15
24

UNIVERSIDAD NACIONAL AUTONOMA DE MEXICO

FACULTAD DE CONTADURIA Y ADMINISTRACION

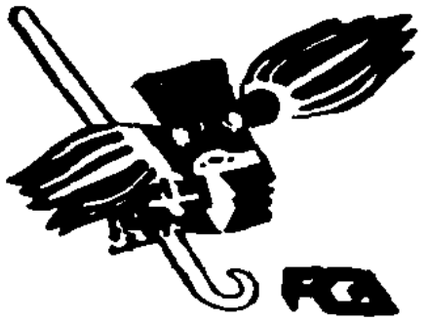
SEGURIDAD LOGICA, FISICA Y AMBIENTAL, PLAN DE CONTINGENCIAS

SEMINARIO DE INVESTIGACION INFORMATICA

QUE PARA OBTENER EL TITULO DE:
LICENCIADO EN INFORMATICA
P R E S E N T A N :

SOFIA MARIBEL PEÑA TRIGUEROS
CLAUDIA PARRAZALES ALONSO

ASESOR DEL SEMINARIO:
C.P. L.A. JOSE ANTONIO ECHENIQUE GARCIA



MEXICO, D.F. 1995

DEDICATORIAS

A MIS PADRES TOÑO Y LUPITA:

POR BRINDARME SIEMPRE LO MEJOR,
CARIÑO, COMPRENSIÓN, ALIENTO E
IMPULSARME A LA SUPERACIÓN,
DEDICO A USTEDES ESTA TESIS.

A MIS HERMANOS, LIZ, LUIS Y YENI:

POR LA PACIENCIA, AYUDA QUE ME BRINDARON
Y POR TODOS ESOS MOMENTOS FELICES
QUE HEMOS PASADO JUNTOS.

A MI ABUELITA CUALA Y A MI TIA OLGA:

CON INFINITO AGRADECIMIENTO POR SU
GENEROSIDAD, NOBLEZA, BONDAD Y
APOYO INCONDICIONAL EN LA
REALIZACIÓN DE MIS ESTUDIOS.

A MIS ESPOSO AGUSTIN:

PORQUE SIEMPRE ESTUVISTE CONMIGO,
POR TU APOYO, CARIÑO Y AMOR
QUE SIEMPRE ME HAS BRINDADO.

A MIS FAMILIARES Y AMIGOS:

POR SU APOYO, CARIÑO Y CONSEJO
A LO LARGO DE MI VIDA.

Sofía Maribel

DEDICATORIAS

A MIS PADRES:

POR SU APOYO INCONDICIONAL
EN TODO MOMENTO, ESPERANDO
QUE ÉSTO SEA UNA SATISFACCIÓN
PARA ELLOS.

A TODA MI FAMILIA Y AMIGOS:

POR MOTIVARME A CONSERVAR
LA ESPERANZA Y VOLUNTAD
PARA ESTE LOGRO.

A MI COMPAÑERA EN ESTE RETO:

PORQUE SIN SU PACIENCIA Y
AYUDA, NO HUBIERA SIDO
POSIBLE.

A JULIO CESAR:

POR SU GRAN COMPRENSIÓN
Y AYUDA CUANDO LO NECESITÉ.

Claudia

CONTENIDO DE LA INVESTIGACIÓN

1. INTRODUCCIÓN

La presente tesis da a conocer los principales conceptos a evaluar de Seguridad Física, Lógica y Ambiental en Informática de una organización. La falta de controles de Seguridad dentro de la organización, aumenta los riesgos que corre ante una contingencia.

La información que no es veraz y oportuna puede provocar grandes pérdidas monetarias para la empresa. Un centro de cómputo maneja gran cantidad de información importante para la organización. Si la información se perdiera y no se tuviera un sistema adecuado (Plan de Contingencias) pasaría un largo tiempo para que la empresa estuviera en operación normal, la información debe estar salvaguardada de robos, sabotajes o desastres naturales que pudieran ponerla en peligro.

En las últimas décadas se ha venido concentrando la información en medios electrónicos.

Hoy en día en las empresas es procesada la información por medio de sistemas automatizados, los cuales sirven para la toma de decisiones. Es necesario mantener la integridad de los datos durante el procesamiento de la información.

Debido a las experiencias en el fraude de las computadoras se han perfeccionado los sistemas de seguridad física y lógica, la desventaja es que se necesita consumir un número mayor de recursos de cómputo

En los últimos tiempos, se han convertido en recursos esenciales dentro de una organización, el hardware, software y el personal, en los cuales las organizaciones invierten millones de pesos, si alguno de estos recursos se perdiera la organización se vería afectada. Los planes de seguridad de una organización deberán tener como objetivo la protección de dichos recursos por medio de controles internos.

El software y el hardware de una organización puede ser destruido o robado, ocasionando que esta no pueda continuar con sus actividades. Su información puede ser conocida por la competencia, negociada ó utilizada para propósitos desautorizados.

Por lo anterior expuesto es necesario someter a las organizaciones a evaluaciones de seguridad lógica, física y ambiental.

Los Planes de Contingencia constan de dos etapas principales, una preventiva y otra correctiva. La preventiva evalúa los controles de seguridad, tan importantes para minimizar riesgos en una amenaza que sufra la organización, la fase correctiva opera una vez que la organización se ve afectada por un desastre y agiliza la recuperación y puesta en marcha de la organización.

2. OBJETIVO

LA PRESENTE INVESTIGACIÓN PRESENTARA UNA METODOLOGÍA PARA LA CREACIÓN DE UN PLAN DE CONTINGENCIAS, PROPORCIONARA CONTROLES PARA LA EVALUACIÓN DE LA SEGURIDAD LÓGICA, FISICA Y AMBIENTAL DE UN CENTRO DE COMPUTO.

OBJETIVO DEL PLAN DE CONTINGENCIA:

CONOCER LOS PROCESOS SISTEMATIZADOS CRÍTICOS PARA LA ORGANIZACIÓN, ASÍ COMO SUS RECURSOS, PARA SU RESGUARDO EN TIEMPOS ADVERSOS, PREVINIENDO LAS POSIBLES Y DIFERENTES SITUACIONES DE DESASTRE, PREPARANDO PROCEDIMIENTOS DE SEGURIDAD PARA LA REANUDACIÓN A LA BREVEDAD POSIBLE DE LAS OPERACIONES NORMALES DE LA ORGANIZACIÓN.

CAPITULO I

AUDITORIA

EN

INFORMATICA

3. AUDITORÍA EN INFORMÁTICA

3.1 CONCEPTOS DE AUDITORÍA EN INFORMÁTICA

Auditoría en informática según José Antonio Echenique[1] "Es la revisión y evaluación de los controles, sistemas, procedimientos de informática; de los equipos de cómputo, su utilización, eficiencia y seguridad, de la organización que participan en el procesamiento de información, a fin de que por medio del señalamiento de cursos alternativos se logre una utilización más eficiente y segura de la información que servirá para una adecuada toma de decisiones".

Para Ron Weber[2] la definición de auditoría informática es la siguiente: " La auditoría es el proceso de coleccionar y evaluar evidencias para determinar las medidas de seguridad de los sistemas automatizados para mantener la integridad de los datos, los archivos de la organización y objetivos eficientes".

La definición de Mair William[3] es la siguiente:
"Auditoría en informática es la verificación de los controles en las siguientes tres áreas de la organización (informática):
- Aplicaciones (programa de producción).
- Desarrollo de sistemas.
- Instalación del Centro de Proceso."

Partiendo de estos conceptos la Auditoría en Informática:

Se encarga tanto de evaluar como de revisar la eficiencia y eficacia de los sistemas en aplicación, la integridad de datos, los sistemas en desarrollo dentro de la organización, los equipos de cómputo, la instalación del centro de cómputo, y sus recursos humanos.

Los principales objetivos de la auditoría en informática son los siguientes:

1. Salvaguardar los activos. Se refiere a la protección del hardware, software y recursos humanos
2. Integridad de datos. Los datos deben mantener consistencia y no duplicarse.
3. Efectividad de Sistemas. Los sistemas deben cumplir con los objetivos de la organización
4. Eficiencia de Sistemas. Que se cumplan los objetivos con los menores recursos

3.2 NECESIDAD DE LA AUDITORÍA EN INFORMÁTICA

La auditoría es necesaria para coleccionar, evaluar evidencias y proporcionar recomendaciones dentro de la organización, que ponen en alto riesgo la continuidad de operaciones.

Las necesidades de auditar el procesamiento de información en la organización, son las siguientes:

a) Controlar el uso de la computadora que cada día, se vuelve más importante y costosa.

b) Los altos costos que producen los errores en una organización.

c) Abusos por computadora

d) Posibilidad de pérdida de información.

e) Toma de decisiones incorrectas

f) Valor del hardware, software y personal

g) Necesidad de mantener la privacía de la organización

La información es un recurso necesario para la organización y para la continuidad de operaciones, provee a la organización una imagen de su ambiente actual, su pasado y su futuro. Si la imagen de la organización es apropiada, está crecerá adaptándose a los cambios de su entorno.

Se debe detectar en el proceso de la información, sus errores u omisiones, y evitar su destrucción por causa de temblores, inundaciones o cualquier contingencia que pudiera suscitarse.

La toma de decisiones incorrectas, producto de datos erróneos proporcionados por los sistemas, traen como consecuencia efectos significativos, que afectan directamente a la organización.

3.3 DEPENDENCIAS MUNDIALES Y NACIONALES ENCARGADAS DE LA AUDITORÍA EN INFORMÁTICA.

El inicio de la auditoría en informática lo encontramos en Los Estados Unidos, con la fundación de la Asociación de Auditores de Procesamientos de Datos (The Electronic Data Processing Auditors Association (EDPAA)) en el año de 1969, teniendo como objetivo fomentar la educación, comunicación, el desarrollo profesional e investigación en los campos relacionados con la auditoría y sistemas de información.

En 1976 fue organizada la Fundación de Auditores de Procesamiento Electrónico de Datos (The Electronic Data Processing Auditors Foundation (EDPAF)) como un ente no lucrativo y dedicado a fomentar la educación, comunicación, desarrollo profesional, elaboración de normas e investigación en lo relacionado a los campos de Auditoría en Sistemas de Información.

El 21 de junio de 1978, la Fundación de Auditores de Procesamiento Electrónico de Datos anuncia oficialmente un programa de Certificación Internacional de manera anual, de la Asociación de Auditores de Procesamiento Electrónico de Datos.

EDP AUDITING. Es una fundación que ha desarrollado métodos para evaluar la seguridad de los sistemas computacionales, con el fin de mantener la integridad de los datos y lograr la eficiencia y efectividad de la organización.

Surge en nuestro país la Asociación Mexicana de Auditores en Informática (AMAI), con la finalidad de difundir los avances tecnológicos en está área con el objetivo de lograr así la actualización profesional continua.

3.4 RAMAS DE LA AUDITORÍA INFORMÁTICA SEGÚN EDP AUDITORS

a) Administración de personal en el área de sistemas
b) Seguridad Lógica, Física y Controles Ambientales
c) Continuidad de Operaciones
d) Adquisición, desarrollo y mantenimiento de Sistemas Operativos
e) Adquisición, desarrollo y mantenimiento de Sistemas en Aplicación
f) Tareas en un Centro de Cómputo

Tomando como base una de las ramas de la auditoría en Informática "la Seguridad Lógica, Física y Controles Ambientales" y enfocándonos a desarrollar posteriormente la Metodología del Plan de Contingencias será importante en el siguiente capítulo profundizar en los conocimientos relativos a dicha rama.

CAPITULO II

SEGURIDAD LOGICA

FISICA

Y

AMBIENTAL

4.SEGURIDAD LÓGICA, FÍSICA Y AMBIENTAL DE UN CENTRO DE COMPUTO.

En las organizaciones es importante un plan de seguridad bien definido, el cual debe tomar en cuenta los controles lógicos, físicos y ambientales para salvaguardar el equipo, los sistemas y la información proporcionando confidencialidad, integridad, protección y disponibilidad.

La evaluación del plan de seguridad debe hacerse periódicamente para determinar las modificaciones a los controles.

Deberá existir una persona encargada de la seguridad, quien deberá detectar las posibles amenazas que sufra la organización, evaluar los controles de seguridad existentes e implementar nuevos controles.

Para que las políticas de seguridad puedan ser implantadas, estas deben ser claras, comunicadas a los grupos adecuados y permanecer por escrito.

Las políticas de seguridad, deben permanecer bajo los siguientes lineamientos:

a) La administración debe conocer, aprobar y apoyar.

b) Facilidad para ser accesadas y controladas.

c) Revisión de las autorizaciones de acceso

d) Hacer conciencia de la seguridad en la organización

La falta de seguridad Lógica, Física y Ambiental puede repercutir en:

1.- Pérdidas Financieras
2.- Pérdida de Creditibilidad
3.- Pérdida del margen de Competitividad

El no contar con un plan de seguridad afectaría la continuidad de operaciones.
La seguridad debe:

1) Proteger la integridad, exactitud y confidencialidad de la información
2) Conservar los activos de desastres provocados por la mano del hombre y de actos hostiles
3) Proteger a la organización contra situaciones externas como desastres naturales y sabotajes.

Una vez analizada la seguridad y su importancia veremos a detalle cada uno de los controles lógicos, y posteriormente físicos y ambientales.

4.1 SEGURIDAD LÓGICA.

La seguridad lógica se encarga de los controles de acceso que están diseñados para salvaguardar la integridad de la información almacenada en la computadora, estos controles reducen el riesgo de caer en situaciones adversas que puedan ocasionar grandes pérdidas, las cuales se pueden dar debido a:

a) Mal funcionamiento de las máquinas.
b) Fallas de los datos o del software.
c) Abuso de responsabilidades.

Se puede decir entonces que un inadecuado control de acceso lógico incrementa el potencial de la organización para perder información, así como se ve disminuida su defensa ante personas tales como competidores, crimen organizado, personal desleal y violaciones accidentales.

4.1.1 DEFINICIÓN DE SEGURIDAD LÓGICA:

La seguridad lógica se encarga de controlar y salvaguardar la información generada por los sistemas, software de desarrollo y los programas en aplicación.

La seguridad lógica identifica individualmente a cada usuario y sus actividades en el sistema, restringe el acceso a datos, a los programas de uso general, de uso específico, las redes y a las terminales.

4.1.2 NECESIDAD DE CONTAR CON LA SEGURIDAD LÓGICA:

La falta de Seguridad Lógica o su violación puede traer las siguientes consecuencias a la organización:

a) Cambio de los datos antes o cuando se le da entrada a la computadora.
b) Código oculto en un programa.
c) Entrada de virus.

La Seguridad Lógica es importante debido a la gran cantidad de información que manejan las organizaciones, la cual puede ser confidencial y puede ser mal utilizada o divulgada por personas que hagan mal uso de ésta.

La Seguridad Lógica puede evitar una afectación ó pérdida de registros, ayuda a conocer el momento en que se produce un cambio o un fraude en los sistemas.

4.1.3 AREAS QUE ESTAN DENTRO DE LA SEGURIDAD LOGICA.

Nos referiremos ahora, a cada una de las áreas que abarca la Seguridad Lógica:

a) Rutas de Acceso.
b) Claves de Acceso.
c) Software de Control de Acceso.

4.1.3.1 RUTAS DE ACCESO

El acceso a la computadora no significa tener una entrada sin restricciones. Limitando el acceso a los niveles apropiados puede proporcionarse una mayor seguridad.

El objetivo de la seguridad de los sistemas de información es controlar las operaciones y su ambiente, a través de monitorear el acceso a información y programas.

Para llegar a utilizar algún tipo de software dentro de un sistema es necesario contar con una ruta de acceso. Proporcionaremos una clasificación general del software. **Ver figura 1.**

Cada uno de los sistemas de información tienen una ruta de acceso. El término ruta de acceso puede ser definido como las áreas ó puntos de la trayectoria seguida en el momento de acceso al sistema.
Un usuario puede pasar por uno ó múltiples niveles de seguridad, antes de obtener acceso a los programas y datos.

Los tipos de restricciones de acceso incluyen los siguientes:

Sólo lectura, sólo consulta, lectura y consulta, lectura y escritura, para crear, actualizar, borrar, ejecutar ó copiar.

El acceso lógico dentro de la computadora esta representado en algunas ocasiones por rutas de acceso muy grandes; cada parte de la ruta de acceso debe contener los niveles apropiados de la seguridad de acceso.

El esquema identifica a los usuarios del sistema, los tipos de dispositivos por los cuales accesan al sistema, el software usado para el acceso al sistema, los recursos que pueden ser accesados y los sistemas donde residen estos recursos. Los sistemas pueden ser en línea, fuera de línea ó en batch y rutas de telecomunicación.

El esquema de las rutas de acceso sirve en la identificación de todos los puntos de control que pueden ser usados para proteger los datos en el sistema. El Auditor debe conocer las rutas de acceso para la evaluación de los puntos de control apropiados. **Ver figura 2.**

4.1.3.2 CLAVES DE ACCESO

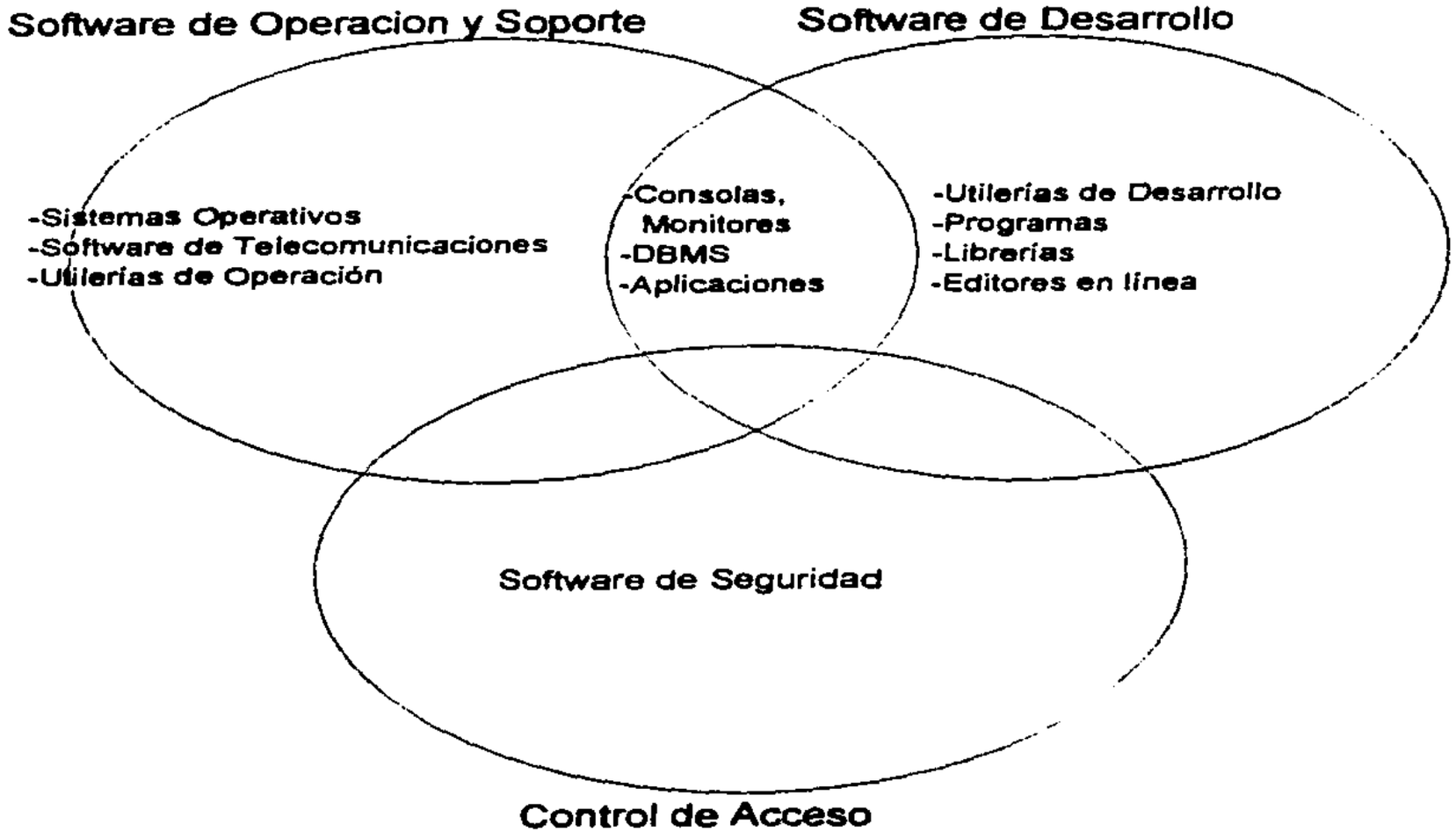
Una importante área en la seguridad lógica, es el control delas claves de accesc de los usuarios.

Existen diferentes métodos de identificación para el usuario:

1. Cuando el Usuario posee un password ó código
2. Cuando el Usuario posee una credencial con banda magnética.
3. Algo específico del usuario (características propias).

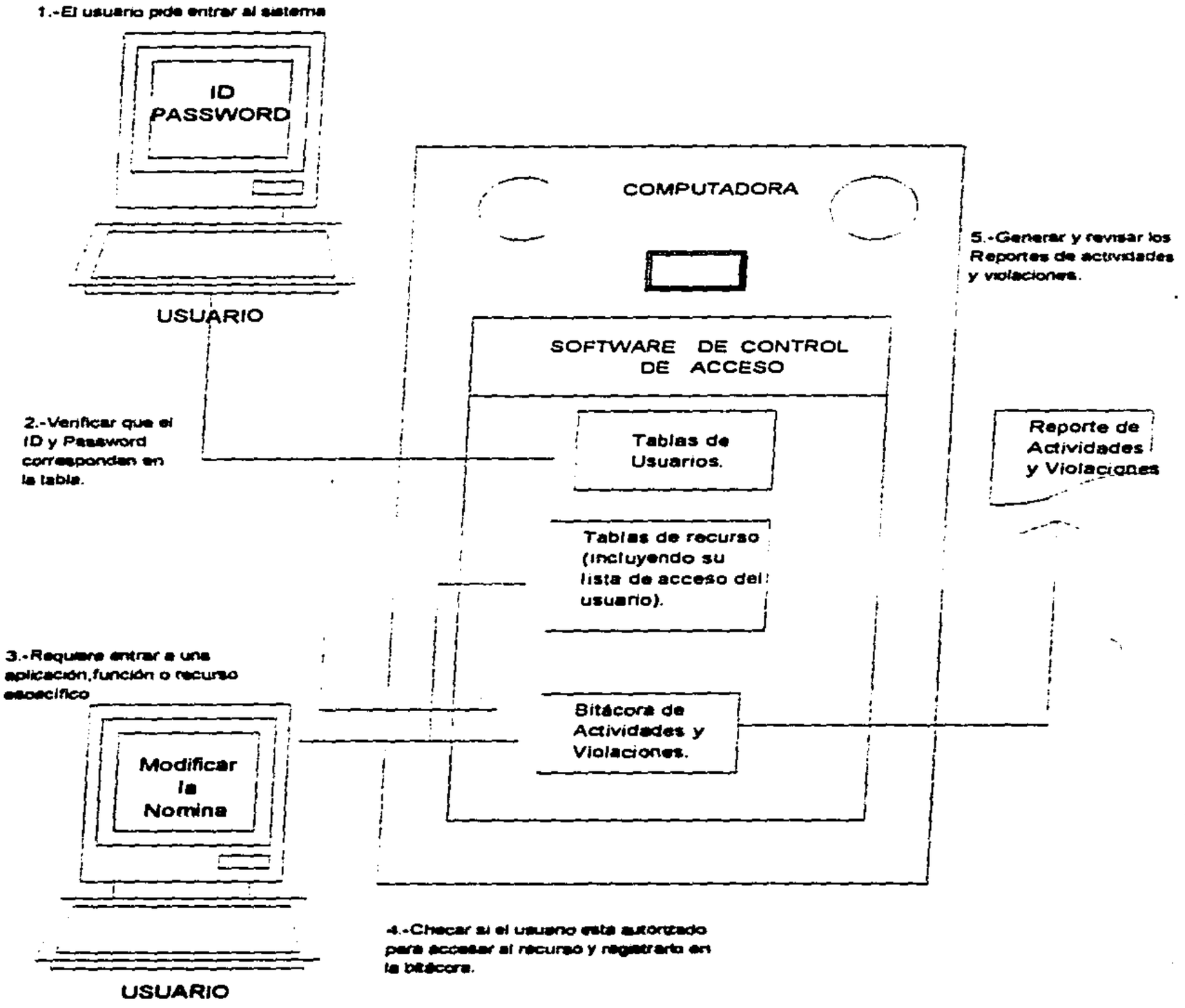
La identificación es definida como el proceso de distinción de un usuario de otros. La identificación de entrada proporcionará un reconocimiento individual, cada usuario debe tener una identificación de entrada única que debe ser reconocida por el sistema.

FIGURA 1



El Software de Seguridad deberá tener control, sobre todo el software del sistema.

ESQUEMA FUNCIONAL DEL SOFTWARE DE CONTROL DE ACCESO.



1. Password ó Código.

La identificación de los individuos es usualmente conocida y asociada con un password. Los passwords pueden ser usados para controlar el acceso a la computadora, a sus recursos ó a funciones específicas.

Primero se verifica que el usuario tenga una identificación de entrada válida y después forzar al usuario a justificar su validez por medio de un password.

