, solamente se requiere instalar un tablero de distribución que provea 120 V monofásico y 230 V bifásico, el cual deberá de ser instalado por contratistas o personal de mantenimiento.
- El sitio de recuperación en frío no dispone de unidades de acondicionamiento de energía (UPS), en caso de ser posible rescatarlas se deberán de instalar en el sitio de recuperación en frío, en caso contrario se deberán de instalar reguladores de voltaje simples con el fin de evitar que las irregularidades de tensión dañen los equipos mientras se encuentran en este sitio temporal.
- En el sitio determinado como sitio de recuperación en frío solo existe ventilación natural, se deberán de llevar a cabo adecuaciones con el fin de mantener los equipos a una temperatura aceptable.

- Los troncales de red y teléfono del edificio que van al sitio principal de distribución están ubicados en el sitio de recuperación en frío, troncales adicionales se deberán de instalar para extender la cobertura hacia los demás edificios de CIMAV.