El password debe ser de una longitud adecuada para ser secreto, este es un método frecuentemente usado en las terminales remotas dependiendo de los requerimientos de seguridad, el password puede ser cambiado semanalmente, mensualmente, ó cada vez que se considere necesario. El password no debe ser desplegado cuando es tecleado.

Los passwords deben ser encriptados, esto reduce el riesgo de que alguien obtenga el password de otras personas.

Los passwords deben de prohibir el uso de nombres, palabras ó cadenas de caracteres difíciles de retener, además el password no debe ser cambiado por un valor pasado. Se recomienda la combinación de caracteres alfabéticos y numéricos. No debe ser particularmente identificable con el usuario, como su nombre, apellido, nombre de su esposa(o) ó nombre de su mascota.

Quien conoce un password puede no ser la persona a la cual pertenece el password, el password puede ser conocido por muchas personas. Si un password no es usado después de 60 días debe ser desactivado para prevenir un posible mal uso.

Cuando un password es robado, puede ser usado muchas veces antes de que sea detectado, hasta las más sofisticadas técnicas de password no aseguran conocer al verdadero usuario. Los passwords suelen ser copiados, sobrescritos y grabados.

2. Credenciales con banda magnética.

La banda magnética de las credenciales es frecuentemente usada para la entrada al sistema.

La identificación típica de un empleado es la credencial con foto, tal vez la máquina no pueda reconocer la foto, pero se puede hacer la comparación entre el poseedor y la foto.

Las credenciales con banda magnética pueden ser fácilmente reconocidas por el sistema, a menos que se encuentren deterioradas.

La ventaja más importante de la credencial es prevenir la entrada de impostores al sistema, una credencial ordinaria es fácil de falsificar por lo que se debe construir la credencial de una manera especial, que no permita ser reproducida.

3.Validación por características.

Es un método para la identificación del usuario, este método es implantado con tecnología biométrica, consiste en la verificación y reconocimiento de la identidad de las personas, basados en la psicología y características propias.

Algunos de los dispositivos biométricos son:

- Las huellas dactiláres.
- Retina.
- La gecmetría de la mano.
- La firma.
- La voz.

La necesidad de una identificación personal y su validación es necesaria para evitar el número de fraudes en las transacciones. Si los perpetradores de la información sienten que pueden ser identificados, tal vez no asuman este riesgo.

4.1.3.3 SOFTWARE DE CONTROL DE ACCESO.

Puede ser definido como el software diseñado para permitir el manejo y control del acceso a los siguientes recursos:

- Programas de librerías.
- Archivos de Datos.
- Jobs.
- Programas en aplicación.
- Módulos de funciones.
- Utilerías.
- Diccionario de datos.
- Archivos.
- Programas.

Controla el acceso a la información, grabando e investigando los eventos realizados y el acceso a los recursos, por medio de la identificación del usuario.

El software de control de acceso, tiene las siguientes funciones:

a) Definición de usuarios.
b) Definir funciones del usuario después de accesar el sistema.
c) Establecimiento de Auditoría a través del uso del sistema.

Cuando el software de seguridad es instalado protege los recursos, identificando y autorizando a los usuarios por medio de passwords que son definidos por este software. Esto puede ser efectuado a través de la creación de archivos ó tablas de seguridad. Los paquetes de seguridad frecuentemente incluyen facilidades para encriptar estas tablas ó archivos.

Por cada usuario debe ser asignado un alcance en el acceso y por cada recurso un grado de protección. Los recursos pueden ser protegidos de un acceso no autorizado.

Algunos paquetes de seguridad pueden ser usados para restringir el acceso a programas, librerías y archivos de datos, otros pueden además limitar el uso de terminales ó restringir el acceso a bases de datos. Estos pueden variar en el nivel de la seguridad dada en archivos de datos. La seguridad puede ser basada en el tipo de acceso (usuarios autorizados para agregar registros a un archivo ó los que únicamente leen registros).

El software de seguridad controla el acceso a funciones o aplicaciones de programas, esto es realizado por medio de la consola. Estas regulan el acceso a las aplicaciones y a las funciones de programas, tomando en cuenta la definición de módulos asociados con una función específica.

La mayor ventaja del software de seguridad es la capacidad para proteger los recursos de accesos inautorizados, incluyendo los siguientes:

- Procesos en espera de modificación por un programa de aplicación.
- Accesos por los editores en línea
- Accesos por utilerías de software
- Accesos a archivos de las bases de datos, a través de un manejador de Base de Datos(DBMS).

Estos paquetes pueden restringir el acceso a los recursos(archivos de datos), reduciendo así el riesgo de los accesos inautorizados.
Otra característica de estos paquetes es la responsabilidad de detectar las violaciones de seguridad, tomando las siguientes medidas:

1. Terminaciones de procesos.
2. Forzar a las terminales a apagarse.
3. Desplegar mensajes de error.
4. Escribir los registros para la auditoría.

La bitácora de auditoría es seleccionada durante la implementación. Por ejemplo: La bitácora puede consistir en registrar los accesos no exitosos, sólo los intentos, un registro de todos los accesos validos y los recursos protegidos. Algunos paquetes definen específicos datos para ser incluidos en la bitácora de auditoría.

Cada bitácora debe incluir la identificación del usuario, los recursos accesados, día, hora, terminal y un específico dato de lo que fue modificado durante el acceso.
Una revisión funcional del software de control de acceso es la siguiente. **Ver figura 3.**

OTROS TIPOS DE SOFTWARE DE CONTROL DE ACCESO.

Algunos tipos de software son diseñados con características que pueden ser usadas para proveerles seguridad. Sin embargo es preferible usar un software de control de acceso para asegurar el ambiente total y completar las características de seguridad provistas por un software específico.

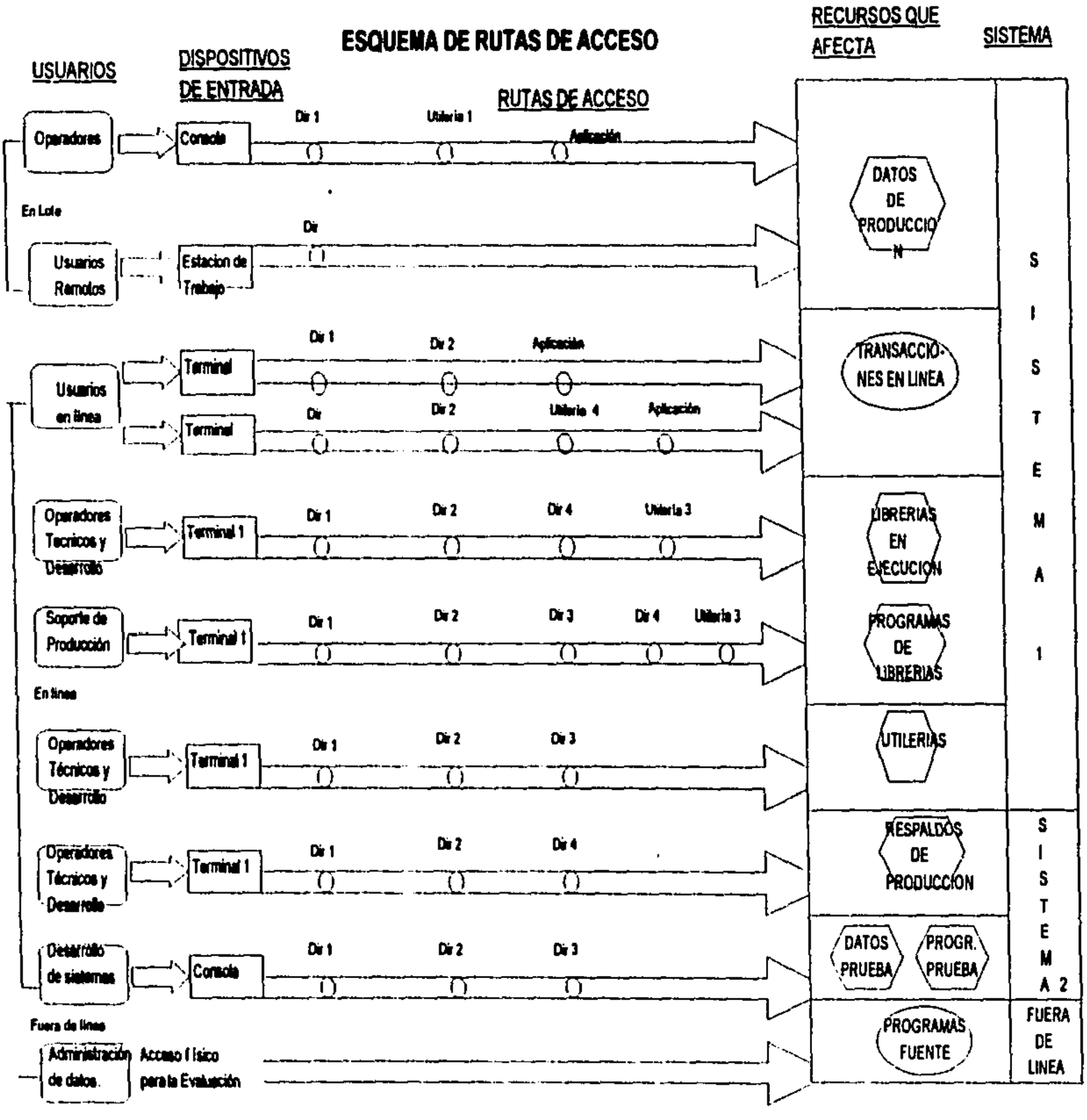
Como existen diferentes tipos de software explicaremos las características de seguridad de los siguientes:

a) Sistemas Operativos
b) Manejadores de Bases de Datos
c) Software de Consolas o Terminales maestras
d) Software de librerías
e) Software de Utilerías
f) Telecomunicaciones

a) SISTEMAS OPERATIVOS.

Pueden ser definidos como una serie de programas que manejan los recursos de las computadoras y sirven como interfase entre el software de aplicaciones y hardware.

ESQUEMA DE RUTAS DE ACCESO



Estos programas manejan y controlan la ejecución de programas en aplicación y proveen los servicios que estos programas requieren. Cada servicio debe incluir un calendario de trabajo (JOB SCHEDULE) manejador de disco y de cinta, un contador de trabajo y un compilador de programas, pruebas y "debugs". El grado de protección sobre estos servicios depende de los sistemas operativos.

Las implicaciones de seguridad relativas a los sistemas operativos (S.O.) incluyen lo siguiente:

1. Control de salidas de los programas al modificarse código.

2. Estos usualmente tienen accesos a los elementos más importantes del sistema, sus actividades deben ser monitoreadas.

3. Los S.O. usan passwords (ID) para prevenir usuarios inautorizados a funciones y utilerías del sistema operativo. Muchas veces estos passwords (ID) están definidos en una tabla del sistema que es activada cuando un sistema es utilizado. Estos passwords (ID's) deben ser cambiados inmediatamente después de los default de venta.

4. Algunos S.O. proveen una característica que puede limitar el número de accesos inautorizados y autorizar usuarios a los recursos protegidos, si esté número es excedido, el usuario inautorizado, es prevenido para el nuevo acceso a estos recursos.

5. Los S.O. permiten una instalación para la implementación opcional de características de seguridad cuando el sistema es instalado.
Algunos Sistemas Operativos contienen sus propias características de seguridad y muchas veces estas no son adecuadas, en este caso es aconsejable integrar al S.O. un producto software de seguridad para proteger los recursos. El valor de los recursos es el factor determinante cuando se decide que tanta protección es necesaria.

6. Los S.O. tienen un completo control sobre las actividades de todas las aplicaciones que están corriendo en el sistema. Si un usuario no autorizado puede lograr accesar los recursos del sistema operativo, este usuario puede hacer modificaciones que alteren el proceso normal del flujo del sistema. El S.O. tiene autoridad para dar facilidades de seguridad y para accesar recursos confidenciales. Este implica el uso de algún producto de seguridad.
El software de funciones de control del S.O. debe proveer una bitácora de auditoría.

7.Tanto el administrador del sistema o el administrador de la Seguridad de Datos, establecen sus privilegios a través del sistema operativo. Individualmente con estos privilegios tienen completo control sobre el sistema operativo y su ambiente, ellos pueden otorgar la autoridad para modificar usuarios y accesar profiles, alterar la generación de procedimientos del sistema y modificar las prioridades de "Jobs" que corren dentro del control del Sistema. Debe existir una bitácora de las actividades del administrador del sistema o del administrador de la seguridad de Datos.

8.Los S.O. permiten la definición de consolas o terminales maestras desde las cuales los operadores pueden introducir comandos al sistema operativo. Las consolas no requieren una señal en proceso para la emisión de comandos. Por lo tanto el acceso a áreas físicas donde las consolas son localizadas debe ser restringido.

Además las caracterfsticas del sistema que permiten a una terminal ser asignada con el status de "Consola" deben ser guardadas a prueba de accesos inautorizados.

b) SOFTWARE MANEJADOR DE BASE DE DATOS.

Es un software para controlar, organizar y manipular los datos. Provee múltiples caminos para accesar los datos en una base de datos. Maneja la integridad de datos entre operaciones, funciones y tareas de la organización.

Cuando un usuario inicialmente requiere del uso del DBMS, se establece un identificador para el usuario y la sesión. Inmediatamente modifica el modo, el usuario puede ser identificado por el ID-Usuario, ID-Terminal, y una aplicación o función.

En espera del modo de modificaciones, el usuario podrá ser identificado por el Job, por la aplicación o función.

El identificador del usuario será usado para rastrear todos los accesos a los archivos de datos a través del DBMS.

Las caracterfsticas de seguridad del software DBMS pueden ser usadas para restringir el acceso a un usuario especffico, a un cierto archivo o a vistas lógicas, los accesos a procedimientos, funciones o software en aplicación es limitado a usuarios autorizados con el propósito de ejecutar sus tareas asignadas. Las vistas de datos lógicos están colocadas en archivos para usuarios particulares, funciones, o aplicaciones y puede ser representada toda o parte del archivo de datos ffsicos o una combinación de campos de múltiples archivos de datos ffsicos. Estas caracterfsticas son usadas para controlar funciones únicas en el DBMS.

Las utilerfas de la Base de Datos proveen funciones de mantenimiento, como respaldos y restauración de la base de datos, reorganización de datos, reportes estadfsticos de las bases de datos y sus relaciones. Estos pueden ser usados además para adicionar o borrar datos y proveer seguridad.

El diccionario de datos (DD , software que provee un método para documentar elementos de la base de datos y puede proveer un método de seguridad de datos en un DBMS. Los elementos de los datos pueden ser seleccionados y presentados como vistas (a estos se les llama subesquema). El DD provee una vista especffica de los datos o da una vista de datos para cada usuario (Por su ID o por el nombre del programa en aplicación). En cada vista de datos especffica el usuario tiene la habilidad para modificar los datos en la vista.

El DD es típicamente accesible en un modo de lectura, está documentación es frecuentemente considerada benéfica para las aplicaciones y desarrollo de mantenimiento. La habilidad para agregar o modificar está información pude ser controlada para asegurar la integridad de la documentación. En general la habilidad para modificar el DD debe ser restringida por el DBMS.

El acceso a determinas entidades es utilizado por los programadores de aplicaciones en pruebas o ambientes de desarrollo.

Todas las modificaciones al DD deben producir una bitácora de auditorfa, como un registro automático de todos los cambios y un medio de recuperación después de alguna interrupción que hubiese ocurrido.

c) SOFTWARE DE CONSOLAS O TERMINALES MAESTRAS.

El software de consolas o temrinales maestras puede ser definido como programas del sistema operativo que proveen soporte y servicio para que las terminales en línea accesen a los programas en aplicación.

Las consolas incluyen funciones de seguridad para restringir el acceso a los datos, vía programas en aplicación.

Estas funciones son frecuentemente basadas en una serie de tablas que definen a los usuarios autorizados, los recursos y programas en aplicación que ellos pueden accesar. Generalmente las consolas pueden sólo limitar el acceso al usuario para entrar a un programa en aplicación, no para el uso de funciones específicas de un programa.

La mayor parte de las consolas mantienen un registro de uso de un password diario válidos o no válidos.

d) SOFTWARE DE LIBRERÍAS

El software de librerías consiste en datos y programas específicos escritos para ejecutar una función en la organización.

Los programas en aplicación (librerías) pueden ser guardados en archivos en el sistema, y el acceso a estos programas pueden ser controlados a través del software (software de control de acceso general) usado para controlar el acceso a estos archivos.

La mayor parte de las organizaciones con gran desarrollo de librerías utilizan software de seguridad específico para controlar el uso de estos programas.

El software de manejo de librerías puede ser usado para mantener y proteger los recursos de programas de librerías, ejecución de "jobs", y en algunas instancias los archivos de datos utilizados por estas.

Una importante función del software controlador de librerías es controlar y describir los cambios de programas en una bitácora. El software de librerías, provee diferentes niveles de seguridad los cuales son reflejados en las bitácoras de auditoría.

Estas librerías deben ser soportadas por un adecuado control de cambios y procedimientos de documentación para proveer un buen control de los cambios en el ambiente.

Los controles de cambios de emergencia deben estar en algún lugar. Porque por la naturaleza de estos cambios (estos frecuentemente son realizados fuera de horas de trabajo normal, son cortos y sin noticia):

a) Accesos de emergencia, concedidos con el propósito de resolver el problema, puede ser inmediatamente revocado después de que el problema es resuelto.

b) Todas las acciones realizadas durante la emergencia deberán ser automáticamente registradas.

Cuando el software de librerías es instalado, son definidas las librerías y sus respectivos niveles de protección.

Los tipos de acceso a la librería pueden ser restringidos durante la instalación. Por ejemplo un programador deberá ser autorizado para leer o modificar un programa.

e) SOFTWARE DE UTILERIAS

Existen dos tipos de software de utilerías, el primer tipo es usado en los sistemas de desarrollo para proveer productividad. Desarrollo de programas y editores en línea son los ejemplos de esté tipo de software. El segundo tipo es usado para asistir en el manejo de operaciones de la computadora. Monitoreos, calendarios de trabajo, sistema manejador de disco y cinta son ejemplos de esté tipo de software.

El software de utilerías tiene privilegios de acceso todo el tiempo, algún tiempo o nunca. Los accesos privilegiados se otorgan a programadores o a usuarios que ejecutan funciones que sobrepasan la seguridad normal.

EJEMPLOS DE UTILERÍAS DE SOFTWARE:

a)Utilerías de monitores.
b)Sistemas manejadores de cinta.
c)Sistemas manejadores de disco.
d)Calendarios de Jobs.
e)Editores en línea.
f)Debugers.
g)Scaners de virus.

f) SOFTWARE DE TELECOMUNICACIONES

Ciertos tipos de software de telecomunicaciones pueden restringir el acceso a las redes y para aplicaciones específicas localizadas en la red.
El software de telecomunicaciones provee la interfase entre las terminales y en las redes y tiene la capacidad para asegurar lo siguiente:

- Controlar la invocación de los programas de aplicación.
- Verifica todas las transacciones que sean completa y correctamente transmitidas.
- Restringe a los usuarios para actuar en funciones seleccionadas.
- Restringe el acceso al sistema a ciertos individuos.

4.1.6. RIESGOS Y CONTROLES A AUDITAR

El mayor riesgo asociado con accesos lógicos es que la integridad, confidencialidad y disponibilidad de Sistemas de Información, datos y recursos deben ser vigilados:

1. La integridad es responsabilidad de los individuos autorizados para modificar datos o programas o por usuarios a quienes se otorgan accesos a aplicaciones de sistema o funciones fuera de sus responsabilidades normales de trabajo.

2. La confidencialidad es responsabilidad de los individuos autorizados a ver reportes mientras están en espera de impresión o para bajar archivos importantes para microcomputadoras.

3. La disponibilidad es responsabilidad de individuos autorizados para alterar los parámetros de control de acceso, al sistema operativo, al sistema manejador de Base de Datos, al monitoreo de teleproceso, o al software de telecomunicaciones.

El grado de control implantado para minimizar estos riesgos debe considerar los siguientes factores:

1. El valor de los datos siendo procesados.
2. La probabilidad de que un acceso no autorizado ocurra.
3. Las consecuencias para la organización si un acceso no autorizado ocurre.

A continuación, hablaremos de los controles de software de seguridad general y de software específico que pueden ser implantados para minimizar el riesgo de la seguridad lógica.

a) CONTROLES DEL SOFTWARE DE SEGURIDAD GENERAL:

Los controles del software de seguridad general aplican para todos los tipos de software y recursos relacionados y pueden ser clasificados como siguen:

1. Vigilar Control de Acceso a programas y a la información.
2. Vigilar los Cambios realizados.
3. Bitácoras de Auditoría.

1. Control de Acceso a Programas y datos. Este control de acceso se refiere a la manera en que cada software del sistema tiene acceso a los datos, programas y funciones. Los controles son usualmente a través del ID (Identificador) o a través del password para identificar a usuarios inautorizados y para controlar el acceso inicial al software.

2. Cambios realizados. Deben ser probados y revisados para ser autorizados. Y una vez autorizados son hechos a los programas en aplicación y datos. Dependiendo de la aplicación , el ambiente y el potencial del efecto de los cambios, este puede ser muy informal o extremadamente rígido. Los procedimientos a seguir para los cambios realizados pueden ser los siguientes:

- Diseño y código de modificaciones.
- Coordinación con otros cambios.
- Asignación de responsabilidades.
- Revisión de estándares y aprobación.
- Requerimientos mínimos de prueba.
- Procedimientos del respaldo en el evento de interrupción.

La bitácora de auditoría debe registrar cambios en el software antes de la implementación. Los procedimientos de cambios de software deben además incluir notificaciones escritas para el departamento apropiado de cada cambio. Los cambios realizados deben incluir independientemente una fase de pruebas realizadas por un grupo fuera del ambiente de desarrollo.

3. Bitácoras de Auditoría. Las Bitácoras de auditoría son usadas para monitorear los accesos permitidos y negados. El software debe contener una bitácora de auditoría del uso de las funciones que el software ejecuta, particularmente si cambian las funciones o se modifican datos. Esta bitácora de auditoría posiblemente sea mantenida en un archivo separado, puede ser manejada

por las actividades del sistema, o tal vez sea una parte del registro. El tipo de bitácoras de auditoría varia gradualmente de acuerdo al software y al vendedor, por ejemplo algún software guarda antes y después imágenes de los cambios, mientras otros solamente tienen una técnica de recuperación que puede ser usada para seguridad en casos necesarios.

Las bitácoras de auditoría generalmente son relacionadas con el sistema operativo o con el software de control de acceso.

Estas bitácoras de auditoría registran las actividades y opcionalmente muestran el registro de los cambios hechos en el archivo o programa. Estas son importantes para el seguimiento de los cambios.

b) CONTROLES DE SOFTWARE ESPECIFICO:

Algunos de los controles usados por los diferentes tipos de software específico son:

El acceso al sistema debe ser restringido para individuos no autorizados
Controlar el acceso a los procesos y a las aplicaciones permitiendo a los usuarios autorizados ejecutar sus obligaciones asignadas y evitar a personas no autorizadas el logro del acceso.

Las tablas de acceso o profiles deberán ser establecidos de manera que sea restringido a los usuarios de ejecutar funciones incompatibles o más haya de sus responsabilidades.

Se deberá contar con procedimientos para que a los programadores de aplicaciones tengan prohibido realizar cambios inautorizados a los programas.

Deberán ser limitados tanto usuarios como programadores de aplicaciones a un tipo específico de acceso de datos(ejemplo: lectura y modificación).

Para asegurar las rutas de acceso deberá ser restringido el acceso a profiles o tablas de seguridad, mismas que deberán ser encriptadas.

Las bitácoras de auditoría deberán ser protegidas de modificaciones no autorizadas.

Deberán ser restringidas las modificaciones o cambios al software de control de acceso, y estos cambios deberán ser realizados de acuerdo a procedimientos autorizados.

- <u>Software de Sistemas Operativos.</u> Los controles incluyen los siguientes:

Los passwords e identificadores deberán ser confidenciales. Los usuarios no autorizados que logran accesar al sistema pueden causar modificaciones no autorizadas.

Deberá ser restringido el acceso al software de sistema operativo.

Los administradores de la seguridad deberán ser los únicos con la autoridad para modificar funciones del sistema incluyendo procedimientos y tablas de usuarios.

El acceso a utilerías del sistema operativo será restringido.

Las instalaciones de sistemas y las reinstalaciones deben ser monitoreadas porque la realización no autorizada puede resultar inválida.

El uso de todas las funciones del software (editores de línea, consolas) es restringido a individuos autorizados.

Las bitácoras de auditoría son revisadas para determinar si un acceso no autorizado ocurre o si son realizadas modificaciones.

- Software manejador de Base de Datos. Los controles incluyen lo siguiente:

El acceso a los archivos de datos deberá ser restringido en una vista de datos lógica, a nivel de tipo de campo. La seguridad en el campo será dada deacuerdo al contenido del campo (validación de campos).

Deberá ser controlado el acceso al diccionario de datos.

La Base de Datos debe ser segura usando las facilidades de control de acceso construidas dentro del software DBMS.

La bitácora de auditoría debe reportar los accesos al Diccionario de Datos.

Las modificaciones de capacidades desde el DBMS para las Bases de Datos son limitadas a personal apropiado.

- Software de consolas o terminales maestras. Estos controles incluyen lo siguiente:

Los cambios realizados al software de consolas ó terminales maestras deberá ser protegido y controlado.

- Software de librerías. Los controles incluyen los siguientes:

El software de librerías mantiene una bitácora de auditoría de todas las actividades realizadas. La información provista en la bitácora incluye el nombre del programa, el número de la versión, cambios específicos realizados, fecha de mantenimiento e identificación del programador.

El software de librerías tiene la facilidad de comparar dos versiones de programas en código fuente y reportar las diferencias.

Debe ser limitado el acceso a programas o a datos almacenados por el software de librerías.

El acceso a passwords o códigos de autorización es restringido a individuos no autorizados.

Los cambios realizados al software de librerías tendrán que ser protegidos y controlados.

Las versiones correctas de los programas de producción deben corresponder a los programas objeto.

- Software de Utilerías. Los controles incluyen los siguientes:

Deberá ser restringido el acceso a archivos de utilerías. Algunas utilerías establecen niveles de utilización por cada función y verifican cada nivel de autorización del usuario antes de darle acceso, utilizando password para preveer accesos no autorizados.

El software de utilerías genera una bitácora de auditoría de usos y actividades. Algunas proveen bitácoras detalladas de actividades con datos protegidos, librerías y otros recursos. Estas bitácoras de auditoría proveen información de cada identificador (ID), fecha y hora de acceso, recursos accesados y tipo de acceso.
Esta sirve como un registro de eventos, incluyendo violaciones a la seguridad y accesos inautorizados. Cada paquete de software puede tener diferentes capacidades de control.

Tomar precauciones para asegurar la manipulación de datos (copiar, borrar, etc.) protegiéndolos de un uso no autorizado.

Asegurar que únicamente personal autorizado tenga acceso a correr aplicaciones.

Las utilerías no deben ser mantenidas en el ambiente de producción y asegurar que únicamente usuarios autorizados tengan acceso a ellas.

Las bitácoras de auditoría producidas por utilerías deben ser cuidadosamente revisadas para identificar alguna violación a la seguridad.

- Software de telecomunicaciones. Los controles incluyen los siguientes:

Controlar el acceso a datos sensitivos y recursos de la red de la siguiente forma:

1. Verificación de "login" de aplicaciones.

2. Control de las conexiones entre sistemas de telecomunicaciones y terminales.

3. Restricción al uso de aplicaciones de la red.

4. Protección de datos sensitivos durante la transmisión, terminando la sesión automáticamente.

Los comandos del operador que pueden dar shoutdown a los componentes de la red sólo pueden ser usados por usuarios autorizados.

El acceso diario al sistema es, monitoreado y protegido.

Asegurar que los datos no son accesados o modificados por un usuario no autorizado, durante la transmisión o mientras esta en almacenamiento temporal.

4.1.6.1 CONSIDERACIONES A AUDITAR.

Cuando se realiza una revisión de seguridad lógica, el auditor interno deberá evaluar y probar los siguientes tres controles implantados para minimizar riesgos.

1.- Control de Acceso a Programas y a la Información.
2.- Control de Cambios.
3.- Bitácoras de auditoría.

La evaluación de todos los tipos de software deberá asegurar que los siguientes objetivos sean cumplidos:

a) El acceso a funciones, datos y programas asociados con el software es restringido a individuos autorizados y debe ser consistente con documentos esperados.

b) Todos los cambios del software deben ser realizados de acuerdo al manejo de autorizaciones.

c) Se debe de mantener una bitácora de auditoría de todas las actividades significativas.

Una auditoría de seguridad lógica puede ser realizada en diferentes formas. La auditoría puede enfocarse en áreas de seguridad que son aplicables a todo tipo de software y pueden cubrir la instalación, mantenimiento y utilización del software.

Otro aspecto puede ser sobre las características de seguridad del software, incluyendo el control de acceso, identificación del usuario y el proceso de autentificación del usuario, ejecutado por el software.

Consideraciones específicas a auditar:

1.-Software de Control de Acceso.
2.-Software de Telecomunicaciones.
3.-Software manejador de Librerías.
4.-Software manejador de Bases de Datos.
5.-Software de Utilerías.
6.-Software de Sistema Operativo.

-Ciclo de Vida del Software.

Durante el ciclo de vida del software deben ser evaluadas su instalación, mantenimiento y operación. Se debe utilizar la auditoría para asegurar que algún cambio hecho al software no comprometa la integridad, confidencialidad o aprovechamiento de los datos o recursos del sistema.

Puede ser usado el Software de Auditoría especializado para revisar todos los cambios y asegurarse que son ejecutados de acuerdo con los procedimientos aprobados por la Gerencia.

a' Instalación y Mantenimiento.

Es la primer fase del ciclo de vida del software en la cual debe ser revisado por el Auditor lo siguiente:

1.-Procedimientos para nuevas pruebas o modificaciones al software, incluyendo al personal responsable, ejecución de pruebas, respaldo de software existente, pruebas de funciones, documentación de cambios, notificación de cambios, revisión y retención de pruebas de salida, y aprobar prioridades para la implementación.

2.-Procedimientos para iniciación, documentación, pruebas y aprobación de modificaciones al software.

3.-Procedimientos para la generación y modificación al software.

4.-Procedimientos usados para ejecutar software y mantenimiento al diccionario de datos para un mayor grado de modificación.

5.-Procedimientos de emergencia usados para dar solución a un específico problema de software.

6.-Mantenimiento y contenido de las bitácoras de auditoría de todos los DBMS y modificaciones del Diccionario de Datos.

7.-Bitácoras a los parámetros del software y de las sentencias del lenguaje de aplicaciones en ejecución.

8.-Acceso a librerías de programas.

b) Operación.

La segunda fase del ciclo de vida del software en la cual debe ser revisado por el Auditor lo siguiente:

1.-Controles de acceso para los programas, librerías, parámetros, profiles o archivos de software asociados.

2.-Procedimientos diseñados para asegurar que el sistema no es instalado (carga inicial del programa) sin el software original, creando un procedimiento de seguridad.

3.-Disponibilidad y control de acceso a los comandos que pueden ser usados para desactivar el software.

4.-Áreas de responsabilidad para el control del software, operación y consistencia de capacidad de acceso.

5.-Horas durante las cuáles el software está disponible.

6.-Procedimientos para la iniciación y terminación del uso del software.

7.-Control de acceso sobre consolas y terminales maestras.

8.-Procedimientos para registrar terminación anormal o errores, los cuales pueden indicar problemas en la integridad del software y documentar los resultados en programas de seguridad.

9.-Controles de acceso sobre escritura de programas y lenguajes de librerías y de aplicaciones en ejecución.

10.-Bitácoras de auditoría sobre las actividades del software.

11.-Dependencia de otro software para continuar la operación, operaciones automatizadas o dependencia al calendario de actividades.

-Software de control de Acceso.

Las consideraciones de auditoría para el Software de Control de Acceso incluye los siguientes:

1.-Diseño y administración.
2.-Procedimientos de identificación del usuario.
3.-Procedimientos de autentificación del usuario.
4.-Recursos para controlar el acceso.
5.-Reportes y Vigilancia del Software de control de acceso reportando y vigilando.

El software de control de acceso usualmente provee utilerías que pueden ser usadas en la ejecución de una auditoría. Los eventos pueden ser registrados en un archivo de auditoría (cambios en el sistema, así como la ocurrencia de otras numerosas actividades, login, archivos de acceso, recursos de acceso, violaciones y cambios de acceso).
Los reporteadores y otras utilerías pueden ser usadas para presentar esta información continuamente.

Diseño y Administración. Los auditores internos deben revisar lo siguiente:

a)Localización de archivos de seguridad y tablas para asegurar que los archivos del software de control de acceso son protegidos.

b)Uso de recursos o controles de acceso a nivel del usuario para asegurar que el software de control de acceso protege datos y recursos en un nivel correcto.

c)Archivos de seguridad o encriptación de tablas usadas para prohibir la vista de tablas individuales.

d)Limitaciones de acceso para archivos de seguridad conteniendo profiles y passwords.

e)Limitaciones de acceso a archivos de seguridad a través de la administración de comandos de la seguridad en línea o utilerías.

f)La jerarquía de seguridad.

g)Los usuarios encargados de la administración de la seguridad, pueden tener gran capacidad para cierto software.

h)Métodos y limitaciones sobre archivos de seguridad o modificación de tablas.

i)Responsabilidades de usuario para la administración de la seguridad, particularmente en un descentralizado ambiente para asegurar que las capacidades definidas son consistentes con las responsabilidades.

j)Definición de parámetros de seguridad, tanto como los recursos definidos, reglas de password, default de niveles de acceso y opciones de login. (Con aprobación de la gerencia, considerando pruebas de protección para accesar recursos protegidos).

-Procedimientos de Identificación del Usuario.
Los auditores deberán ejecutar los siguientes pasos:
Deberán ser revisados y aprobados los métodos usados para definir usuarios para el software.

Las siguientes situaciones deberán ser revisadas por un apropiado nivel de dirección:

- Las identificaciones del usuario para corroborar que sean individuales y no compartidas.
- Probar la revocación de usuarios inactivos.
- El despliegue de la última fecha y hora en que algún I. D. específico fue usado. Esta información podrá ayudar para identificar actividades ilícitas.
- Revocación o desconexión de identificaciones de usuario siguiendo un específico número de acceso inválido. Este control puede también limitar actividades ilícitas.
- El uso de comienzo y fin de fechas para ID de usuario de empleados contratados.
- El uso de grupos de usuarios para el recurso de acceso a los archivos. Los usuarios deberán ser asignados a los grupos apropiados.
- Propietarios de datos y recursos para asegurar que ellos son los apropiados responsables.

-Procedimientos de autentificación del Usuario.
Los auditores internos deberán revisar lo siguiente:

1.- Deberá ser evaluado el uso de passwords o información personal durante la sesión.

2.- Deberá ser identificada la disponibilidad de automatizar funciones una vez identificado el usuario, y autentificación de procedimientos.

3.- Deberá ser identificado el uso de passwords por otro personal que no sean usuarios autorizados.

4.- Los procedimientos para el uso de passwords para asegurar que este es protegido cuando es usado por el usuario.

5.- La máscara del password para asegurarse que el área donde los caracteres son tecleados no se desplieguen.

6.- La sintaxis del password. Algún software de control de acceso puede restringir el uso de ciertas palabras o cadenas de caracteres.

7.- El procedimiento de expiración del password.

8.- El mantenimiento de la historia del password. Este puede ser usado para prevenir usuarios que reutilizan un password por un específico período de tiempo.

9.- Procedimientos para suplir identificaciones de usuarios y passwords, por procesos batch.

-Los Recursos para controlar el Acceso.
Los auditores internos deberán revisar lo siguiente:

1.- Posibles niveles de acceso.
2.- Niveles de acceso por default particularmente para usuarios o jobs que no tienen un ID de usuario.
3.- El acceso del usuario a archivos de seguridad.
4.- Que la seguridad sea implantada en el nivel correcto.
5.- Procedimiento para asegurar la protección automática.
6.- Procedimientos para la protección de recursos.

7.- Uso de "Rutas rápidos" o aceleradas funciones a través de controles.
8.- Controles de acceso sobre aplicaciones locales o remotas.
9.- Restricciones de acceso sobre recursos críticos del sistema, tales como sistemas, programas y aplicaciones en ejecución, librerías del lenguaje, catálogos del sistema y directorios, diccionarios de datos, logs y archivos de password, tablas de definición de privilegios, algoritmos de encriptación y tablas de datos.

- Reportes y Vigilancia del Software de Control de Accesos.

El auditor interno deberá revisar los siguientes pasos:

1.- Login, identificación del acceso autorizado al sistema y el uso de recursos.

2.- Las identificaciones de acceso no autorizado.

3.-La identificación de archivos de seguridad, mantenimiento a tabla y el uso de comandos sensitivos.

4.- El login de usuarios privilegiados y sus actividades.

5.- Las restricciones de acceso a archivos de log del sistema, estos archivos frecuentemente contienen las bitácoras de auditoría al control de acceso.

6.- Sistema operativo o Software de control de acceso existente.

7.-Las violaciones a la seguridad.

8.- Los archivos de seguridad y la generación de reportes de las actividades del usuario para asegurar que los propietarios de datos y recursos son notificados de los eventos de seguridad en un período de tiempo.

-Sistemas Operativos.

El auditor deberá revisar, evaluar y probar el uso y procedimientos que gobiernan programas, usuarios y funciones del Sistema Operativo, especialmente los siguientes:

1.-Las facilidades del S.O. como son la supervisión y privilegios para programas y usuarios.

2.-Controles de Acceso sobre tablas que definen privilegios de usuarios, programas y funciones.

3.-Controles de Acceso sobre consolas o terminales maestras y privilegios asociados.

4.-Bitácoras de auditoría.

5.-Posibilidad y uso del Control de Acceso sobre los default de inicio de ID'S de usuarios y passwords.

6.-Comandos de software o funciones que son consideradas importantes como mantenimiento de seguridad al profile.

7.-Diagnostico de utilerías del S.O. que pueden ser usados para leer o almacenar áreas que contienen información importante.

-Software del Sistema Manejador de Bases de Datos.

Las siguientes funciones de software que restringen el acceso a datos, recursos y los procedimientos que gobiernan el uso de estas funciones.
El auditor deberá revisar, evaluar y probar lo siguiente:

1.-Procedimientos usados por el software de control de acceso para restringir el acceso a la Base de Datos y al Diccionario de Datos.

2.- El diseño de una restricción de acceso en los archivos por niveles, incluyendo restricciones sobre archivos físicos y lógicos en el DBMS y en el Diccionario de Datos.

3.-Seguridad de campos, uso de profiles de usuarios y passwords y restricciones de acceso.

4.-Si el software ejecuta la función de identificación del usuario y procedimientos de autentificación.

5.-Comandos y funciones del Diccionario de Datos, (utilerías del administrador de la Base de Datos, comandos para modificar DBMS, archivos o definiciones de archivo).

6.-Accesos de los programadores, acceso a DBMS y comandos o funciones del DD.

7.-Bitácoras de Auditoría.

8.-El software de desarrollo que afecta a la seguridad del DBMS.

El manejador de la Base de Datos y el Diccionario de Datos usualmente proveen utilerías para revisar e imprimir las capacidades de acceso, información del usuario y bitácoras de auditorías.

-Software del Manejo de librerías.

Las funciones del software restringen el acceso a librerías críticas y los procedimientos que gobiernan el uso de esas funciones deberán ser revisados, evaluados y probados. El auditor deberá revisar, evaluar y probar lo siguiente:.

1.-Documentación de librerías.
2.-Programas fuentes y ejecutables.
3.-Jobs en ejecución y lineamientos de control.
4.-Parámetros de corrida.
5.-Uso de software para restringir el acceso a librerías.
6.-Restricción en acceso a librerías de producción.
7.-Restricciones de funciones que pueden ser usadas para modificar el estado de un programa (pruebas a producción).
8.-Acceso a librerías en prueba.
9.-Convenciones para dar nombre a librerías que son usadas para facilitar la seguridad.
10.-Métodos para clasificar y restringir el acceso a librerías por tipo (fuentes, objeto, carga y control de job).
11.-Si el software ejecuta funciones de identificación de usuario y procedimientos de autentificación.
12.-Procedimientos inusuales de las librerías.
13.-Capacidades de la Bitácora de auditoría.
14.-Los números de versión de software.

Los reportes escritos pueden ser usados para reportar las actividades de las librerías de logs de acceso al software manejador de librerías o bitácoras de auditoría.

-Software de Utilerías.

El auditor deberá evaluar, revisar y probar los siguientes procedimientos diseñados para limitar el acceso a comandos de utilerías o funciones:

1.-Funciones o comandos de utilerías.
2.-Los controles de acceso sobre comandos o funciones de utilerías.
3.-Seguridad de acceso a los programadores para la utilización de funciones o comandos de utilerías.
4.-Si el software ejecuta las funciones de identificación del usuario y procedimientos de autentificación
5.-Capacidades de uso de utilería para cada grupo de usuarios.
6.-Bitácoras de Auditorías.

El software de utilerías no provee bitácoras de auditoría. El reporte escrito del software típicamente debe ser usado para esto puede utilizarse el software de control de acceso, si este es integrado con el software.
Deberán ser usados reportes para monitorear el control de acceso.

-Software de Telecomunicaciones.

El auditor deberá revisar, evaluar y probar la posibilidad y uso de las funciones del software que restringe el acceso en las redes de Telecomunicaciones y los procedimientos que gobiernan su uso, especialmente los siguientes:

1.- Restricciones al acceso de la red basados en tiempo, día, usuario, lugar y terminal.
2.- El apagado automático de terminales inactivas en un específico tiempo (terminales que pueden ser usadas).
3.- Facilidad de acceso no autorizado basada en protocolos de transmisión y líneas rápidas para la conexión rápida.
4.- El número de seguridad de entrada (revisar la posibilidad de este número para acceso local o tableros de boletín nacional.)
5.- "Auto-respuesta", facilidad de uso sobre modem.
6.- Horas durante las cuales la línea esta disponible.
7.- Recursos y funciones posibles a través del acceso de entrada.
8.- Uso de identificación de la terminal físicamente
9.- Controles de acceso sobre los recursos de la red.
10.- Controles de acceso sobre tablas de configuración de red.
11.- Controles de acceso a funciones de la red.
12.- Seguridad física sobre líneas telefónicas y telecomunicaciones.
13.- El uso de Red de área local y la conectividad para otras LANS, WANS o redes en otro lugar.
14.- Si el software ejecuta las funciones de la identificación del usuario y procedimientos de autentificación
15.- Procedimientos para la protección de comunicaciones (desde las conexiones hasta la recepción no autorizada).
16.- Posibilidad y uso de encriptación de datos o mensajes técnicos de identificación.

Los reportes escritos pueden ser usados para reportar las actividades de la red, de logs de acceso a software de telecomunicaciones o bitácoras de auditoría. Estos pueden además hacerlo con el software de control de acceso.

-REPORTES ESPECIALES DE AUDITORÍA.

Los reportes especiales de Auditoría deberán mostrar lo siguiente:
1.-Personal registrado por el sistema que al no corresponder el password con su identificador o el personal que ha intentado más de dos veces entrar al sistema sin un password autorizado.

2.-Identificaciones de usuario no usados hace 6 meses.

3.-Identificaciones de usuarios con privilegios especiales.

4.-Un reporte de referencias cruzadas que debe mostrar a los ID's usuarios con cada acceso a las aplicaciones.

5.-Listar todos los ID's usuarios por grupos.

4.2 SEGURIDAD FÍSICA Y AMBIENTAL

4.2.1 DEFINICIÓN DE SEGURIDAD FÍSICA Y AMBIENTAL.

La segurida Física y Ambiental tiene como objetivo establecer polfticas, procedimientos y prácticas para evitar las interrupciones prolongadas del servicio de procesamiento de información debido a contingencias como incendio, inundación, huelgas, disturbios, sabotaje.

4.2.2 NECESIDAD DE CONTAR CON SEGURIDAD FÍSICA Y AMBIENTAL.

Al seleccionar un lugar para un centro de cómputo se debe dar especial consideración a la protección del procesamiento de información y al equipo. Se puede perder tiempo de procesamiento a causa de accidentes, desastres o sabotaje.

Desastres naturales: Daños por inundación, rayo, terremoto o tornados pueden ser evitados o minimizados por técnicas de construcción y/o selección de lugar.

Accidentes: Daños accidentales al centro de cómputo o a la información de entrada o salida, pueden causar perdida considerable de tiempo. La reducción de daños accidentales puede ser obtenida por las siguientes medidas:

a) Prohibir fumar, tomar o comer alimentos dentro del centro de cómputo. La comida, el tabaco y los lfquidos pueden ocasionar incendios o dañar equipo delicado(especialmente en caso de lfquidos). Estas prohibiciones deben de estar claramente señaladas a la entrada del centro.
b) Evitar el uso de zapatos con suelas plásticas ya que ellos pueden producir potencial estático. Las descargas de potencial estático en una computadora pueden causar el mal funcionamiento del sistema.
c) Restringir el acceso a el centro de computo a personal no autorizado.

4.2.3 ÁREAS QUE ESTÁN DENTRO DE LA SEGURIDAD FÍSICA Y AMBIENTAL.

4.2.3.1 UBICACIÓN Y CONSTRUCCIÓN DEL CENTRO DE COMPUTO

No es recomendable ubicar centros de cómputo dentro de atractivas paredes de vidrio ubicadas en avenidas principales con gran afluencia peatonal y vehfcular o con visitas frecuentes, principalmente para evitar terrorismo y sabotaje.

La selección del local deberá ser más conservadora, los centros de cómputo deberán ser colocados lejos de las áreas de tránsito tanto terrestres como aéreas.

La construcción del interior del centro de cómputo no debe ser de materiales catalogados como inflamables que despidan humos sumamente tóxicos, las divisiones entre los cubículos deben de ser a prueba de incendios, deben quedar perfectamente selladas, de preferencia que no despidan polvo (por ejemplo el tirol planchado).

En lo posible se deben tomar precauciones en cuanto a la orientación del centro de cómputo (centros sumamente calurosos a los que todo el día les esta dando el sol) se deben evitar en lo posible los grandes ventanales, evitando el vidrio en las áreas de recepción y en caso de que se utilice, debe estar reforzado a prueba de balas y de incendios.

Los centros de cómputo son de alto riesgo y susceptibles de sufrir ataques externos, por lo tanto deben estar aislados de las instalaciones, por lo general este requisito interfiere con la eficiencia del flujo de trabajo pero es indispensable en las instalaciones de alta seguridad.

Las dimensiones mínimas del centro de cómputo están determinadas por la cantidad de componentes del sistema, el espacio mínimo requerido por cada unidad para su mantenimiento, área de operación, paredes y paneles removibles pueden ser utilizados para facilitar ampliaciones futuras.

Además en el centro de cómputo se debe prever espacio para lo siguiente:

a) Almacenamiento de cintas.
b) Formatos y papel para impresora.
c) Mesas de trabajo y muebles.
d) Área y mobiliario para mantenimiento.
e) Equipo de telecomunicaciones.
f) Área de programación.
g) Consolas del operador.
h) Area de recepción.
i) Microcomputadoras.
j) Fuentes de poder.

Los archivos maestros y/o registros deberán ser guardados en una bóveda anti-incendio bajo máxima protección.

Piso elevado

Este tipo de pisos permiten organizar el tendido y protección del cableado del sistema, más la facilidad de reacomodar el sistema.
Los pisos elevados también proveen un excelente método para llevar el aire acondicionado cerca de las unidades del sistema, permitiendo la adición o recolocación de las rejillas de aire cuando son agregadas o recolocadas máquinas en la sala.

Un piso elevado debe ser capaz de soportar una carga uniforme de no menos de 1200 kilos por metro cuadrado.
La capacidad de soportar unidades adicionales debido al potencial de crecimiento futuro del sistema debe ser considerado.
La distancia entre la superficie del piso del edificio y el piso elevado debe tener 45 cm. cuando es usado como cámara plena de aire acondicionado, la altura del plafón, desde el piso falso terminado debe ser de 2.4 mts.
Los paneles del piso elevado deben poder ser removidos fácilmente para permitir la instalación del cableado del sistema.

Es recomendable que el acabado del piso del centro de cómputo sea hecho con plástico laminado antiestático.

También proporciona una superficie de fácil limpieza con un trapo húmedo o con aspiradora.

4.2.3.2 AIRE ACONDICIONADO

Los ductos de aire acondicionado deben estar limpios, ya que son una de las principales causas de polvo, este es indispensable en el centro de cómputo ya que las fluctuaciones de aire y los desperfectos ocasionan que las computadoras tengan que ser apagadas.

Las instalaciones del aire acondicionado son una fuente de incendio muy frecuente, así mismo son susceptibles de ataques físicos, especialmente a través de los ductos.

Se deben instalar redes de protección en todo el sistema de ductos exterior e interior, se habrá de contar con detectores de humo que indique la posible presencia de fuego, así como con extinguidores.

En la construcción del Centro de Cómputo es importante el aire acondicionado y consecuentemente la ambientación a ser mantenida en ese lugar, para mantener la humedad relativa del espacio dentro de las tolerancia especificadas.

Si se permite la infiltración de grandes volúmenes de aire frío (por debajo de 15 grados centígrados), o se introducen intencionalmente, el sistema de aire acondicionado debería tener los medios para agregar la humedad adicional al lugar. El comportamiento de un sistema de procesamiento de datos es afectado cuando la humedad llega a rebasar los límites requeridos por el equipo.

Se recomienda que la presión de aire en la Sala de Cómputo sea ligeramente superior que la de áreas adyacentes, para reducir así la entrada de polvo y suciedad.

4.2.3.3 INSTALACIÓN ELÉCTRICA Y SUMINISTRO DE ENERGÍA.

A continuación se describen dispositivos que reducen el riesgo de daño al equipo debido al sistema eléctrico.

Las variaciones de energía en una línea pueden ser causados por el encendido o apagado de máquinas eléctricas, tales como motores, ascensores, equipos de soldadura, sistemas de aire acondicionado, etc. Aún el flujo de corriente de un sistema de iluminación puede producir "Picos de ruido" que podrían exceder el nivel de energía aceptable para alguna unidad del sistema, por lo cual es altamente recomendado que la entrada de potencia del sistema éste completamente aislada de cualquier carga eléctrica. En zonas grandes cargas eléctricas industriales o condiciones de entrada de potencia marginales, pueden ser necesarias aislaciones adicionales para prevenir variaciones de energía en el sistema.

Sistema ininterrumpido de abastecimiento de corriente (UPS).

Estos dispositivos eléctricos reducen el riesgo de tener un accidente por los cambios de corriente. Dichos protectores son típicamente construidos dentro de un sistema de corriente ininterrumpido UPS(Uninterruptible power supply system).

Un sistema UPS consiste en un generador, ya sea de batería o de gas, que hace interfase entre la energía eléctrica y el dispositivo de entrada de energía eléctrica a la computadora. Lo que hace es dar una consistencia a la corriente eléctrica que hace funcionar a la computadora en caso de haber una falla en el abastecimiento de energía eléctrica. El UPS provee de energía eléctrica a la computadora por cierto período de tiempo; dependiendo de lo sofisticado que sea el UPS, la corriente eléctrica proveniente del UPS puede ser de días o de algunos minutos que permitan respaldar.

Switch de apagado en caso de emergencias.

Tal vez existe en algún momento la necesidad de apagar la computadora y sus dispositivos periféricos en caso de que el centro de cómputo donde se encuentre la computadora, se este incendiando o si hubiera evacuación. Dos switch de emergencia servirían para este propósito, uno dentro del cuarto de máquinas y el otro cerca, pero afuera del cuarto. Deben ser claramente identificados con un letrero, deben ser accesibles e inclusive a salvo de gente que no tiene autorización para utilizarlo. Los switch deben estar bien protegidos de una activación accidental.

Tener dos diferentes estaciones de abastecimiento de energía eléctrica.

El cableado de energía eléctrica que alimentan a nuestro centro de cómputo están expuestos al medio ambiente- agua, fuego y excavaciones. Para reducir el riesgo de falta de energía eléctrica lo que se debe hacer es abastecerse de energía eléctrica no sólo de una estación de electricidad sino de dos. Así si falla una por lo menos nos queda la otra estación de electricidad funcionando.

Los cables deben estar dentro de paneles y canales eléctricos.

Incendios por causas de la electricidad son siempre un riesgo. Para reducir el riesgo, los cables deben ser puestos en paneles y canales resistentes al fuego. Estos canales y paneles generalmente se encuentran en el piso del centro de cómputo.

Sistema de distribución eléctrica.

Se recomienda que el sistema sea conectado a una única fuente de poder. El alimentador principal y los conductores de tierra, deberán ser aislados. Circuitos ramificados para iluminación y sistemas de aire no deberán estar conectados a los tableros de potencia utilizados por el sistema.

Tableros de distribución eléctrica.

El proveedor debe dar un tablero de distribución, el que deberá contar con un interruptor general, voltímetro, amperímetro, frecuentímetro y un interruptor individual por cada una de las unidades que configuren en el sistema. El tablero debe ubicarse en un lugar accesible y cada interruptor debe estar debidamente rotulado para su fácil localización.

Requerimientos del servicio eléctrico.

El suministro eléctrico debe ser trifásico 220 voltios y 60 Hz. También debe proveerse una conexión de tierra.

Toma corrientes para servicio.

Deberán existir enchufes de corriente que estén localizados dentro de los 2.5 metros de cada máquina.

Un enchufe de corriente deberá servir a más de una máquina.

Barra de tierra.

Todos los conductores de tierra de las máquinas deben estar ligados fuertemente a una barra sólida de tierra, del mismo tipo que la barra de neutro. Estas barras deben estar localizadas en el tablero de conexiones eléctricas.

4.2.3.4 INUNDACIÓN, TUBERÍAS Y DRENAJES.

Los centros de cómputo no deben colocarse en sótano o en áreas de planta baja, sino de preferencia, en las partes altas de una estructura de varios pisos.
La mejor opción es no colocar el centro de cómputo en áreas donde el riesgo de inundación es evidente.
Algunas causas pueden ser la ruptura de cañerías o por el bloqueo del drenaje, por lo tanto la ubicación de las cañerías en un centro de cómputo es una decisión importante.
El daño causado por el drenaje es un riesgo, cuando el centro de cómputo se localiza en un sótano. Deben instalarse, si es el caso, detectores de agua o inundación, así como bombas de emergencia para resolver inundaciones inesperadas.

4.2.3.5 AUTORIZACIÓN DE ACCESOS, PROCEDIMIENTOS Y MONITOREO DE DISPOSITIVOS.

Es importante asegurar que los controles de acceso sean estrictos durante todo el día. En especial durante los descansos y cambios de turno.

El personal de mantenimiento y cualquier otro personal ajeno a la instalación se debe identificar antes de entrar a esta. El riesgo que proviene de este personal es tan grande como el de cualquier otro visitante.

Se debe limitar el acceso a los individuos no autorizados por la gerencia. esta autorización debe ser explícita, el personal autorizado debe tener una llave de acceso al centro.

En los centros de cómputo se pueden utilizar los siguientes recursos para controlar el acceso:

Puerta con cerradura.- Requiere de la llave tradicional de metal debe de ser difícil de duplicar esta llave.

Puerta de combinación.- Este sistema usa una combinación de números para permitir el acceso, la combinación debe ser cambiada regularmente o cuando el empleado sea transferido o termine su función laboral dentro de ese centro de computo. Esto reduce el riesgo de que la combinación sea conocida por gente no autorizada.

Puerta electrónica.- Este sistema usa una tarjeta de plástico magnética como llave de entrada. Un código especial interno en la tarjeta es leído por un sensor activando el seguro de la puerta. Este sistema tiene ventajas sobre las puertas de cerradura y las de combinación, debido a que;

a) A través del código interno, las tarjetas pueden ser asignadas como identificación individual.
b) A través del código interno y el sensor el acceso puede ser restringido a puertas particulares o bien a horas particulares del día.
c) Son difíciles de duplicar.
d) La tarjeta es fácil de desactivar en el caso de que el empleado sea

transferido a otro centro, o que la tarjeta sea robada o perdida.
e) Las alarmas pueden ser activadas automáticamente si se detecta una entrada ilegal.

Puertas sensoriales.- Son activadas por los propios individuos por alguna parte única de su cuerpo como puede ser la huella digital, la voz, los ojos o bien por la firma. Este sistema es usado principalmente en los centros militares.

Registros de entrada .- Todos los visitantes deben firmar el registro de visitantes indicando su nombre, su compañía, la razón para la visita, la persona que va a visitar.
El registro se encuentra en la recepción al entrar al centro de cómputo, el visitante debe además tener una identificación (licencia de manejo o credencial).
Se debe identificar y admitir tanto a los empleados como a los visitantes de uno en uno.

Identificaciones con foto.- Las identificaciones deben tener una foto para todo el personal del centro, las tarjetas de los visitantes deberán ser de un diferente color para la fácil identificación.

Video cámaras.- Estas deben ser localizadas en puntos estratégicos para que los guardias de seguridad puedan monitorear el centro, los cassettes deben ser retenidos para un posible análisis.

Guardias de seguridad.- Es usual que los guardias utilicen las cámaras y las puertas de seguridad, las guardias deben ser turnadas para proteger la organización de pérdidas.

Escolta controladora para el control del acceso de visitantes.- Todos los visitantes deben ser escoltados por un empleado responsable. Se dice que son visitantes los amigos, proveedores, ingenieros de mantenimiento y auditores externos.

Puertas dobles.- Se encuentran en las entradas de los cuartos importantes del centro de cómputo y consisten en dos puertas, para que la segunda puerta abra la primera debe estar cerrada.

Entrada única.- Debe ser monitoreada por un recepcionista, todo el personal debe entrar a través de ella, si existen muchas entradas crece el riesgo de que personas no autorizadas penetren.

4.2.3.6 ALARMAS.

Sistema de alarma: Un sistema de alarma debe tener puntos para activar, de tal manera que solamente se pueda entrar y salir por las puertas.

El personal de seguridad debe poder ofr la alarma cuando sea activada. Deben existir reportes de seguridad y documentos sobre la distribución de tarjetas.

Todas las áreas deben estar protegidas contra accesos ffsicos no autorizados. Las alarmas contra robo deben ser usadas hasta donde sea posible en forma discreta, de manera que no se atraiga la atención de que existe un dispositivo de alta seguridad. Tales medidas no sólo se deben aplicar en el centro de cómputo sino también en áreas adyacentes.

4.2.3.7 DETECCIÓN DE HUMO Y FUEGO, EXTINGUIDORES.

-Detectores de fuego y humo. Se deben colocar cuidadosamente evitando la relación con los aparatos de aire acondicionado, ya que estos pueden difundir el calor o el humo y no permitir que se active el detector.

-El detector de humo que se elija deberá ser capaz de detectar los distintos tipos de gases que desprendan los cuerpos en combustión. Algunos no detectan el humo o el vapor que proviene del plástico quemado que se usa como aislante en electricidad y en consecuencia los incendios ocasionados por un corto circuito tal vez no se detecten.

-Los detectores de humo y calor se deben instalar en el centro de cómputo, en las áreas de oficinas, incluyendo el depósito de papelería y en el perímetro físico de las instalaciones. Es necesario colocar detectores de humo y de calor bajo el piso y en los conductos de aire acondicionado.

-Las alarmas contra incendios deben estar conectadas con la alarma central del lugar, o bien directamente con el departamento de bomberos.

-Se debe serciorar la organización que los controles de seguridad contra incendios satisfaga los estándares mínimos del departamento de bomberos.

-La documentación de los sistemas, la programación, y las operaciones también necesitan protección contra incendios. La destrucción de esta documentación puede imposibilitar la utilización de archivos de respaldo. Se deben establecer procedimientos que garanticen la actualización de toda la documentación como rutina y que las copias de seguridad se almacenen en un lugar lejano, así como las copias de seguridad de los programas y los archivos.

Tipos de equipo contra incendio.

Debe existir un sistema de detección de humo por ionización para aviso anticipado, este sistema debe hacer sonar una alarma e indicar la situación del detector activado. El sistema de detección no debe interrumpir la corriente de energía eléctrica al equipo de cómputo. Se debe contar con un dispositivo manual de emergencia para cortar el sistema eléctrico y aire acondicionado y debe instalarse en cada salida del centro de cómputo.

Se deben colocar en lugares estratégicos del centro cómputo extintores portátiles de CO (recomendable para equipo eléctrico). El equipo respiratorio debe estar a la mano, tanto en el área de cómputo como para el uso de los bomberos en caso de incendio.

Por su parte, los detectores de ionización del aire se colocan en el techo y piso falso, repartidos de manera uniforme y estando todos conectados al tablero del equipo de control contra incendio. En este tablero se localiza un reloj que puede calibrarse de 0 a 60 segundos para provocar un disparo de gas halón a través de boquillas de aspersión estratégicamente colocadas en el techo de la sala, para permitir la evacuación del personal y desconectar el sistema, ya que el gas halón afecta la capa de ozono.

Es necesario definir y documentar los procedimientos que se deben seguir en caso de incendio. Además se debe entrenar al personal acerca de su uso, con frecuencia muchos empleados no saben exactamente que deben hacer en caso de incendio.

Las cintas y discos magnéticos deben almacenarse en una sala aparte, contando con un acceso al área donde se localiza el equipo de cómputo. Esta sala debe contar con todas las condiciones ambientales y de seguridad necesarias ya que la información almacenada ahí tiene más importancia que el propio equipo de cómputo. Las cintas y discos magnéticos deben almacenarse en armarios fabricados especialmente con paredes de por lo menos dos horas de resistencia al fuego.

Para asegurar que los sistemas de detección se encuentran en buenas condiciones, el cuerpo de bomberos debe inspeccionar el sistema y recargar los extintores anualmente. También se le debe notificar al cuerpo de bomberos la localización del centro de cómputo, para que en caso de incendio estén preparados con el equipo apropiado.

La participación de los bomberos tanto en el diseño como en la aplicación de los procedimientos para detectar, prevenir y extinguir incendios puede ser muy valiosa.

Planes de evacuación del centro plenamente probados y documentados.

Los planes de evacuación son importantes para la seguridad humana, sin embargo éste plan no debe descuidar la atención que se le debe al centro de procesamiento de la información.

4.2.3.8 TEMPERATURA Y HUMEDAD

Los equipos de procesamiento de datos, necesitan de un sistema de aire acondicionado diseñado para operación constante, en base a los siguientes parámetros:

-Disipación térmica (BTU)
La disipación térmica de cada unidad de sistemas es mostrado en Unidades Térmicas Británicas por hora.

-Movimiento de aire (CFM)
El Movimientos de Aire es mostrado en Pies Cúbicos por minuto.

-Iluminación
La Iluminación debe ser incluida en los cálculos de carga total de calor. Si la iluminación es seccionada, este cálculo debe ser hecho como si todas las luces estuvieran encendidos al mismo tiempo.

-Pérdidas por transferencia de calor
Existen pérdidas por transferencia de Calor, por lo siguiente:
-Pérdidas a través de paredes, piso y techo.
-Diferencias en temperatura entre la Sala de Cómputoy áreas adyacentes.
-Ventanas expuestas a los rayos del sol.

Los cambios de temperatura durante la operación del computador deben ser minimizados. La variación cíclica de temperatura sobre el rango completo de operación no debe realizarse en menos de 8 horas.

La temperatura ideal recomendada para el Centro de Cómputo es de 22 grados Centígrados y ésta debe ser usada como la base para el diseño del sistema de aire acondicionado.

La Humedad debe ser agregada o quitada al sistema de aire acondicionado, tanto como sea necesario. Generalmente, la humedad debe ser agregada ya que al enfriar el aire se remueve la mayorfa del vapor de agua por condensación.

Se recomienda que se instalen instrumentos registradores de temperatura y humedad. Dichos instrumentos son necesarios para proveer un continuo registro de las condiciones ambientales en el área del equipo.

CAPITULO III

PLAN DE CONTINGENCIAS

5. PLAN DE CONTINGENCIAS.

El plan de contingencias junto con el plan de seguridad sirven para proveer a la organización los requerimientos para la recuperación de desastres.

La metodología tiene como finalidad conducir un plan de recuperación en una contingencia que sufra la organización de la manera más efectiva.

5.1 DEFINICIÓN DE PLANES DE CONTINGENCIA. (DISASTER CONTINGENCIA PLANNING (D.C.P.))

El Plan de Contingencia es definido como:

LA IDENTIFICACIÓN Y PROTECCIÓN DE LOS PROCESOS CRÍTICOS DE LA ORGANIZACION Y LOS RECURSOS REQUERIDOS PARA MANTENER UN ACEPTABLE NIVEL DE TRANSACCIONES, PROTEGIENDO ESTOS RECURSOS Y PREPARANDO PROCEDIMIENTOS PARA ASEGURAR LA SOBREVIVENCIA DE LA ORGANIZACION EN TIEMPOS DE DESASTRE.

Un Plan de Contingencias es un Plan en donde intervienen los niveles ejecutivos de la Organización y el personal usuario y técnico de los procesos.

El Plan de Contingencias se basa en entender a la Organización, los objetivos que soporta, las operaciones que realiza, evalúa la perdida de cada proceso, dando a conocer que se haría en una situación critica, y preguntando que se puede hacer cuando se presente.

Un desastre puede afectar el ambiente normal de la Organización. Algunas organizaciones pueden ser afectadas en menor o mayor grado, lo cual puede traer substanciales perdidas a la organización.

El estar preparados para una recuperación en caso de desastre y continuar con las operaciones normales de la organización, debe estar contemplado en un Plan de Contingencias.

Las organizaciones han ido implantando la tecnología necesaria para irse adaptando a su medio ambiente. Es importante la dependencia que tienen las organizaciones de la tecnología.

Las Organizaciones deben de identificar sus procesos críticos.
El tiempo y los recursos para desarrollar, probar y dar mantenimiento al Plan de Contingencias deben ser provistos por los niveles ejecutivos de la Organización.

En la Organización el proyecto del Plan debe tener una alta prioridad.
El Plan de Contingencias anteriormente sólo tomaba en cuenta los procesos basados en la Computadora. Sin embargo se debe tomar en cuenta todo aquello que asegure la continuidad de la organización, incluyendo registros manuales y documentación fuente.

Si la Organización se encuentra en una área que esta propensa a terremotos y temblores, el Plan de Contingencias debería tener procedimientos para ocupar otros servicios en un Centro de Cómputo alternativo.

La Organización debe describir los limites del Plan, para facilitar la creación del mismo. Los miembros de la Organización deben participar en determinar los alcances y limitaciones del Plan.

Objetivos del Plan de Contingencia

- *Minimizar el impacto del Desastre en la Organización.*
- *Establecer tareas para evaluar los Procesos de la organización indispensables.*
- *Evaluar los Procesos de la organización, con el apoyo y autorización respectiva a través de una buena metodología.*
- *Determinar el costo del plan de recuperación, incluyendo capacitación y organización para restablecer los procesos críticos de la organización cuando ocurra una interrupción de Operaciones.*

Un efectivo Plan de Recuperación es relativamente económico en comparación con un Seguro.

Necesidad de contar con Planes de Contingencias

Las empresas rehúsan trabajar con un Plan de Contingencias, piensan que es poco probable que les suceda un desastre, robo, o perdida de la información, las organizaciones piensan que sus sistemas son complejos y que nadie fuera de la organización los va a entender y a utilizar.

Las empresas tienen que tomar conciencia de la importancia del Plan de Contingencias. Un centro de cómputo debe protegerse de algunos desastres naturales como pueden ser :

- *temblores*
- *inundaciones*
- *huracanes*
- *incendios*

Los riesgos de no contar con un Plan de Contingencia son los siguientes:

- *Interrupción de las operaciones, resultado de no poder atender a los clientes, perdida de oportunidades e inhabilitación para competir.*

- *Perdidas Financieras.*
  Pago tardío de las Deudas.
  Retrasos en los Estados Financieros
  No aprovechar las Ofertas.

- *Salir del mercado.*

5.2 METODOLOGIA DEL PLAN DE CONTINGENCIAS.

La Metodología del Plan de Contingencias determina los procesos críticos de la organización para restablecer sus operaciones y debe de tomar en cuenta ser eficaz y eficiente, los aspectos legales, el impacto de servicio al cliente y los riesgos para que sobreviva la Organización.

Los procesos críticos de la Organización deben de estar definidos e identificados, así como los Recursos necesarios para la continuidad de los procesos. Los recursos incluyen al personal, equipo, transportación, oficina, espacio industrial, formas, datos y registros vitales.

Es necesario identificar los procesos críticos, y los recursos necesarios para minimizar el Impacto de Desastre.

Generalmente existen algunas precauciones y procedimientos en las organizaciones, que pueden hacer mínimos los costos previniendo un desastre.

Las experiencias han mostrado que las organizaciones necesitan comprender la importancia de su información.

Las compañías que tienen información crítica resultado de procesos automatizados, deben enviar regularmente copias de respaldo de sus archivos a un Centro Alternativo.

Se debe considerar el impacto que causaría un desastre en un Centro de Computo.

Como parte de la preparación de un Plan de Contingencias en las Organizaciones debe existir seguridad física, lógica y ambiental para reducir desastres, las cuales fueron explicadas en el capítulo anterior.

El siguiente paso es identificar y documentar procesos alternativos para procesos identificados como críticos para la organización. Si existen otros procedimientos dentro de la Organización que tengan recursos similares aprovechables, estos podrían ser considerados como posibles procedimientos alternos.

La Organización debe tener números telefónicos de Emergencia y teléfonos particulares de su personal. Estos teléfonos deberán estar almacenados en un lugar seguro y accesible.

En la preparación de un Plan Contingencias, las utilerías de software pueden ser usadas para respaldar Procesos Críticos

Es importante que en la prueba del Plan exista disciplina en la ejecución. La disciplina es importante no solo para facilitar la Recuperación, sino para prever la detección de problemas (en el momento del desastre), para minimizar la pérdida de vidas y costos.

Es importante que el Plan de Contingencias sea mantenido y modificado regularmente para que refleje los cambios en la Organización.

La Estructura de la Metodología a desarrollar será la siguiente:

Consiste en dos documentos separados:

1. La Base del Plan.
2. Las utilerías de software y manual de procedimientos para la recuperación.

La duración y la complementación del Plan de Contingencias contempla lo siguiente:

a) La naturaleza, la extensión y la complejidad de las actividades de la Organización.
b) El grado de riesgo al que la Organización esta expuesta.
c) El tamaño de las Instalaciones de la Organización (Centros de cómputo y número de usuarios).
d) El esfuerzo que la Organización esta preparada para contribuir en el desarrollo del Plan.

La Base del Plan de Contingencias maneja el nivel de tareas para el desarrollo del Plan, describe que se necesita para que sea realizado y cómo las tareas deben ser complementadas en un modelo de un Plan de Trabajo. Debe contener una jerarquía común de unidades de trabajo.

Etapas en el Proyecto del Plan de Contingencias:

- *Análisis del Impacto en la Organización,*
- *Selección de la Estrategia,*
- *Preparación del Plan, Prueba y Mantenimiento.*

FASES:

En cada etapa existe un número de fases relativas que necesitan ser realizadas, al final de cada fase es preparada una liberación. La Fase de liberación es la documentación del trabajo complementado en cada etapa.

TAREAS:

En cada fase existe un número de tareas que tienen que ser efectuadas. Las tareas describen que se necesita hacer para complementar el trabajo de una Fase, típicamente una tarea es concluida por la realización de pasos intermedios, la Combinación del Producto de las tareas hace posible la liberación de las Fases.

PASOS:

Es el nivel mas bajo de la jerarquía por cada tarea son definidos una serie de pasos, los pasos sirven para ejecutar las tareas.

PUNTOS DE APROBACION FORMAL:

Al final de cada etapa los puntos de aprobación formal son dados por lo siguiente:

a) *Obtener aprobación formal, que el trabajo especificado haya sido completamente terminado.*
b) *Verificar que el proyecto tenga seguimiento con la siguiente etapa.*
c) *Preparación y aprobación del Plan detallado para el siguiente grupo de fases que serán realizadas.*

Las Etapas de la Metodología del Plan de Contingencias son las siguientes:

Etapa 1. Análisis del Impacto de la Organización.

El proyecto comienza con el Análisis del Impacto en la Organización durante este se identifican sus procesos críticos.

En esta etapa se pretende identificar pérdidas financieras y efectos operacionales por la perdida total ó parcial de actividades esenciales.

Etapa 2. Selección de la Estrategia.

Cada uno de los riesgos y su probabilidad de ocurrencia deben ser identificados.

Las Medidas de Prevención de desastre deben estar respaldadas en un lugar seguro. Se debe de considerar y evaluar rangos de estrategias de recuperación posibles. Al final de la etapa de Selección de la Estrategia de Recuperación, una debe ser elegida.

Etapas en el Proyecto del Plan de Contingencias:

- Análisis del Impacto en la Organización,
- Selección de la Estrategia,
- Preparación del Plan, Prueba y Mantenimiento.

FASES:

En cada etapa existe un número de fases relativas que necesitan ser realizadas, al final de cada fase es preparada una liberación. La Fase de liberación es la documentación del trabajo complementado en cada etapa.

TAREAS:

En cada fase existe un número de tareas que tienen que ser efectuadas. Las tareas describen que se necesita hacer para complementar el trabajo de una Fase, tfpicamente una tarea es concluida por la realización de pasos intermedios, la Combinación del Producto de las tareas hace posible la liberación de las Fases.

PASOS:

Es el nivel mas bajo de la jerarquía por cada tarea son definidos una serie de pasos, los pasos sirven para ejecutar las tareas.

PUNTOS DE APROBACION FORMAL:

Al final de cada etapa los puntos de aprobación formal son dados por lo siguiente:

a) Obtener aprobación formal, que el trabajo especificado haya sido completamente terminado.
b) Verificar que el proyecto tenga seguimiento con la siguiente etapa.
c) Preparación y aprobación del Plan detallado para el siguiente grupo de fases que serán realizadas.

Las Etapas de la Metodología del Plan de Contingencias son las siguientes:

Etapa 1. Análisis del Impacto de la Organización.

El proyecto comienza con el Análisis del Impacto en la Organización durante este se identifican sus procesos crfticos.

En esta etapa se pretende identificar pérdidas financieras y efectos operacionales por la perdida total ó parcial de actividades esenciales.

Etapa 2. Selección de la Estrategia.

Cada uno de los riesgos y su probabilidad de ocurrencia deben ser identificados.

Las Medidas de Prevención de desastre deben estar respaldadas en un lugar seguro. Se debe de considerar y evaluar rangos de estrategias de recuperación posibles. Al final de la etapa de Selección de la Estrategia de Recuperación, una debe ser elegida.

Etapa 3. Preparación del Plan , Prueba y Mantenimiento.

El Plan de la Recuperación de la Organización es proyectado y probado. La preparación del Plan de Recuperación requiere de la participación del personal de la Organización para asegurar que ellos sean miembros en el Plan y que estén disponibles cuando este suceda.

Al final de esta etapa, el Plan de Recuperación entra en una Fase de Prueba, asegurando que se trabaje en forma eficiente.

El Plan de Contingencias debe ser elaborado asegurándose de que este siempre sea mantenido y revisado regularmente o modificado adaptando los procedimientos.

Deberá existir un Coordinador de la Recuperación, y este debe ser encargado de las pruebas.

Después de la Creación Inicial, el Plan debe ser formalmente revisado, después de un Período de varios meses se deben de asegurar que los procedimientos de Recuperación hayan sido mantenidos y probados apropiadamente.

Documentación del Plan de Contingencias:

Toda la documentación asociada con el Plan de Contingencias y del Control de Procedimientos, juega un importante Rol dentro de la Organización.

Todos los participantes trabajan en interpretar los requerimientos.

Los documentos sólo son usados después de ser aprobados.

CONTROL DE DOCUMENTOS:

La documentación producida durante el Proyecto del Plan de Contingencias, Cae en dos categorías:

1. Los documentos que forman parte de la liberación final y deben ser mantenidos durante la vida del Plan.

2. Los documentos intermedios que son producidos en una parte del Desarrollo del Plan, los cuales no deberán ser mantenidos.

Ambas categorías son importantes. Los primeros dan las bases para el mantenimiento del Plan y los intermedios asisten para la revisión de los procesos y proveen evidencias de la calidad del sistema.

ARCHIVAR EL DOCUMENTO:

Después de que el Plan de Contingencias sea desarrollado algunos de los documentos deberán ser archivados.

A cada director se le dará una copia, la cual deberá tener la versión, la fecha y el lugar donde deberá estar el documento.

Algunas copias deberán ser almacenadas donde estén protegidas de desastres, deterioro o pérdida.

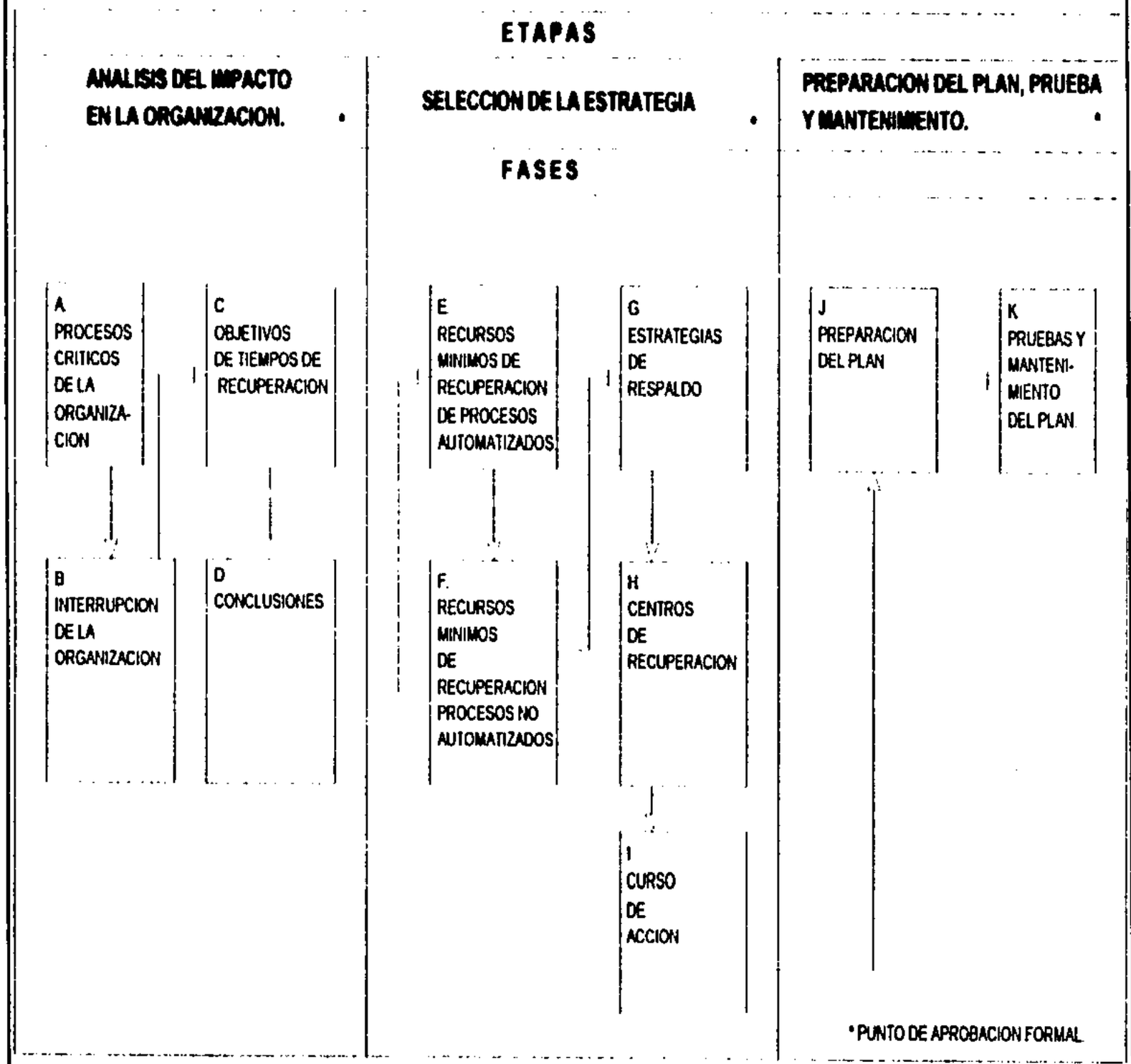
IDENTIFICACIÓN DEL DOCUMENTO:

1. Titulo del Documento.
2. Identificación o número de Referencia.
3. Número de la versión y fecha.
4. Autor.

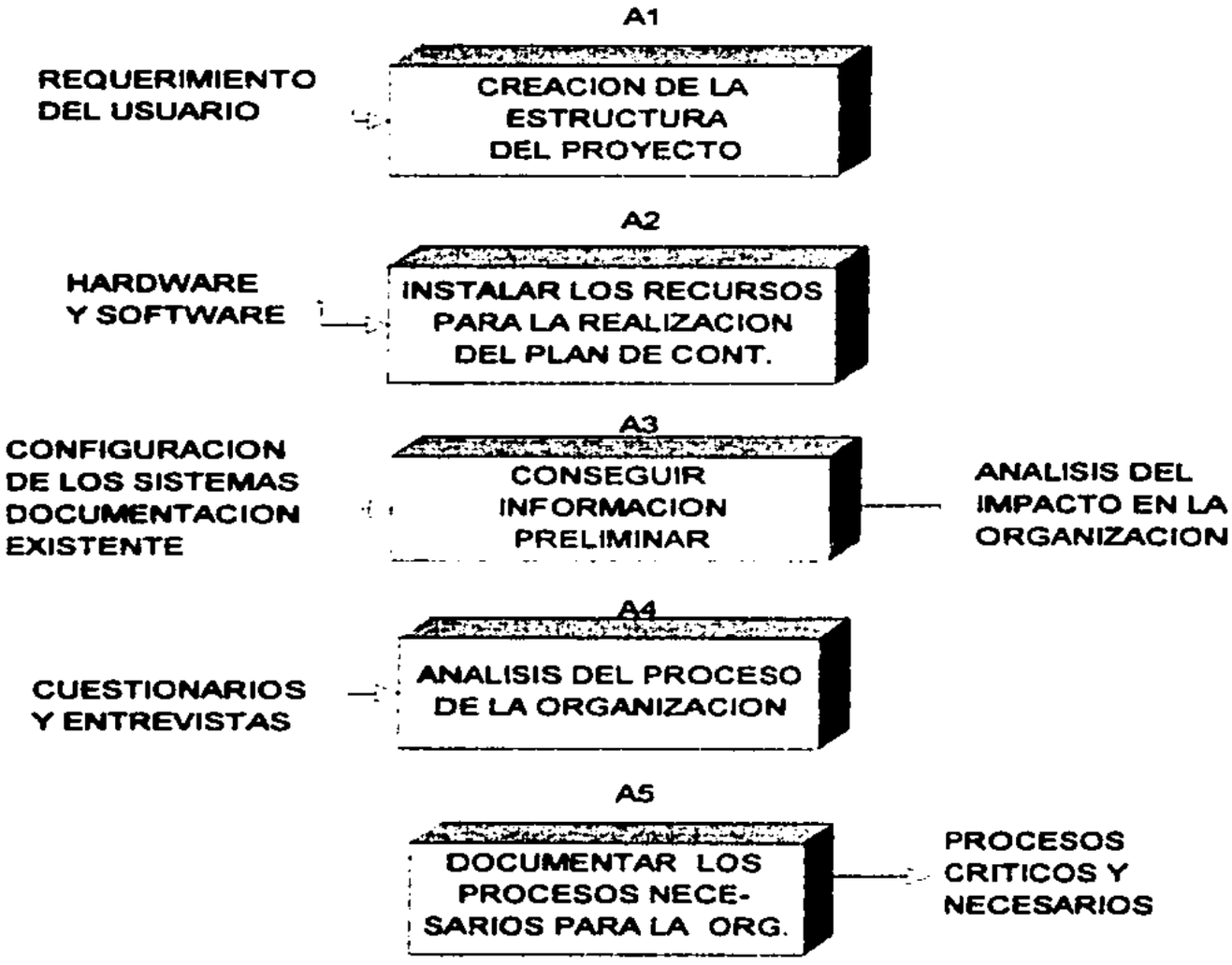
Número de la Versión. La vida del Documento tendrá varios cambios. Los lineamientos a seguir para controlar las versiones son:

- Historia,
- Número de páginas,
- Aprobación del Documento,
- Control de Cambios y
- Distribución del Documento.

CIRCULO DE VIDA DEL PLAN DE CONTINGENCIAS



FASE A. PROCESOS CRITICOS DE LA ORGANIZACION
RELACION DE TAREAS.



5.3 ANÁLISIS DEL IMPACTO EN LA ORGANIZACIÓN.

Es la etapa para identificar cada proceso de la Organización, determinar los procesos que son crfticos para su continuidad y definir los procesos que deberán estar incluidos en el Plan de Contingencias. Es el paso vital en la Implementación del Plan de Contingencias.

Existen diferentes Métodos para determinar los procesos crfticos de una Organización:

a) Todos los procesos son crfticos:
Con este Método, la decisión es tomada por todos los departamentos y se parte de que todas las funciones de cada departamento son criticas, comúnmente 1 o 2 departamentos son eliminados, pero en general todo es clasificado como crftico.
Si este Método es el elegido, se deben listar todas las Funciones de cada departamento. Este método no es recomendable porque para el Plan de Contingencias se llevarfa mucho tiempo. Serfa costoso y llevarfa tiempo respaldar todas las Funciones en todos los Departamentos.

b) Mandatos de los Gerentes:
Este Método asume que los gerentes conocen lo qué es critico, para mantener un aceptable nivel en la Organización. La identificación de Funciones Crfticas, es hecha en base de la Intuición de los Gerentes. El beneficio de este Método es el tiempo que es ahorrado durante la fase inicial. Lo peligroso es que el Método es basado en una intuición y no es un riguroso análisis.

c) Análisis de Riesgos:
Consiste en la Determinación de Pérdidas Financieras, por cada Función y Proceso de la Organización. Esto se obtiene por la determinación de la probabilidad de un desastre y la pérdida anual. Esto es comparado con el Nivel de Pérdida Financiera aceptable para la Organización. Son Crfticos aquellos procesos de los que se esperan grandes pérdidas.
Sin embargo no se puede determinar exactamente el Riesgo.

d) Análisis del Impacto en la Organización.
La Metodologfa del Plan de Contingencias se basa en la Técnica de Análisis de Impacto en la Organización.
Son distribuidos cuestionarios para todos los departamentos de la Organización. Los cuestionarios completos y la información obtenida durante las entrevistas predefinen criterios para determinar los procesos Crfticos. Este Método tal vez tome mas tiempo inicialmente que el Método de "todos los procesos son crfticos". Sin embargo disminuye consideradamente tiempo y dinero cuando es desarrollado el Plan de Recuperación.

OBJETIVOS:

- Identificar los procesos crfticos y necesarios de la organización, las dependencias crfticas de los sistemas.
- Los procesos con probabilidad de ser destruidos, tomando en cuenta perfodos de pérdida especfficos de tiempo(3 horas, un día o una semana).
- Determinar recursos alternativos de información y servicio.
- Determinar el costo financiero de un desastre y el probable tiempo de recuperación.
- Identificar amenazas especfficas de cada proceso crftico, (instalación de luz, localización geográfica, etc.)
- Los sistemas que ponen en riesgo la continuidad de las operaciones de la organización.

INSERTAR HOJA

5.3.1 PROCESOS CRÍTICOS DE LA ORGANIZACIÓN.

En esta fase, la primera tarea es crear la estructura necesaria para la ejecución del proyecto del Plan de Contingencias. Consiste en la identificación de los procesos críticos de la organización, para que sobreviva y continúen sus operaciones.

Después de que la información este reunida con entrevistas y cuestionarios será analizada para determinar cada proceso crítico. La clasificación de los procesos será el resultado del análisis, discutido con la Gerencia o Dirección, para asegurar que todos los procesos apropiados sean incluidos en el Plan de Contingencias. Los procesos que son identificados como críticos en esta fase serán considerados en el Plan de Contingencias.

Esta Fase consiste en lo siguiente:

ENTRADAS: Requerimientos del usuario para el Plan de Contingencias.
Hardware
Software
Configuración de los Sistemas Implementados.
Procesos existentes
Documentación existente para la recuperación.

TAREAS: Creación de la Estructura del Proyecto.
Instalación de recursos para el desarrollo del plan.
Conseguir información preliminar
Realizar el análisis del proceso de la Organización.
Documentar los procesos críticos de la Organización.

PRODUCTOS: Cuestionarios de análisis del negocio.
Cuestionarios de funciones críticas.
Resultados de las entrevistas.

FASE DE LIBERACION: Liberación de procesos críticos y necesarios para la organización.

FORMAS: Cuestionario de análisis del negocio.
Cuestionario de funciones críticas.

5.3.1.1 CREACIÓN DE LA ESTRUCTURA DEL PROYECTO.

Establecer la estructura del Plan maestro, así como el equipo para la consecución de un Plan de Contingencias.

- Los objetivos y su ámbito de acción.
- Determinación del comité oficial del proyecto.
- Seleccionar al coordinador para la recuperación.
- Seleccionar a los miembros del proyecto.
- Establecer las tareas del comité
- Seleccionar las utilerías del proyecto.
- Establecer la estructura del proyecto y su duración.

LOS OBJETIVOS DEL PROYECTO Y SU ÁMBITO DE ACCIÓN.

Confirmar los objetivos del proyecto a través de discusiones entre los miembros o representantes de la organización.

Confirmar el ámbito de acción, debe quedar claro y todos de acuerdo, que extensión debe tener, deberá ser decidido por el director basado en estadísticas de desastres regionales ocurridos, los costos percibidos, incluir el impacto de los desastres regionales.

Se debe acordar el uso de un software específico para el mantenimiento del Plan. Al discutir los beneficios de un software para la implementación del Plan se debe de tomar en cuenta:

a) Documentación entre ligas, procesos y datos, incluyendo la integridad de los datos entre los sistemas.
b) Documentación de archivos.
c) Documentación de localización de respaldos, y generación de respaldos.

DETERMINACION DEL COMITE OFICIAL DEL PROYECTO.

La organización deberá estar involucrada en la determinación del comité oficial del proyecto y la dirección debe estar preparada para dar los recursos apropiados y prioridad para desarrollar el proyecto, probarlo y mantenerlo.

El equipo del proyecto no puede hacer el trabajo por si solo, la organización tiene que implantar un Plan.

Debe estar involucrado el personal suficiente en el desarrollo del proyecto, este debe tener una alta prioridad y asegurar que sea completado en un tiempo razonable.

Para ayudar en la Planeación y Preparación del Plan e involucrar a la organización en el proyecto, la Dirección debe proveer una carta o comunicado para informar del proyecto a los miembros de la organización, comunicando que el proyecto es prioritario.

Cada persona involucrada en el Plan de Contingencias, no debe dejar incompletas sus tareas ordinarias, porque el tiempo que invierte en el Plan no ha sido especificado en sus calendarios diarios de actividades.

Se busca aumentar la conciencia de la seguridad en el empleado y sus responsabilidades.

a) Que los empleados estén conscientes de mantener sus passwords (identificaciones de entrada) secretos.
b) Que reporten violaciones al Administrador de la seguridad.
c) Que lean las políticas de seguridad.
d) Mantener la seguridad Física, manteniendo las puertas cerradas, controlar y guardar las llaves de acceso al Centro de Cómputo.
e) El reforzamiento puede darse por medio de boletines.

ESTABLECER LA DIRECCIÓN DEL PROYECTO

Si el proyecto es dirigido o guiado por un Comité de Dirección asistir a este en el establecimiento del comité y asegurarse que sea representativo de todas las áreas del negocio.

SELECCIONAR AL COORDINADOR PARA LA RECUPERACIÓN.

En conjunto con el comité o con el Gerente si no se estableció el comité, nombrar un miembro para la posición de coordinador de recuperación de la organización. El Coordinador debe ser responsable por el proyecto para crear el Plan Inicial de Contingencia e idealmente, debe ser el líder del equipo responsable de la recuperación del desastre.

Una vez que el Plan de Contingencias es completado, el Coordinador de la Recuperación de la Organización debe familiarizarse con las operaciones diarias de la Organización, tener suficiente autoridad para obtener la cooperación de todos los niveles de la Organización y poseer cualidades para llevar a cabo la fase de recuperación del desastre.

Si el cordinador no es miembro de la dirección, todo el personal debe estar enterado de las responsabilidades y posición del coordinador de Recuperación de la Organización.

El Coordinador de la Recuperación de la Organización tiene las siguientes tareas:

- Enterar a la Organización del Plan de desarrollo del proyecto de Recuperación.
- Ser responsable del seguimiento de las modificaciones, pruebas y mantenimiento del Plan de Recuperación.
- Debe ser la persona responsable de las declaraciones en los eventos de desastre.
- Coordinar a los equipos de Recuperación y tareas en los eventos de desastre.

El coordinador de Recuperación de la Organización es un individuo que comenzará totalmente a familiarizarse con los proyectos del Plan de Contingencias. Esta persona debe ser parte importante del equipo del proyecto, debe estar involucrada en todos los pasos y tareas durante el proyecto.

SELECCIONAR A LOS MIEMBROS DEL PROYECTO.

Cuidadosamente se deben definir los recursos requeridos, tomando en cuenta la disciplina y el número de integrantes del equipo del proyecto, asegurándose que sean elegidos los requerimientos que vayan acorde con las necesidades del proyecto.

Definir a los miembros del proyecto, si es necesario elaborar un organigrama con los niveles de responsabilidad, deliberar sobre la asignación de tareas del proyecto para personal específico y publicar la lista de asignaciones de trabajo.

SELECCIONAR LAS UTILERÍAS PARA EL PROYECTO.

Seleccionar utilerías y técnicas para desarrollar el proyecto monitoreando y controlándolo. En particular considerar el uso de utilerías de software y seleccionar las más apropiadas si es que en la Organización aún no tuvieran un estándar.

Para iniciar el proyecto se deben de tomar en cuenta las siguientes tareas:

a) Establecimiento de responsabilidades.
En cuanto a si un software va a ser usado, establecer las responsabilidades de su adquisición, instalación y mantenimiento, así como de la entrada de datos.

b) Establecer los estándares para la documentación. procedimientos de control de documentos que serán usados durante el proyecto. Establecer estándares de numeraciones, referencias y control de versiones. Si la Organización tiene estándares para la generación de documentos, asegurarse que el proyecto cumpla con estos estándares.

c) Seleccionar software para administrar el proyecto.
Este software debe ser usado durante procesos administrativos, durante

el proyecto, incluye procesadores, gráficos, hojas de cálculo. si la Organización cuenta con estándares adoptar los apropiados.

d) Establecer la calidad del Plan.
Definir y establecer el control y revisión de los procesos.

ESTABLECER LA ESTRUCTURA DEL PROYECTO Y SU DURACION.
Preparar un proyecto inicial del Plan en el cual incluya el personal y recursos requeridos para el proyecto. Presentar los productos del trabajo jerárquicamente, fases, tareas, pasos.

Establecer personal representativo de la organización con responsabilidad para acordar todos los dictámenes y puntos formalmente aprobados e incluir sus nombres en el proyecto del plan.

PLANEACION DEL PROYECTO
El calendario del proyecto y las tareas a considerar son las siguientes:
- Resoluciones tomadas
- Recursos Disponibles
- Presupuesto del Proyecto
- Calendario

Preparar los recursos y presentarlos en un calendario, en una gráfica de gantt o en una hoja de actividades.

Balancear los recursos en el calendario, verificar que cada fecha de terminación es aceptable y que los recursos requeridos están dentro de la capacidad del personal.

Revisar los requerimientos del personal del proyecto basados en los recursos presentados en el calendario.

SOMETER EL PROYECTO DEL PLAN PARA SU APROBACIÓN.
Someter el plan del proyecto al comité y a la gerencia, discutiendo su contenido.
Resolver algunas preguntas y si es necesario modificar el plan. En esta etapa talvez se requieran varias reuniones.
Obtener la aprobación y autorización del procedimiento.

5.3.1.2. INSTALACIÓN DE RECURSOS PARA EL DESARROLLO DEL PLAN.

Seleccionar e instalar Hardware y Software para preparar y mantener el Plan de Contingencias.

SELECCIONAR EL SOFTWARE APROPIADO.
Puede ser utilizado algun software especffico para el desarrollo del Plan de Contingencias o bien un software de propósitos generales que contenga un procesador de textos.

ADQUISICIÓN DE HARDWARE.
Determinar los requerimientos, adquirir el equipo de cómputo adecuado con capacidad necesaria o si se tiene equipo para ser usado asegurarse de la capacidad. Determinar cual será el lugar de instalación del Plan de Contingencias, en organizaciones medianas y grandes.

INSTALACIÓN DEL SOFTWARE
Instalar el software seleccionado en computadoras y preparar las bases de datos para su uso y en caso necesario con aplicaciones desarrolladas con este propósito.

DECIDIR LAS POLÍTICAS PARA EL USO DEL SOFTWARE.

Previamente deben ser determinadas las políticas y estándares para el uso de software. Tomando en cuenta la compatibilidad del software elegido con todas las áreas de la organización.

DETERMINAR LAS MEDIDAS DE SEGURIDAD.

Es importante tomar medidas de seguridad para la utilización del software seleccionado, ya que la información utilizada para el desarrollo del plan es confidencial y de suma importancia para la organización.

El responsable del plan será el encargado de específicar las políticas de seguridad en cuanto a: manejo de passwords y respaldos de seguridad.

Así mismo deberá determinar la información que deberá contener la bitácora y el tiempo de su vigencia para ser desechado.

5.3.1.3. CONSEGUIR INFORMACIÓN PRELIMINAR

Crear una muestra de cuestionarios y conducir las entrevistas preliminares para identificar procesos críticos para la continuidad de las operaciones fundamentales de la organización.

Está tarea comienza con el diseño, creación y prueba de los cuestionarios:

- Los cuestionarios en el análisis del impacto de la organización son usados para dirigir las entrevistas.

- Los cuestionarios deberan servir para analizar a detalle las funciones de la organización.

- Un beneficio adicional de analizar los procesos críticos de la organización es conocer la documentación e integración de la información, que usualmente está en propiedad de diversos individuos, esto ayuda a la mejor toma de decisiones.

OBTENER ENTREVISTAS PARA DETERMINAR PROCESOS CRITICOS DE LA ORGANIZACION CON LOS JEFES DE DEPARTAMENTO

Deben ser conseguidas las entrevistas con los jefes de departamento para obtener una revisión inicial de la organización y confirmar la naturaleza y sus procesos.

Estas entrevistas deben incluir lo siguiente:

1. Antecedentes de la organización, tales como la naturaleza, líneas de productos, transacciones anuales (Compras y Ventas), mercado y competidores.

2. Áreas de la organización y jefes de departamento.

3. Información estratégica y decisiones de operación.

4. Seguridad en el Centro de Cómputo y en las áreas más importantes de la organización.

5. Algunos riesgos específicos que pongan en peligro los procesos críticos de la organización.

6. Conocimiento de los requerimientos legales (Multas, estándares de la industria, requerimientos de auditoría en relación con el plan de contingencias).

7. Algún plan de contingencias previamente emprendido.

Los directivos deben conocer la información general para el mantenimiento de la organización, pero talvés no tengan el conocimiento específico de la información.

El área de procesamiento de datos identifica las fuentes de información, el coordinador del plan de contingencias debe ser capaz de dar respuesta a las consultas del personal directivo de la organización.

Es importante identificar las características de la organización que hacen posible el éxito de la misma.

La información obtenida deberá ser protegida y deberá incluir lo siguiente:

1. Características de producción y servicio.
2. Características del cliente.
3. Filosofía del mercado.
4. Naturaleza de precios en el mercado, crédito y términos de contrato, planes de garantía.
5. Manufacturación, producción o servicios
6. Distribución y prácticas de almacenamiento.
7. Naturaleza de compra de materiales y servicios, establecimiento de su costo.
8. Características de los proveedores.
9. Intensidad de trabajo y características de localización de la fuerza de trabajo.
10. Existencia de planes especiales de compensación incluyendo incentivos gubernamentales.
11. Naturaleza de planes de beneficio empleadas, incluyendo percepciones, seguros y retiros.
12. Proyectos de desarrollo.
13. Naturaleza y extensión de actividades de desarrollo de investigación.
14. Impuestos.

RECOLECCIÓN DE DATOS EXISTENTES

Mucha de la información requerida para el proyecto del Plan de Contingencias puede existir en varias formas en la Organización.

Se deberá obtener la Documentación existente que contenga los antecedentes de la Organización. Estos deben incluir:

1. Organigramas
2. Descripción de procesos operativos.
3. Medidas de Seguridad existentes contra desastre.
4. Seguros.
5. Procedimientos de Desastre existentes.

El Coordinador del Plan de Contingencias debe ser responsable para asignar tareas de Recolección de datos a ciertos individuos.
Los Departamentos deben tener implantada su propia estrategia de respaldo.

Se debe de asegurar que el personal asignado a la tarea de recolección de datos este instruido.

DEFINICIÓN DE LA LISTA DE ENTREVISTAS PARA LA RECOLECCIÓN DE INFORMACIÓN.

Las entrevistas deben ser derivadas de la estructura de la organización, previa discusión con el Consejo Administrativo, deberán ser guiadas por el Coordinador del Plan de Contingencias.

El Plan de Entrevistas debe ser preparado, discutido y puesto en marcha. El personal que debe ser entrevistado es el siguiente:

1. El Jefe de Procesamiento de Datos.
2. Supervisores de Procesamientos de Datos.
3. Jefes de los Departamentos.

4. Personal de Seguridad.
5. Agentes de Seguros.
6. Auditores Internos o Externos.
7. Consejero Legal.
8. Representante de Personal Médico.

El personal de Procesamientos de Datos frecuentemente no esta enterado de la importancia funcional de los sistemas que soporta. Es más apropiado en las aplicaciones crfticas automatizadas consultar a los usuarios o a los jefes de departamento. De cualquier manera el Departamento de Procesamiento de Datos conoce el procedimiento a detalle de estas aplicaciones.

Estas entrevistas y cuestionarios probablemente requieren de información confidencial, como son direcciones de empleados, detalles de medidas de seguridad implantadas y documentación de procedimientos que están operando. El comité del Plan de Contingencias requiere de cooperación del personal de la organización el cual deberá estar enterado a través de un memorándum que contenga:

a)Propósitos del Proyecto.
b)Prioridades del Proyecto.
c)Comité encargado del Proyecto.
d)Breve explicación de como será utilizada la información.

PREPARAR LOS CUESTIONARIOS DEL ANÁLISIS DEL IMPACTO EN LA ORGANIZACION.

Las Entrevistas y Cuestionarios del Análisis del Impacto de la Organización deberán estar basadas en las discusiones con los Jefes de departamento.

Estos cuestionarios no deben intentar hacer preguntas específicas, sino de las áreas en general. Las entrevistas deberán de ser consistentes.

Deberán ser incluidas otras áreas no automatizadas que pueden tener información crftica y recursos ffsicos(maquinarfa) para la continuidad de la organización.

Ejemplo de un cuestionario para guiar la entrevista sobre el análisis del Impacto en la Organización.

Considerar las siguientes preguntas:

1. ¿Cuáles áreas del negocio son de mayor responsabilidad?

De estas identifica los componentes que en tu opinión son:

¿Lo esencial para que la organización sobreviva?
¿Lo esencial para mantener las funciones más importantes de la organización?
¿Funciones no crfticas para la organización y que pueden ser suspendidas temporalemente en un evento de emergencia.

2. ¿Cuáles son las consecuencias financieras de la pérdida de un componente clave de la organización?

Provee la información básica de cada componente de tu responsabilidad. Esto puede ser en forma de diagrama de flujo que deberá identificar entradas y salidas en las áreas de la organización. Esto debe incluir funciones sistematizadas, funciones manuales y sus interdependencias.

3. ¿Con qué información y facilidades cuentas en cada área de la organización?

Identificar todos los recursos internos y externos de datos,aplicaciones por computadora y las facilidades con las que tu cuentas, incluyendo personal clave y comunicaciones.

PREPARACIÓN DE CUESTIONARIOS DE LAS FUNCIONES CRITICAS

Los cuestionarios de funciones crfticas son diseñados para recolectar información que refleje la importancia de cada proceso en la organización. Un cuestionario deberá ser aplicado para cada proceso.

Para determinar lo que es "crftico", se deberá usar la medida de "tolerancia" que es definida como la capacidad de continuar con los procesos durante una interrupción de las actividades normales de la organización. Si la tolerancia de un proceso particular es pequeña, el proceso es probablemente crftico. La tolerancia puede ser cuantificada en terminos monetarios.

Los manuales de procedimientos pueden ser eficaces para continuar los procesos en un término corto pero talvés sean ineficientes, costosos sobre largos perfodos.

Los usuarios deben conocer el valor de los sistemas crfticos, por que ellos son los responsables. La experiencia muestra que son probablemente imparciales para evaluar lo crftico de sus sistemas.

Las preguntas deben ser directas para determinar procesos crfticos y métodos alternativos.

Si esto sucede todos los usuarios tienen una evaluación similar, son desarrolladas y reconocidas las estrategias alternativas.

La experiencia además muestra que cuando los cuestionarios son cortos y fáciles de completar, la mayorfa de las personas los regresan a tiempo y son correctos.

Probar y confirmar el contenido de los cuestionarios de funciones criticas, deberán ser discutidos y aprobados.

PRUEBA Y CONFIRMACIÓN DE LOS CUESTIONARIOS Y ENTREVISTAS DEL ANÁLISIS DEL IMPACTO DE LA ORGANIZACION.

Estos cuestionarios son necesarios antes de hacer las entrevistas de procesos específicos.
Estos cuestionarios deben ser discutidos y aprobados antes de hacer las entrevistas.(VER GUIA DE ANALISIS PARA UNA AREA DE LA ORGANIZACION)

DISTRIBUCIÓN DE CUESTIONARIOS
El coordinador del Plan debe distribuir los cuestionarios a todos los entrevistados más importantes. Estos probablemente deben ser para gerentes y jefes de departamento de la Organización. Los cuestionarios deben distribuirse a tiempo para que las entrevistas contemplen los puntos relevantes y es apropiado distribuirlos a todos los empleados quienes usan y manejan sistemas diariamente para asegurar que toda la información relevantes sea revisada.

El Coordinador de la recuperación de la organización deberá responsabilizarse de contactar a los individuos para asegurarse que estén preparados para las entrevistas y revisión de cuestionarios.

Los cuestionarios de las Funciones Críticas deben ser distribuidos al mismo tiempo que los cuestionarios de Impacto en la Organización juntos con información concerniente a los propósitos de las entrevistas, procedimientos, duraciones y tiempos. (VEASE CUESTIONARIO ANEXO)

PROPÓSITO DE LAS ENTREVISTAS PRELIMINARES.

El propósito de las entrevistas preliminares es para identificar lo siguiente:

1. Las áreas vitales de la organización para que la corporación sobreviva.
2. Los componentes críticos entre cada área de la organización.
3. Los sistemas esenciales para cada área de la organización.
4. Dependencia y facilidades de soporte.
5. Dependencia e impacto en otras áreas de la organización.
6. Pérdidas financieras directas y costos de recuperación involucrados en el seguimiento de las pérdidas.
7. Costos de un probable desastre como repercusión en las ventas.
8. Responsabilidad de los entrevistados.
9. Descripción del Trabajo realizado y procesos involucrados.
10. Número de Personas y Habilidad requerida para realizar el proceso.
11. Métodos alternativos de posibles procedimientos.
12. Procedimientos sugeridos de recuperación.
13. Prioridades de Recuperación.

El Plan de Contingencias es un Plan Técnico en el cual la participación del personal es valiosa.

Las guías de análisis de las áreas de la Organización deben ser usadas para asistir en la generación de discusiones en diferentes procesos críticos. Ellos incluyen componentes esenciales sugeridos, dependencias críticas, recursos alternativos y probabilidad del impacto de destrucción para diferentes áreas como:

1. La Gerencia y Ventas.
2. Personal.
3. Nómina
4. Mercadotecnia.
5. Producción.
6. Distribución.
7. Inventario.

Como en la mayoría de los Planes de Contingencias en el pasado estaban enfocados en las operaciones basadas en los sistemas automáticos. Es necesario en las entrevistas mencionar que el Plan de Contingencias intenta cubrir todos los procesos de la organización. Algunos no basados en la computadora deben ser discutidos y el cuestionario de las funciones críticas llenado.

CONDUCIR LAS ENTREVISTAS DE LOS SISTEMAS DE INFORMACIÓN.

Además de las entrevistas generales, es requerida información más detallada sobre los sistemas automáticos y durante las entrevistas con el jefe de procesamiento de Datos y especialistas se deberán revisar los sistemas y sus componentes esenciales como son:

- Términos de Información, estrategias tecnológicas y propósitos de desarrollo de sistemas.
- Personal de Procesamiento de Datos y detalles de escritorio.
- Instalaciones del Centro de Datos y funciones específicas.
- Hardware, modelo y configuración.
- Comunicaciones, redes, LAN, WAN (incluyendo microcomputadoras).
- Periféricos como terminales, impresoras y capacidad de disco.
- Facilidades esenciales de soporte.

- Tiempos de Proceso.
- Procesos en línea y batch.
- Lista de las Aplicaciones mayores.
- Plan de Contingencias existente.
- Localización y frecuencia de respaldos de programas y datos.
- Historia de Fallas en el sistema.

REVISIÓN DE LOS RESULTADOS DE LAS ENTREVISTAS.

Tomar en cuenta:

Cuestionarios de Funciones Criticas.
Cuestionarios de análisis de impacto en la organización.
Entrevistas.

CUESTIONARIO DE OPERACIÓN

1. Impacto de una hora de interrupción en el Centro de Cómputo.
   a) La mayor interrupción operacional en el servicio al cliente, es el tener grupos de personal totalmente parado.
   b) Inconveniente, pero el centro de las actividades del negocio continúan intactas.
   c) Esencialmente insignificante.

2. Impacto de una interrupción total en el Centro de cómputo, dos o tres semanas.
   a) Casi fatal, no hay fuentes de respaldo.
   b) Facilidades de respaldo externas, menores ingresos y mayores costos.
   c) Caro. Algunos procesos pueden ser preservados.

3. Aptitud del personal.
   a) En el centro de cómputo la fuerza de trabajo es organizada.
   b) Son inexpertos. (medios organizados).
   c) Son desorganizados.

4. Número de operaciones criticas en sistemas en Línea o en sistemas en Batch.
   a) 10 o más.
   b) 6-9.
   c) 3-5.
   d) 0-2.

5. Localización de los sistemas.
   a) En una área especifica.
   b) Dos o tres áreas.
   c) Corre por múltiples departamentos.

6. De fácil recuperación después de la interrupción.
   a) 3 o 4 días en sistemas críticos.
   b) 12 o 24 horas en sistemas crfticos.
   c) Sin problemas (recuperación inmediatamente).

7. Control de recuperación después de la interrupción.
   a) Mucho tiempo consumido y costoso por los sistemas interrelacionados.
   b) Alguna interrupción.
   c) Relativamente rápido, daño controlado.

8. Facilidad de copias manuales.
   a) Imposible.
   b) Algo es posible.
   c) Relativamente fácil.

GUIA DE ANALISIS PARA UNA AREA DE LA ORGANIZACION.

DEPARTAMENTO: ADMINISTRACION

AREA DE LA ORGANIZACION: NOMINA

INFORMACION GENERAL	COMPONENTE ESENCIALES	DEPENDENCIAS CRITICAS	RECURSOS ALTERNATIVO	IMPACTOS PROBABLES
-SUELDOS Y SALARIOS -EFECTIV -PAGO -TIEMPO -SERVICIOS -COMISIONES AGENTES -COMISIONES VENTAS. -PAGOS DE PRODUCTIVIDA	-REGISTROS STAFF -MODIFICACION EN LINEA -SERVICIOS EXTERNOS -CINTAS Y DISCOS -PAGOS DE PRODUCCION -SERVICIOS A TERCEROS -IMPUESTOS -OTRAS CONTRIBUCIONES. -COMISIONES Y BONOS. -PRODUCCION.	-SISTEMAS DE COMPUT -MICROCOMPUTADORAS -PAQUETES DE SOFTWARE -IMPRESORA -REDES. -SERVICIOS POSTALES -INTERDEPENDENCIA CON EL PERSONAL	-SISTEMAS MANUALE -PAGOS PREVIOS -CARGOS A TERCEROS	- COSTOS DE MANTENIMIENTO. -CARGOS ADMINISTRATIVOS. -INSATISFACCIONES DE EMPLEADOS -PAGOS DE COMISIONE O BONOS. -COSTOS DE RECUPERACION DE DATOS.
INFORMACION QUE MANEJA EL AREA?	QUE ACTIVIDADES PRINCIPALES REALIZA?	DE QUE DEPENDE PARA REALIZAR SUS FUNC.? CUALES SON SUS RECUR.?	COMO SE PODRIA SOLUCIONAR?	QUE IMPLICARIA DEJAR DE TENERLO AUTOMATIZADO?

CUESTIONARIO DE FUNCIONES CRITICAS

DEPARTAMENTO _____ DIVISION: _____

TELEFONO OFICINA:

JEFE: _____ EXT: _____

CALLE: _____

CIUDAD: _____ PISO: _____

EDO.PROVINCIA: _____ C.P._____

NOMBRE DE LA FUNCION: _____

DESCRIPCION DE LA FUNCION: _____

COMENTARIOS: _____

CON QUE FRECUENCIA ES REALIZADA LA FUNCION?:

ANUAL _____ SEMESTRAL _____ MENSUAL _____ SEMANAL _____ DIARIO _____

OTRA EXPLICACION: _____

1. CUAL SERIA EL COSTO PARA LA ORGANIZACION SI ESTA FUNCION NO FUERA REALIZADA?:

   POR DIA: $

   POR SEMANA: $

   POR MES: $

2.ESTIMAR CUAL SERIA EL COSTO ADICIONAL (MULTAS, PERDIDAS DE ARRENDAMIENTO, CONTRATOS CANCELADOS) EN QUE LA ORGANIZACION PUEDE INCURRIR SI ESTA FUNCION NO ES REALIZADA.

   POR DIA: $

   POR SEMANA: $

   POR MES: $

DE ACUERDO AL RANGO DE IMPORTANCIA DARLES VALOR DEL 0 AL 9

3. LA VIDA HUMANA ES PUESTA EN RIESGO SI ESTA FUNCION NO ES REALIZADA?:

   POR DIA: $ RANGO: _____

   POR SEMANA: $ RANGO: _____

   POR MES: $ RANGO: _____

4. LA ORGANIZACION TENDRA CONFLICTOS SI ESTA FUNCION NO ES REALIZADA?:

   POR DIA: $ RANGO: _____

   POR SEMANA: $ RANGO: _____

   POR MES: $ RANGO: _____

5. ESTO IMPACTARIA A LA OPERACION EFICIENTE DENTRO DE LA ORGANIZACION?:

POR DIA: $ RANGO: _____

POR SEMANA: $ RANGO: _____

POR MES: $ RANGO: _____

6. EL SERVICIO A LOS CLIENTES ES AFECTADO POR LA NO REALIZACION DE ESTA FUNCION?:

POR DIA: $ RANGO: _____

POR SEMANA: $ RANGO: _____

POR MES: $ RANGO: _____

7. LOS REQUERIMIENTOS LEGALES PUEDEN NO SER CUMPLIDOS SIN ESTA FUNCION?:

POR DIA: $ RANGO: _____

POR SEMANA: $ RANGO: _____

POR MES: $ RANGO: _____

5.3.1.4 COMPLETAR EL ANALISIS DE LA ORGANIZACION.

Determinar a partir de la información conseguida, los procesos críticos para la operación de la organización.

ESTABLECER CRITERIOS PARA DETERMINAR LAS FUNCIONES CRITICAS.

Establecer límites y criterios de las funciones críticas, los procesos serán clasificados como sigue:

Crítico : Escencial para la sobrevivencia de la organización.
Necesario: Escencial para mantener las funciones críticas de la organización.
Opcional : No crítico para las funciones de la organización.

Sugerir criterios financieros por niveles para evaluar pérdidas o costos adicionales, sobre perfodos específicos de tiempo como un día, una semana o un mes los cuales indican que la pérdida de estos procesos es crítica. Ejemplo: Evaluar pérdidas sobre un monto significativo en la organización, en un perfodo de tiempo, indica que el proceso es crftico.

ACTIVIDAD	PERIODO	PERDIDA EN LA ORGANIZACION
Nómina	Una semana	N$ 100,000.00
Facturación	Una semana	N$ 50,000.00

El Coordinador del Proyecto con Autorización del Jefe de Depto. debe evaluar las perdidas de cada actividad.

DETERMINACION DE LOS REQUERIMIENTOS NECESARIOS.

Determinación de algunos requerimientos formales para un desastre contenidos en un Plan de Contingencias.

I. Requerimientos de Auditorfa.
II. Requisitos legales.
III. Estandáres de la Industria.

El Coordinador de la recuperación de la organización debe estar familiarizado con los requerimientos. Identificar los riesgos potenciales a los que esta expuesta.

COMPLEMENTAR EL ANALISIS DE LOS PROCESOS CRITICOS DE LA ORGANIZACION.

La información recolectada es analizada usando los cuestionarios, resultado de entrevistas y el criterio.
Cada respuesta en los cuestionarios debe ser valorada.

IDENTIFICAR TODO LO CRITICO Y NECESARIOS PARA LA ORGANIZACION.

La clasificación de los procesos de la organización como crfticos, necesarios u opcionales determina cuales procesos deben ser considerados en el Plan de Contingencias.
"Ningún proceso del negocio evaluado como Opcional sera incluido en el Plan de Contingencias".
Discutir la clasificación de procesos crfticos con la gerencia y modificar lo necesario.

5.3.1.5 DOCUMENTAR LOS PROCESOS CRITICOS Y NECESARIOS DE LA ORGANIZACION

Documentar los procesos crfticos y necesarios de la organización para determinar cuáles deberán ser incluidos en el Plan de Contingencias.
Esta documentación es usada para determinar los departamentos de la organización que serán tomados en cuenta.

DETERMINAR LOS DEPARTAMENTOS CRITICOS.

El Coordinador de la recuperación de la Organización debe identificar a los departamentos que no deben de ser incluidos, cada uno de estos sirve como soporte de los departamentos críticos identificados.

DOCUMENTAR LOS PROCESOS NECESARIOS DE LA ORGANIZACION.

Recolectar toda la información reunida a la fecha de acuerdo a los procesos críticos y necesarios de la Organización.

Esto deberá incluir información de cada proceso completo, tiempos críticos, dependencias del sistemas y habilidades requeridas.

Preparar una tabla de referencias cruzadas mostrando cada proceso crítico de la organización por cada departamento y anotar las dependencias, cuando un proceso crítico es realizado por varios departamentos. Ejemplo:

PROCESOS	DEPTO. 1	DEPTO. 2
Nómina	Todo	
Control de Inventario	Reg.de Prov.	Pago a Prov.

Esta información es usada para determinar, la recuperación de procesos en cada departamento y el orden en que son recuperados en caso de un desastre.

Toda la información resultado de la Metodología DCP con excepción de los respaldos se referirá como crítica y como un elemento necesario de la organización. Los elementos no clasificados como críticos o necesarios no son incluidos como parte de la Metodología del Plan de Contingencias (DCP).

Se deben utilizar las utilerías del Plan de Contingenicas para guardar toda la información de la organización.

DISCUTIR Y ACORDAR LOS PROCESOS CRITICOS DE LA ORGANIZACION.

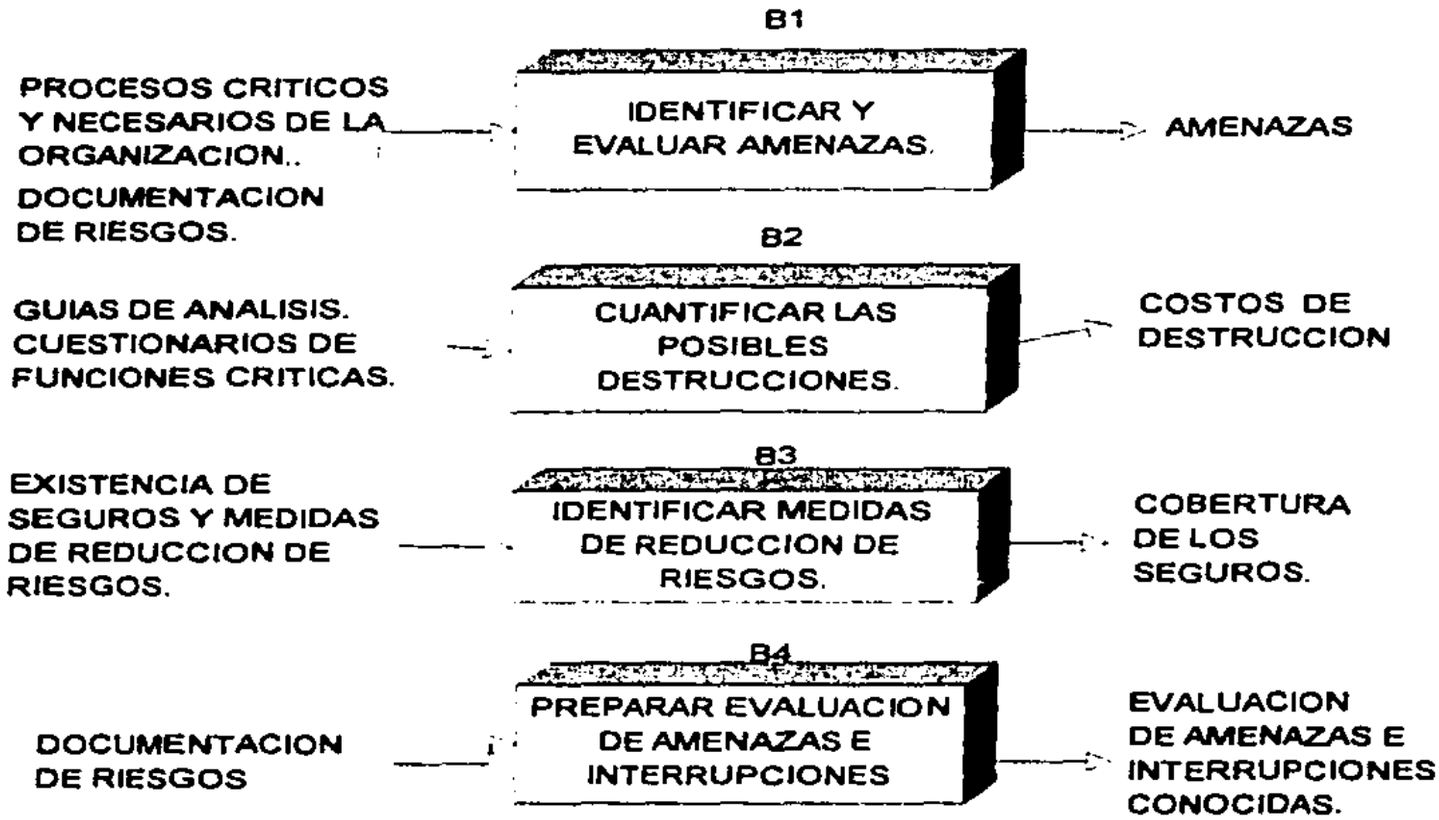
El Coordinador del Plan de Contingencias (DCP) debe ser un enlace entre jefes de departamento y el equipo del proyecto particularmente haciendo énfasis en los procesos críticos previamente acordados con la Gerencia.

OBTENER APROBACION DEL PROYECTO Y OBTENER AUTORIZACION PARA CONTINUAR.

El proyecto del Plan de Contingencias (DCP) debe ser totalmente aceptado por el gerente antes de continuar. Esto incluye:

- Preparar el alcance del Plan. (que magnitud de desastre debe ser prevista en el plan).
- Aprobación formal de la selección de los procesos críticos y necesarios de la organización.

FASE B. INTERRUPCION EN LA ORGANIZACION
RELACION DE TAREAS.



5.3.2 INTERRUPCION EN LA ORGANIZACION.

Identificar y evaluar la importacia de algunos riesgos para los procesos crfticos y necesarios de la organización.

Teniendo identificados los procesos y funciones clave, es necesario identificar y evaluar los riesgos para la operación continua.
Es importante entender la diferencia entre amenaza y riesgo para apreciar los procesos lógicos de la metodologia.
Las definiciones son:
Amenaza: Persona o cosa conocida como peligrosa.
Riesgo: Desastre o Pérdida natural.

El aspecto relevante del riesgo es la probabilidad de que una amenaza lo cause.
La metodología primero identifica el riesgo y gradualmente el potencial de la amenaza en la organización.

La reducción del riesgo y la evaluación de las amenazas.

ENTRADAS:	Procesos crfticos y necesarios de la organización. Documentación de Riesgos. Guías de análisis de los departamentos. Cuestionarios de Funciones Crfticas. Existencia de seguros. Existencia de medidas de reducción de riesgos.
TAREAS:	Identificar y evaluar amenazas. Cuantificar posibles destrucciones. Identificar medidas de reducción de riesgos. Preparar evaluación de amenazas e interrupciones.
PRODUCTOS:	Amenazas. Evaluación de amenazas e interrupciones conocidas. Costos de interrupción. Cobertura de seguros.
FASE LIBERADA:	Evaluación de amenazas y riesgos.
FORMAS:	Hojas de Riesgo y Amenazas. Guías de Análisis de Areas de la Organización.

5.3.2.1 IDENTIFICAR Y EVALUAR LAS AMENAZAS.

Identificar y evaluar la probabilidad de ocurrencia e impacto de las posibles amenazas en los procesos crfticos y necesarios de la organización.

Existen muchas amenazas que pueden interrumpir las operaciones de la organización de la organización y varios métodos para clasificar estas amenazas.

Colocar las amenazas en categorias para identificarlas, las amenazas para evaluar son las siguientes:

- Agua,
- Fuego,
- Fallas de Energia,
- Interrupciones mecanicas o fallas del software,
- Problemas especfficos relacionados con personal.

La identificación y evaluación de amenazas es necesaria para preparar prevenciones y procedimientos de recuperación.

La identificación de amenazas además provee ventajas como las siguientes:

- Identificación de medidas preventivas dondesean requeridas.
- Detectar susceptibilidades previamente desconocidas para dirigir planes y procedimientos.
- Incrementar el conocimiento del personal sobre amenazas y evidencias de este, cuando comienzan los problemas.
- Podemos además sensibilizar el propósito en el personal en la preparación del Plan de Contingencias.
- Podemos identificar interdependencias entre departamentos y lograr una mejor cooperación interdepartamental para lograr proteger vulnerabilidades.
- Identificar cuales costos son posibles compartir, para prevención de amenazas en los sistemas.

Existen expertos quienes pueden ser consultados para asistir en la evaluación de amenazas de servicio de emergencias. El coordinador de la Recuperación de la Organización debe proveer información sobre amenazas locales, basadas en el conocimiento de la organización su industria y su experiencia.

FACILIDAD PARA IDENTIFICAR AMENAZAS.

Hay muchas formas de amenazas. El mejor método de agrupar estas amenazas es por el fénomeno que causa en las operaciones de la organización, al ser interrumpidas.

Después de inspeccionar el lugar, los expertos deberán entregar un reporte escrito que incluya:

- Los bomberos identificarán amenazas de fuego.
- Personal de servicio médico, quienes pueden identificar amenazas a la seguridad del personal.
- Departamento de policia quienes pueden identificar amenazas de seguridad.
- Departamento de Salubridad, quien puede identificar amenazas por falta de higiene.
- Personal de auditorfa quienes identifican la perdida de integridad de los datos.
- Algunos otros servicios quienes identifican amenazas particulares.

Las amenazas a la organización pueden existir por el tipo de actividad realizada en las áreas cercanas.

Para asistir en la identificación de amenazas de entidades externas a la organización, es recomendado un mapa de las áreas cercanas, anotando las actividades de otras entidades en la misma área, como organizaciones, rfos, caminos, aeropuertos, vías de ferrocarril.

Identificar todas las amenazas relevantes como crfticas para la organización. Las amenazas a la organización pueden ser influenciadas por entidades externas como: filiales, divisiones y unidades de operación que son autónomos o controladas centralmente.

La evaluación deberá también considerar amenazas a Centros de Computo externos, los cuales dan servicios importantes como respaldos, subestaciones eléctricas, líneas de teléfono opcionales y amenazas específicas a los centros de computo bajo revisión.

El documento identificador de amenazas deberá ser complementado anotando los detalles de las amenazas.

IDENTIFICAR AMENAZAS PARA PROCESOS AUTOMATIZADOS.

En el pasado de acuerdo a estadísticas las causas mas comúnes de desastre en procesamiento de datos, fueron fuego y agua.

En la última década, la prevención de fuego en los sistemas ha sido prevista y cada vez son mas organizaciones las que hacen uso de la probabilidad y efectos de desastre por el fuego. El agua es considerada la mayor amenaza al procesamiento de datos.

El fuego puede destruir sistemas crfticos no considerados en el procesamiento de datos, los cuales deberán ser contemplados en el Plan de Contingencia.

Fallas de energía eléctrica, mal funcionamiento del software y daños deliberados son las mayores amenazas al procesamiento de datos.
Al revisar los sistemas para identificar amenazas deberán existir los siguientes controles:

1.Personas no autorizadas no pueden accesar a:
- a) Procesos Batch o en línea.
- b) Menus de Acceso.
- c) Profiles.
- d) Dispositivos de Acceso.

2.Adecuar controles de entradas a procesos de transacciones:
- a) Edición de programas y validación.
- b) Llaves de entrada.
- c) Bitácoras de Auditoría.

3.Verificar la entrada de Datos:
- a) Controles en sesiones en línea.
- b) Controles en Batch.
- c) Controles de programas.
- d) Verificación de archivos internos.
- e) Controles en transmisión de datos.
- f) Procedimientos de recuperación.

IDENTIFICAR AMENAZAS PARA PROCESOS NO AUTOMATIZADOS.

Los procesos de la organización no automatizados que son crfticos y necesarios son frecuentemente sujetos de diferentes clases de amenazas comparados con los procesos automatizados de la organización. Los procesos de la organización automatizados y los no automatizados deben ser considerados separadamente.

El uso de la experiencia de los auditores en identificación de datos y procedimientos de Control de la Organización pueden ser usadas en este paso.

Modificar el documento haciendo notas sobre los detalles de las amenazas identificadas.

PROBABILIDAD DE AMENAZA EN LOS ACTIVOS.

Las guías de análisis de los riesgos sirven para ayudar a la evaluación de amenazas en los procesos crfticos de la organización.
La destrucción total de una organización es poco probable. La ocurrencia de pequeños accidentes es más probable y estos deben ser considerados.

Los rangos utilizados para las amenazas potencialmente peligrosas para la organización son:

- ALTO: La amenaza es real y es probable que se presente el problema algún día.
- MEDIO: La amenaza existe pero es poco probable que se presente el problema en circunstancias especiales.
- BAJO: La amenaza no es realmente probable en la organización.

5.3.2.2 CUANTIFICAR POSIBLES DESTRUCCIONES.

Cuantificar el impacto de alguna amenaza destructiva para los procesos crfticos de la organización.

Las amenazas identificadas como potencialmente peligrosas para la organización y para los procesos crfticos deben ser evaluados o medidos de alguna forma.

La más apropiada medida común del impacto de desastres en las operaciones de la organización es el aspecto financiero.

Pérdidas potenciales en ingresos, costos adicionales en la operación y costos intangibles para la organización necesitan ser cuantificados por cada amenaza identificada en los procesos crfticos y necesarios de la organización.

Las guías de Análisis de áreas de la organización, vistas en la fase anterior sirven para asistir en el reconocimiento de impactos probables de destrucción.
Existen guías que deben ser modificadas por alguna información especffica de la situación.

Los procesos no automatizados deben ser considerados por separado, el impacto de destrucción para este tipo de proceso puede ser mas devastador y mas diffcil de cuantificar que el de un proceso automatizado. Las operaciones no automatizadas frecuentemente proveen documentos fuente originales y otra información importante que no es capaz de estar respaldada en la base de datos.

CUANTIFICAR LA PERDIDA EN LOS INGRESOS.

Determinar que áreas de ingresos pueden ser afectadas si se identifican amenazas relacionadas con aplicaciones criticas ocurridas ahf.
Las áreas de ingresos pueden incluir perdidas en ofertas, la inhabilidad de proporcionar buenos servicios, cancelaciones de reembolsos y muchos otros.

En este punto se deben de incorporar y estimar la perdida de ingresos intangibles debidos a cosas tales como perdida de buenas relaciones con los clientes.

Para cada una de las amenazas, estimar la perdida de ingreso debido a la destrucción de las operaciones normales para cada periodo especffico de tiempo, como un dfa, una semana o un mes.

CUANTIFICAR LOS COSTOS ADICIONALES.
Determinar donde se encuentran los costos adicionales debidos a una amenaza potencial relacionada con las aplicaciones crfticas y necesarias.
Estos Costos Adicionales tal vez incluyen pérdidas por descuentos, personal o multas legales. En este punto incorporar los costos estimados de restauración de operaciones.

Por cada una de estas amenazas, estimar los costos adicionales incurridos debido a la destrucción de las operaciones normales para periodos especfficos de tiempo como un dfa, una semana o un mes.

Además es necesario conducir discusiones y entrevistas para identificar y obtener detalles precisos.

CUANTIFICAR EL DESASTRE EN PROCESOS DE LA ORGANIZACION NO AUTOMATIZADOS.

Considerar el efecto para identificar las amenazas potenciales en todos los procesos de la organización no automatizados.

Estos deben de comprender las entradas de datos no automatizados (que predominan en los procesos de la organización automatizados como documentos Fuente de proveedores o de Almacenes).

La mayor parte de procesos crfticos no automatizados consiste en:

- Encontrar los registros vitales no registrados en la computadora, por ejemplo:
  documentos fuente originales de entradas prioritarias de datos, documentos legales originales, contratos o registros manuales guardados (archivados).
- Artículos ffsicos como maquinarfa en las fabricas necesarios para la producción.
- Teléfono, energfa, agua, drenaje y gas.

Para cada una de estas amenazas estimar los costos por perfodos especfficos de un dfa, una semana y un mes.

CUANTIFICAR COSTOS INTANGIBLES.

Determinar en donde se pueden dar las perdidas intangibles provocadas por amenazas potenciales.

El Coordinador de la Recuperación de la organización tal vez pueda proveer información estimada de los Costos Intangibles asociados con la destrucción de la organización basadas en el conocimiento de la misma.

Esto incluye:

- Pérdida de Relaciones con los Clientes.
- Pérdida de Competencia en el Mercado.
- Pérdida de información usada en Estrategias de Mercado y Decisiones de Operación.
- Oportunidades en los Negocios.
- Reducción de Flujo de Caja.
- Reducción de la Confianza de Proveedores, en términos de Crédito.
- Insatisfacciones de Empleados y Rotación.
- Pérdida de Investigación y desarrollo.

Para cada una de estas amenazas estimar el costo para la organización, de pérdidas intangibles debidas a destrucciones en las operaciones normales por perfodos especfficos de tiempo como un dfa, una semana o un mes.

La información del Cuestionario de las Funciones Criticas tal vez den las bases para estimar mas información para cuantificar estas perdidas.

5.3.2.3 IDENTIFICAR MEDIDAS DE REDUCCION DE RIESGOS.

Examinar medidas para reducir riesgos existentes e identificar los riesgos restantes para la organización y revisar los seguros existentes.

De esta manera los aspectos relacionados con el riesgo probablemente causen una amenaza.

Por ejemplo: Contar con controles ffsicos de acceso es una necesidad no una amenaza, sin embargo el no contar con ellos es una deficiencia la cual incrementa el riesgo, lo cual puede causar una amenaza.

Las medidas de reducción de riesgo deben ser revisadas para contrarrestar las Amenazas Potenciales identificadas.

Los seguros deben de ser revisados, su cobertura, costos y beneficios relativos.

Los documentos de Amenazas y Destrucciones deben ser preparados y discutidos.

IDENTIFICAR LAS MEDIDAS EXISTENTES PARA LA REDUCCION DE RIESGOS.

Identificar las medidas de reducción de riesgos existentes como: sistemas de detección de fuego, sistemas de supresión de fuego, controles de acceso físicos o procedimientos de seguridad de los centros de cómputo.

Revisar los procedimientos para el control y probar estas medidas para asegurarse que son efectivas y mantenidas adecuadamente.

Las medidas de reducción de riesgos, además incorporan funciones para la Prevención de desastres como:

- Mantenimiento regular de equipo (incluyendo todas las computadoras).
- Seguir recomendaciones de auditoria y técnicas de control.
- Procedimientos Manuales seguidos por los usuarios.

Prevención de errores y desastres intencionales a los sistemas pueden ser disminuidos adoptando un apropiado software de desarrollo que puede proveer:

- Controles de acceso lógico sobre ambientes de desarrollo.
- Pruebas por separado y transferencia de librerías.
- Control de Cambios.
- Reportes de Control incluyendo generación automática de:

a) Reportes por excepción,
b) Bitácoras de auditoría,
c) Reportes de violaciones en el acceso.
d) Totales de archivos, sumarios,
e) Estadísticas,
f) Procesos de respaldo y recuperación.

IDENTIFICAR LOS RIESGOS RESTANTES.

Uno de los Objetivos del Plan de Contingencias es exponer las amenazas posibles y minimizar el impacto de estas.

Las Amenazas a la Organización identificadas al inicio de esta fase son clasificadas, dependiendo de la probabilidad de su ocurrencia.

REVISION DE LOS SEGUROS EXISTENTES.

Los seguros contratados con su cobertura pueden ser medidas de reducción de Riesgos.

Los seguros reducen los Riesgos que sufren en Perdidas Financieras, debido a eventos destructivos que causan perdidas Físicas.

De cualquier forma estos nos dan un camino para continuar rápidamente con los procesos críticos en tiempos cortos, sin embargo sólo una parte del Plan de Contingencias se relaciona con lo financiero de la Recuperación de la Organización.

Se debe revisar la siguiente información:

- Extensión de la Cobertura. Que es lo que se cubre, que riesgos. Si la cobertura esta restringida a daños materiales (reemplazos o reparaciones), o solo terceras partes de Obligaciones.
- Condiciones especiales atacadas por políticas y exclusiones.
- Período de Indemnización. Por costos de trabajo extra y pérdidas por

sus consecuencias.
- Compensaciones Monetarias.

Si la Organización es una área afectada por desastres naturales como inundaciones, determinar la extensión de la Cobertura, para cada acto y las condiciones atacadas si cada evento recurre.

El Plan de Contingencias de la recuperación debe ser efectivo en un mínimo de tiempo y si las medidas de prevención de desastre existen, el riesgo de la Organización es significativamente reducido.

Esto no es necesario para asegurar que los Procesos de la Organización pueden ser totalmente recuperados.

Reducir los costos de seguros es frecuentemente viable a la Organización que puede reducir la probabilidad de un desastre debido a la Instalación de medidas de reducción de riesgos y una prueba del Plan de Contingencias.

REVISION DE LA COBERTURA DEL SEGURO.

Existen 4 Tipos Comunes de Seguros relacionados con los sistemas:
- Daños o destrucción de hardware.
- Pérdida en datos y programas ó el costo de reproducción de estos si es posible.
- Gastos Extras. Identificados en el Plan de Contingencias en cuanto a las operaciones normales.
- Seguros para interrupciones de la organización en cuanto a renovar el procesamiento de datos.

Algunas políticas de seguros relacionadas con los sistemas, deben ser revisadas, los Riesgos deben estar identificados y evaluar si la cobertura es adecuada. Incluyendo:

* Cobertura del Equipo:
  - Valores reemplazables.
  - Límites de tiempo para notificar a la compañía de seguros acerca del equipo nuevo adquirido, y
  - Cobertura de equipo en tránsito.

* Cobertura Media:
  - Costos de recolección, conversión y grabado de datos destruidos.
  - Valor de cintas físicas, discos y tarjetas.
  - Valor de archivos de datos.
  - Cobertura de programas (fuentes y ejecutables).

* Cobertura de Gastos Extras:

Incluye gastos anormales incurridos en operaciones como daños en los datos (costo de renta de equipos, ocupaciones temporales, alquiler de personal de transporte, proveedores de Centro de Computo temporales).

* Cobertura de los Seguros de interrupción:
  - Costos de restauración de Sistemas y documentación de programas para las aplicaciones existentes y para las aplicaciones en desarrollo en el tiempo de desastre.
  - Formas de Entrada.
  - Documentos Fuente.
  - Otros registros necesarios para el Procesamiento de Datos (legales de impuestos y bitácoras de auditoría).
  - Disturbios eléctricos.

- Filtración de agua.
- Extremas Temperaturas.
- Fallas estructurales y contaminación.
- Revisiones regulares de políticas y límites en la Cobertura por las adecuaciones.

REVISAR LA COBERTURA DE LA ORGANIZACION EN CASO DE INTERRUPCION.

Los Seguros en las Organizaciones son usados para compensar los destrucciones como consecuencia de un desastre. Los Seguros pueden reducir los costos financieros iniciales causados por un desastre y cubrir los costos base de la Recuperación.

Si la organización es una área afectada por desastres naturales como una inundación determinar la extensión de la Cobertura para cada acto y las condiciones atacadas para reclamar si cada Evento ocurriera.

REVISION DE COBERTURAS DE SEGUROS EN CENTROS ALTERNATIVOS.

Deberán ser revisadas las coberturas de seguros en centros de cómputo alternativos, considerando:

- La Cobertura debe compensar el desastre dando como alternativa un Centro de Procesamiento y Respaldo (Off-Site) con software apropiado, archivos de datos y documentación.
- Revisiones regulares de políticas y límites de cobertura.

5.3.2.4 PREPARAR EVALUACIONES DE AMENAZAS E INTERRUPCIONES.

Preparar una sección en el análisis de impacto de la Organización, evaluando las amenazas, costos potenciales de destrucción y medidas de reducción de Riesgos, (incluyendo seguros), para contrarrestar cada riesgo.

El peligro identificado de posibles amenazas es evaluado usando las medidas de Reducción de Riesgos. Las hojas de riesgo completan la evaluación. La información obtenida en esta fase es recolectada para proveer un resumen de:

- Todas las amenazas potenciales de la organización.
- Medidas de Reducción de Riesgos para contrarrestar estas amenazas
- Costos potenciales de destrucción en la organización.

COMPLEMENTAR LA EVALUACION DE AMENAZAS Y EL DOCUMENTO DE INTERRUPCION.

La información de esta tarea es recolectada en la etapa de Análisis de Impacto de la Organización. Para cada amenaza Potencial identificada, documentar el impacto esperado y los costos estimados por la interrupción, costos y efectos intangibles. Documentar cualquier Riesgo existente y tomar medidas para reducir este riesgo.

Se debe preparar una Hoja de Evaluación de Riesgos mostrando por cada amenaza identificada el Costo estimado de interrupción sobre períodos específicos de tiempo.

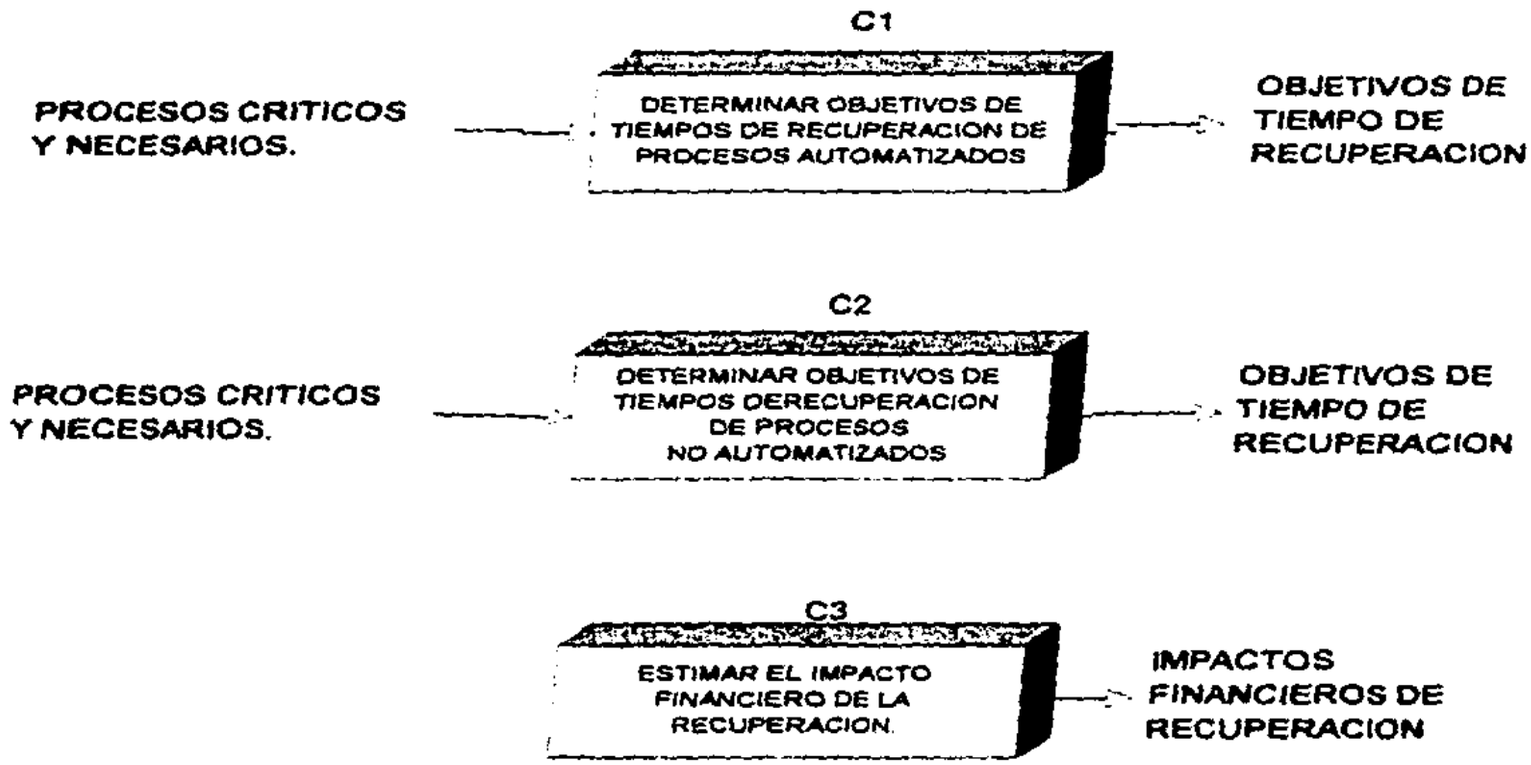
Preparar un documento que muestre los riesgos potenciales, no contrarrestados con las existentes medidas de reducción de riesgos.

Discutir y acordar el documento de evaluación de amenazas e interrupciones.

El coordinador de la recuperación de la organización, debe discutir con sus superiores en cuanto a los propósitos de la Evaluación y como combatir lo concluido.

TABLA DE CONTENIDO

FASE C. OBJETIVOS DE TIEMPO DE RECUPERACION RELACION DE TAREAS.



5.3.3. OBJETIVOS DE TIEMPOS DE RECUPERACION.

Determinar el tiempo de recuperación de cada proceso crítico de la organización en un evento de emergencia.

Como parte de la Evaluación de los procesos críticos, es necesario considerar un tiempo máximo para la Organización que puede estar sin cada proceso (antes que suceda un desastre), y deba ser restablecido. Esto sirve para identificar el tiempo de recuperación.

En este etapa, es determinado el tiempo de recuperación. En eventos de Desastres Regionales, es necesario tomar en cuenta los tiempos estimados de los demás áreas similares.

El tiempo de recuperación de procesos críticos, automatizados y no automatizados son considerados por separado como tareas independientes.

ENTRADAS: Procesos Críticos y Necesarios.

TAREAS: Determinar objetivos de tiempos de recuperación de los procesos automatizados
Determinar objetivos de tiempos de recuperación de los procesos no automatizados.
Estimar el Impacto Financiero de la Recuperación.

PRODUCTOS: Objetivos de Tiempo de Recuperación.

FASE LIBERADA: Impacto Financiero de Recuperación.

5.3.3.1 DETERMINAR OBJETIVOS DE TIEMPOS DE RECUPERACION DE PROCESOS AUTOMATIZADOS.

Determinar el tiempo máximo en que la organización puede estar fuera de operación sin problemas, con cada uno de los procesos automatizados.

Por cada aplicación automatizada que fue definida en la primera parte como crítica para la organización, determinar el lapso de tiempo entre la interrupción del proceso de la organización y la recuperación de este, hasta llegar a los niveles normales de operación.

La confiabilidad de un sistema se refiere al tiempo en que este puede operar con éxito. En cada sistema crítico se puede determinar una medida probabilística que indique la posible falla de un sistema en un período de tiempo determinado.

La probabilidad del impacto de la interrupción en los procesos de la organización fue considerada durante la evaluación de riesgos en la fase de interrupción de la Organización. Determinar el objetivo de tiempo de recuperación de cada aplicación, el impacto en la organización causado por la pérdida de la función considerando diferentes períodos de tiempo.

La frecuencia con que cada proceso de la organización es considerado esta dada por los puntajes críticos asignados. Son identificados algunos periodos críticos donde los procesos deben ser recuperados más rápidamente. Si el personal de Nómina paga mensualmente ellos necesitan sus aplicaciones al final del mes, sin embargo debe de ser más urgente un proceso que se necesite cada quincena.

En la determinación de objetivos de tiempos de recuperación de las aplicaciones críticas, todos los requerimientos de cada aplicación deben de ser considerados como prioritarios, hardware, software, datos, personal y proveedores.

El objetivo de tiempo de recuperación de cada tipo de aplicación requerida debe ser estimado, tomando en consideración cada requerimiento, documentación apropiada y respaldos existentes. Esto sirve para determinar requerimientos más específicos de una aplicación, proveedores, sistemas de retroalimentación, datos ó software de aplicación. Los requerimientos específicos menores son el hardware y el software, debido a que probablemente son requeridos en más aplicaciones y su objetivo de tiempo de recuperación tal véz dependan de aplicaciones que requieren un tiempo corto de recuperación.

Los individuos involucrados en la operación de cada proceso crítico automatizado deben ser los que contribuyan a definir los objetivos de tiempos de recuperación y los requerimientos de las aplicaciones.
El coordinador de el Plan de Recuperación debe encargarse de revisar la información y los tiempos de recuperación, así mismo deberá presentar los estimados a sus superiores.

ESTIMAR OBJETIVOS DE TIEMPOS DE RECUPERACION DE LOS PROCESOS AUTOMATIZADOS.
Estimar el tiempo máximo de recuperación de cada aplicación antes de que la organización comience a sufrir impactos críticos.
Estimar y documentar el objetivo de tiempos de recuperación en condiciones de emergencia y en condiciones de operación normal.

Considerar métodos alternativos de procesamiento (registros manuales) por términos cortos de emergencia. los procesos manuales no son alternativos viables para periodos largos, ya que requieren una labor intensa. además si la naturaleza de la organización tiene dependencias tecnológicas, es probable que los procesos automatizados provean de servicios que son imposibles de procesar manualmente. Si el proceso manual es una alternativa viable, se debe considerar personal extra.

La vigencia de restaurar una aplicación va a depender de varios factores:
Si la aplicación opera en batch (lote) ó en línea (on-line), si esto es un proceso crítico en tiempo (proceso mensual) ó si la organización tiene aplicaciones que interactuen con servicios al cliente.

REVISION DE PROVEEDORES.
Considerar a los proveedores utilizados en la aplicación y en que tiempo estos pueden ser necesitados, las formas de los cheques pueden ser necesitadas inmediatamente para las cuentas por pagar.

Si un proceso manual es considerado viable como un método de emergencia, considerar algunas formas extras requeridas para registrar toda la información antes de ser procesada. Cuando se diseñan algunas formas extras, esta información debe ser eventualmente utilizada como entrada para los sistemas automatizados y además estas formas deben parecerse a los formatos de entrada del sistema.

Preparar una lista de proveedores, tomando en cuenta los procesos críticos automatizados, así como los objetivos de recuperación, y asegurarse que cada proveedor se encuentre dentro del objetivo de recuperación.

REVISAR LOS SISTEMAS DE RETROALIMENTACION.
Considerar que algunos datos son usados en aplicaciones de otros sistemas (los retroalimenta).
Estimar en que tiempo los datos utilizados por otros sistemas deben ser requeridos para alimentar otras aplicaciones.
Si el sistema al que retroalimenta la aplicación es crítico, aunque este no sea crítico, debe ser estimado su tiempo de recuperación.

Si la aplicación esta considerada como de retroalimentación a otro sistema crítico y necesario, este debe estar dentro de la revisión de tiempos de recuperación. Si la aplicación retroalimenta a un sistema no crítico, este no debe ser considerado.

Preparar una lista de datos de transferencia al proceso crítico, y el objetivo de tiempo de recuperación de cada sistema de retroalimentación, para asegurar que el proceso crítico de la organización reciba las entradas apropiadas, que permita recuperarse a la organización en los tiempos requeridos.

REVISION DE DATOS.

Dado el tiempo de recuperación en cada aplicación estimar, el menor tiempo en el que los datos pueden estar disponibles.

Estimar la recuperación de todas las aplicaciones de cada dato, identificando el respaldo correcto, restauración y prueba

Preparar una lista de tareas relacionadas con la recuperación de datos para procesos criticos automatizados y el objetivo de tiempos para realizar estas tareas.

REVISAR EL SOFTWARE DE APLICACION.

Por cada proceso crítico, identificar y documentar el software de la aplicación específica.

Dado el tiempo estimado en cada aplicación para que esta sea operada y sus datos sean recuperados, estimar el tiempo permitido para la recuperación del software de aplicación. Esté tiempo de recuperación debe incluir tiempo de identificación de recuperación de respaldos, configuración y prueba.

Preparar una lista de tareas relacionas con la recuperación de software de aplicación.

REVISION DE SOFTWARE DE SISTEMAS.

Identificar y documentar cada sistema, incluyendo el software para soportar las aplicaciones.

Dar el tiempo estimado de recuperación de cada sistema, incluyendo tiempos de identificación y recuperación de respaldos, configuración y prueba. Preparar una lista de tareas relacionadas con la recuperación de sistemas.

w

REVISION DE HARDWARE.

Dar el tiempo estimado de recuperación para que vuelva a operar el software, estimando y documentando la recuperación del hardware. Incluyendo estimados para las tareas de recuperación como transportación del equipo, si es necesario, asistencia técnica externa, configuración y prueba.

Además considerar periféricos y otro equipo usado como impresoras, dispositivos de comunicación, scaners, etc. Preparar una lista de tareas relacionadas con la recuperación del hardware.

REVISION DE UTILERIAS.

Considerar y documentar las utilerías que son requeridas como de: telecomunicaciones, eléctricas, etc.

Preparar una lista de utilerías para permitir la recuperación en los tiempo deseados.

REVISION DE PERSONAL.

Considerar y documentar el personal que es requerido en la recuperación de la aplicación, incluyendo a los involucrados en el transporte de respaldos, instalación y configuración de software de aplicación, sistemas y hardware.

Preparar una lista de cada persona requerida durante la recuperación del proceso.

DOCUMENTAR LOS OBJETIVOS DE TIEMPOS DE RECUPERACION PARA TODAS LAS OPERACIONES REQUERIDAS.

Recopilar la información y documentar los procedimientos de las listas previas para producir objetivos de tiempos de recuperación para cada proceso crítico automatizado.

Discutir y confirmar los tiempo de recuperación y los tiempos requeridos.

5.3.3.2. DETERMINAR OBJETIVOS DE TIEMPOS DE RECUPERACION DE LOS PROCESOS NO AUTOMATIZADOS.

Determinar el tiempo máximo para cada proceso crítico no automatizado, que pueda estar fuera de operación sin problemas para la organización.

Para cada proceso no automatizado que sea crítico, se debe estimar el tiempo desde que sucede la interrupción hasta que se la recuperación. (Tomando en cuenta la operación emergente y en niveles de operación normal).

Se deben identificar períodos criticos de tiempo donde los procesos deben ser recuperados más rápidamente.

Para determinar el objetivo de tiempo de recuperación, es necesario tener todos los requerimientos de cada proceso, máquinaria y equipo usado, fuentes de datos, proveedores y personal.

Los individuos involucrados en la operación del proceso critico no automatizado deben ser los que contribuyan en las discusiones y acuerdos tomados en los objetivos de recuperación y procesos requeridos.

Se asume que los procedimientos no automatizados deben estar documentados, para la determinación de tiempos de recuperación de cada proceso básico.

El coordinador de la recuperación de la organización debe ser involucrado en la revisión de la recuperación, y en la presentación de estos estimados a la gerencia.

ESTIMACION DE TIEMPOS DE RECUPERACION DE PROCESOS NO AUTOMATIZADOS (MANUALES).

Para procesos no automatizados debe haber métodos alternativos en condiciones de emergencia, será necesario revisar los cuestionarios de las funciones críticas y las entrevistas relacionadas con el impacto de la organización y procesos de destrucción de la organización.

La urgencia de restaurar procesos de la organización depende de diferentes factores: evaluar si es de operación diaria, o de período de un mes. Tomar en cuenta los períodos criticos donde los tiempos de recuperación difieren dependiendo de posibles desastres.

REVISION DE LOS PROVEEDORES.

Considerar a los proveedores que intervienen en el proceso de la organización y como intervienen en restaurar el proceso de la organización, (para proveer materiales o componentes).

Preparar lista de proveedores utilizadas en procesos no automatizados de la organización y los tiempos de recuperación y contacto con los proveedores para asegurar que los procesos sean recuperados en los tiempos requeridos.

REVISION DE LOS SISTEMAS DE RETROALIMENTACION.

Considerar la información generada por esté proceso que sirve como entrada a otro proceso de la organización, si el siguiente proceso es crítico, los tiempos de recuperación de esté deben ser determinados.

Preparar una lista de datos que se transfieren a procesos críticos. Asegurarse que el proceso de la organización reciba las entradas apropiadas para permitir la recuperación de la organización en el tiempo estimado.

REVISION DE DATOS.

Estimar el tiempo en que los datos deberán estar disponibles.

Estimar tiempos intermedios para todas las tareas relacionadas con la recuperación de datos para los procesos de la organización, incluyendo identificación de la localización de respaldo, manipulación o modificación si se requiere.

Preparar una lista de tareas relacionadas con la recuperación de datos y tiempos para llevar a cabo estas tareas y asegurar que los procesos del negocio reciben los datos apropiados para permitir la recuperación en los tiempos requeridos.

REVISION DEL EQUIPO.

Identificar algún equipo usado en el proceso de la organización, maquinaria industrial, algún soporte de equipo, estimar el tiempo de recuperación de cada equipo. En esté estimado considerar el mantenimiento o alguna otra maquinaria requerida para la operación.

Preparar una lista de tareas relacionadas con la recuperación del equipo y estimar tiempos requeridos.

REVISION DE UTILERIAS.

Incluir en las consideraciones, que servicios de utilerías son requeridos, como telecomunicaciones, electricidad, gas o agua y como deben ser suministrados.

Preparar una lista de utilerías requeridas para soportar las operaciones críticas de la recuperación.

REVISION DEL PERSONAL.

Considerar el personal requerido en la recuperación de la organización incluyendo transportistas e instaladores del equipo.

Listar a cada persona requerida y alternativa durante la recuperación de la organización.

Documentar el tiempo de recuperación para todos los procesos no automatizados requeridos.

Discutir y confirmar el tiempo de recuperación y los recursos requeridos.

5.3.3.3 ESTIMAR EL IMPACTO FINANCIERO DE LA RECUPERACION.

Determinar el costo financiero de recuperación de los procesos una vez que el desastre haya ocurrido.

Los costos financieros de los procesos actuales involucrados en la recuperación de la organización deben ser estimados. Esta información, junto con el impacto financiero de la destrucción, determina el costo total causado por la pérdida de los procesos de la organización.

Este costo es usado para comparar el costo de las medidas de seguridad para reducir el riesgo, sirve para determinar el apropiado nivel de medidas a implantar para proteger el proceso de la organización.

Las medidas de seguridad deben de costar menos que el costo de la recuperación de un proceso.

El costo de la recuperación depende de el grado de destrucción.

ESTIMAR EL COSTO DEL TIEMPO INVOLUCRADO DEL PERSONAL EN LA RECUPERACION DE PROCESOS.

Estimar las horas no productivas, tiempo trabajado por el personal en la recuperación del proceso. Estimar el tiempo de espera del personal no involucrado en las tareas de recuperación hasta el momento en que quede restaurado el proceso. Estimar el costo de este tiempo, incluyendo costos de tiempos extras para la recuperación, talvés sea necesario trabajar varias horas para recuperar los procesos, lo más rápidamente posible. Estos costos deben de ser estimados para cada nivel de desastre.

ESTIMAR EL COSTO DEL EQUIPO EXTRA USADO EN LOS PROCESOS DE RECUPERACION.

Estimar y documentar el costo del equipo que es usado para la recuperación del proceso. Esto debe de incluir equipo telefónico, hardware, vehículos, equipo de seguridad, maquinaría y utilerías.

Estos costos deben de ser estimados por cada grado de desastre.

ESTIMAR LOS COSTOS DE PROVEEDORES/SERVICIOS REQUERIDOS PARA SOPORTAR EL PROCESO DE RECUPERACION.

Estimar y documentar los costos de algunos servicios externos que son requeridos. Considerar el costo de soporte externo de recursos de servicio de emergencia (departamento de bomberos, proveedores de hardware, proveedores de software, firmas de ingenieros, consultores que proveen utilerías y servicios de seguridad).

En un evento de desastre el personal debe estar distribuido, tener comida y transporte, estimar los costos de esta parte para la recuperación.

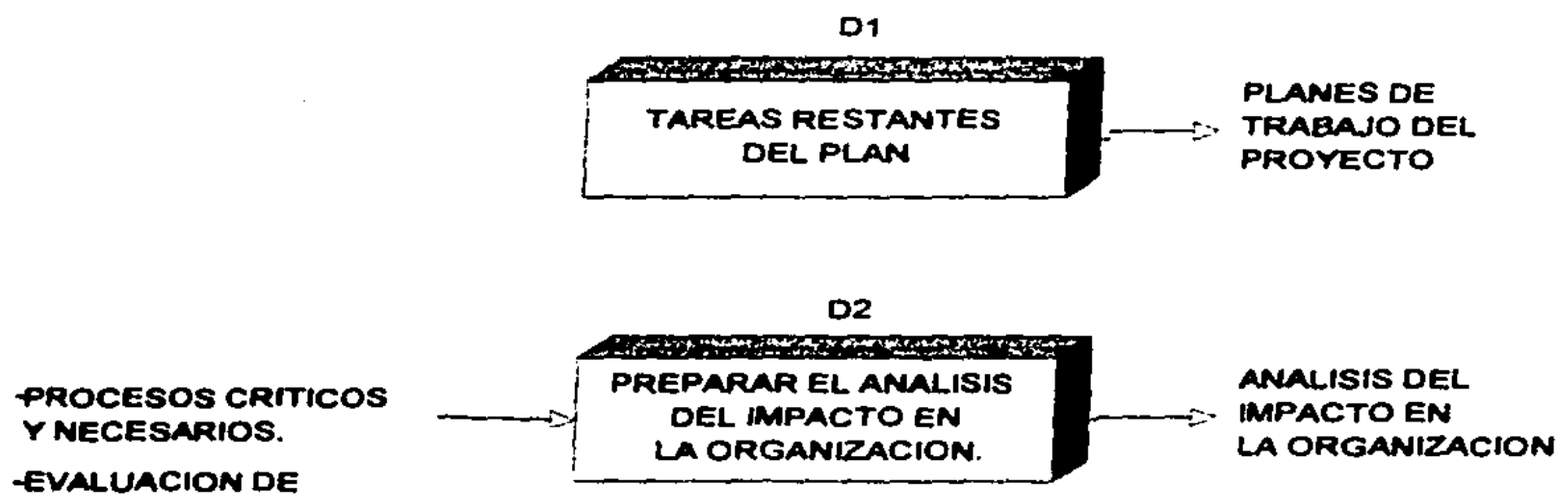
Estos costos deben ser estimados por cada grado de desastre.

REVISAR LA COBERTURA DE LOS SEGUROS ESTIMANDO EL COSTO DE LA RECUPERACION.

Los seguros no substituyen los procedimientos del plan de recuperación, pueden ayudar en el financiamiento de la operación de recuperación.

Discutir y confirmar el impacto financiero del proceso de recuperación con los Gerentes y resolver las preguntas y dudas si es necesario preparar una lista de acciones para modificar.

FASE D. CONCLUSIONES
RELACION DE TAREAS.



- INTRODUCCION
- OBJETIVOS
- EVALUACION
- PROCESOS CRITICOS
- AMENAZAS
- IMPACTO FINANCIERO
- TIEMPOS DE RECUPERACION
- OTRAS CONSIDERACIONES
- SELECCION DE ESTRATEGIAS
- PLAN DE TRABAJO.

5.3.4 CONCLUSIONES.

Preparar la evaluación del análisis del impacto de la organización. para la siguiente etapa del Plan de Contingencias.

El análisis del impacto de la organización, debe contener una evaluación de los procesos de la organización con respecto a la interrupción de la operación normal.

El mayor enfásis del análisis el impacto de la organización son los costos potenciales y el impacto de la organización desde la destrucción hasta la operación normal de los procesos críticos de la organización.

ENTRADAS: Procesos críticos y necesarios de la organización.
Evaluación de amenazas e interrupción.
Objetivo de tiempos de recuperación.
Impacto financiero de la Recuperación.

TAREAS: Tareas restantes del Plan.
Preparar el análisis del Impacto de la Organización.

PRODUCTOS: Planes de trabajo del proyecto.

FASE
A LIBERAR: Análisis del impacto de la organización.

5.3.4.1 LAS TAREAS RESTANTES DEL PLAN.

Preparar el proyecto del Plan y los costos de los calendarios para la siguiente estapa del Plan de contingencias.

La terminación de la etapa de análisis del impacto en la organización ayuda a entender a la organización y lo que es involucrado en el plan de contingencias.
Se debe de preparar la etapa de selección de la estrategia.

PREPARAR EL PLAN DE TRABAJO DE LA ETAPA DE SELECCION DE LA ESTRATEGIA.
Como tarea final en la conclusión de la fase del análisis del impacto de la organización se deberá desarrollar un plan de trabajo para la selección de la estrategia, identificando las tareas necesarias para completar la etapa. Por cada tarea en la etapa de selección de la estrategia se debe de estimar lo siguiente:
-Número de personas involucradas en el proyecto con adecuados perfiles.
-Cantidad de tiempo de cada miembro que invertira en cada tarea.
-Calendarizar la duración de cada tarea.
-Costo del tiempo del personal y costos adicionales
-Costo de hardware, software y utilerías.

El estimado debe de incluir el costo de tiempo y el esfuerzo requerido por el coordinador de la recuperación del negocio y de otros miembros de la organización.

PREPARAR LOS COSTOS DEL PROYECTO Y ESTIMAR TIEMPOS.
Por cada fase subsecuente preparar un estimado incluyendo:

-Recursos de personal y calendarios.
-Cantidad de tiempo estimado para completar la fase.

-Costo del tiempo del personal y tiempo máquina.
-Costo de riesgos adicionales y medidas de reducción de riesgos.

Para cada determinada situación documentar los recursos usados para preparar estimados.

REVISAR Y VALIDAR LOS ESTIMADOS.

Para la selección de la estrategia y de todos los estimados obtener una estimación por otra persona diferente a la que lo preparo. Esta revisión debe enfocarse en razonables recursos y en los estimados. El Coordinador de la Recuperación de la Organización debe preparar ó revisar los estimados de personal sin que la organización sea involucrada en el proyecto, en conjunción con otros miembros del proyecto familiarizados con las tareas involucradas.

Discutir y aprobar el contenido del plan del trabajo.

5.3.4.2 PREPARAR DOCUMENTO DEL ANALISIS DEL IMPACTO DE LA ORGANIZACION.

Proveer y evaluar la recuperación de una interrupción potencial de procesos críticos de la organización.

El análisis del impacto de la organización da a conocer los costos potenciales del impacto de la destrucción para operaciones criticas de la organización, esto incluye:

-Identificación de procesos críticos de la organización, automatizados y no automatizados.
-Amenazas potenciales, para cada proceso critico de la organización.
-Medidas existentes de reducción de riesgos.
-Costos potenciales de interrupción de cada proceso necesario en la organización.
-Seguros existentes y coberturas para asistir en la recuperación financiera de las operaciones.
-El menor tiempo requerido de cada proceso de la organización en una recuperación de emergencia desde que sucede el desastre hasta la operación normal de la organización.

DETERMINAR LAS PRIORIDADES DE LA RECUPERACION.

Basado en la clasificación de los procesos críticos y necesarios de la organización, estimar los costos de la interrupción de la organización, el estimado del costo de la recuperación.

Asignar prioridades de recuperación de cada proceso crítico de la organización.

Estas prioridades ayudarán a determinar el objetivo de recuperación de las operaciones y estructurarán las tareas de recuperación.

La recuperación parcial de un proceso talvés sea suficiente para completar los procesos críticos. Durante la recuperación solo se deberá restaurar información actual y los archivos historicos se recuperarán en una etapa posterior.

Determinar las prioridades de recuperación, (estas dependen del tiempo de recuperación del desastre, por ejemplo un día de la semana talvés afecte la nómina, un mes puede afectar los estados financieros reportados, un año puede afectar el Balance General y reportes financieros de mercado). El coordinador de la recuperación de la organización debe proveer una guía y asistencia para las prioridades de la recuperación basado en sus conocimientos.

Asignar prioridades de recuperación a procesos críticos de la organización.

RECOLECTAR DATOS DE LA FASE DEL ANALISIS DEL IMPACTO EN LA ORGANIZACION.
Incluir en un documento lo siguiente:

-Lineamientos del trabajo a realizar.
-Acordar alcances y objetivos del análisis del impacto de la organización.
-Puntos a evaluar.
-Identificar procesos críticos de la organización, ambos los automatizados y los no automatizados y el método por el cual fueron estos seleccionados.
-Evaluación de amenazas y interrupciones.
-Tiempos mínimos de recuperación.
-Otras consideraciones.
-El detalle del plan de trabajo para la selección de la estrategia del proyecto.
-Un plan de trabajo para las tareas de las etapas restantes.
-Detalle de apéndices y sumarios de información.

DISCUTIR EL ANALISIS DEL IMPACTO DE LA ORGANIZACION CON LOS DIRECTIVOS.

Confirmar de nuevo con la gerencia los recursos requeridos para completar el desarrollo del plan de contingencias y mantener el desarrollo del plan hasta su término.

El coordinador de la recuperación debe ser responsable de la prueba y mantenimiento del plan y debe proveer los suficientes recursos para completar esta tarea, incluyendo tiempo y personal requerido para asistir al coordinador.

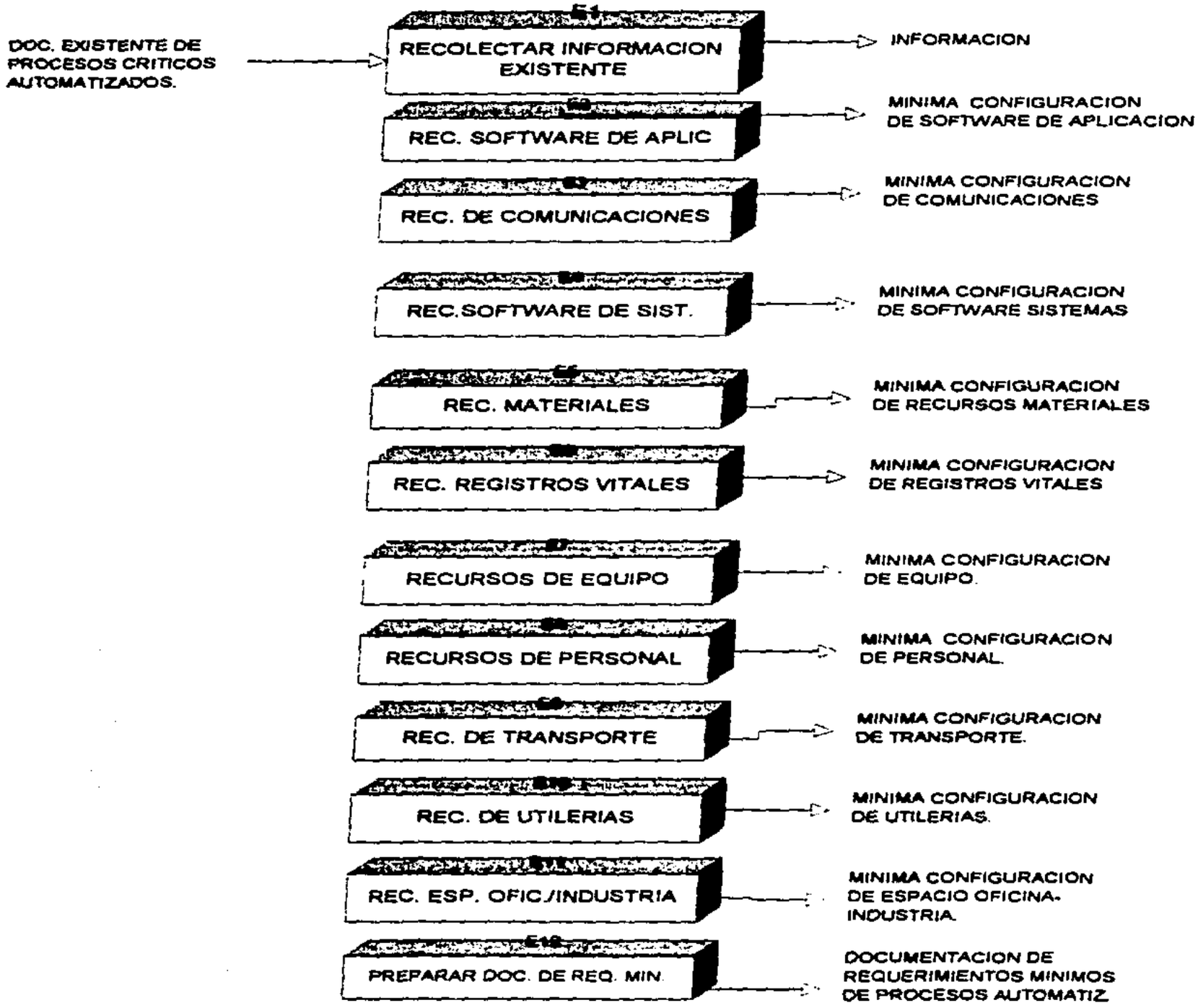
Discutir con la gerencia, resolver las dudas y si es necesario preparar una lista de acciones para modificaciones.

Obtener la aprobación de la fase del análisis del Impacto de la Organización.

TABLA SUGERIDA DEL CONTENIDO
ANALISIS DEL IMPACTO EN LA ORGANIZACION. .

Introducción
.
1.Alcances y objetivos del análisis del impacto en el negocio.
2. Sumario de Evaluaciones
3. Funciones críticas de la organización.
4. Evaluación de amenazas e interrupciones.
5. Impacto financiero de la recuperación.
6. Objetivos de tiempos de recuperación.
7. Otras consideraciones.
8. Plan de Trabajo para la etapa de la Selección de la estrategia.
9. Plan de trabajo para todo el proyecto.
Apendices.

FASE E. RECURSOS MINIMOS DE RECUPERACION DE PROCESOS AUTOMATIZADOS. RELACION DE TAREAS.



5.4. ETAPA DE SELECCION DE LA ESTRATEGIA

Es concerniente a la elección del más apropiado respaldo y opciones de recuperación del desastre.

-Definiendo los requerimientos mínimos para la operación de todos los procesos críticos de la organización.
-Opciones de Respaldo.
-Opciones de Recuperación
-Identificar medidas para reducir los riesgos de interrupción de la organización.
-Selección de la más apropiada estrategia de recuperación.

5.4.1. RECURSOS MINIMOS DE RECUPERACION (PROCESOS AUTOMATIZADOS)

Identificar en detalle los recursos requeridos para operar los procesos críticos automatizados de la organización bajo condiciones de recuperación.

Cada proceso tiene un número determinado de recursos requeridos. En esta fase se hace una investigación detallada.

Hay dos fases involucradas en la recuperación de una interrupción de la organización:

-La primera es la preparación de los centros de recuperación.
-La segunda es la operación de procesos críticos bajo condiciones de recuperación.

Los requerimientos definidos como escenciales para correr aplicaciones, podrán proveer una "configuración mínima" requerida para operar todos los procesos críticos automatizados de la organización bajo condiciones de recuperación.

ENTRADAS:	Documentación existente de procesos críticos automatizados.
TAREAS:	Recolectar información existente Determinar requerimientos de recursos de software aplicaciones. Determinar requerimeintos de recursos de comunicaciones. Determinar requerimientos de recursos de software de sistemas. Determinar requerimientos de recursos de materiales. Determinar requerimientos de recursos de registros vitales. Determinar requerimientos de recursos de equipo. Determinar requerimientos de recursos de personal. Determinar requerimientos de recursos de transporte. Determinar requerimientos de recursos de utilerías. Determinar requerimientos de recursos de espacio oficina/industrial. Preparar la documentación de requerimientos mínimos.
PRODUCTOS:	Información de discusiones. Configuración mínima de software de aplicación. Configuración mínima de comunicaciones. Configuración mínima de software de sistemas. Configuración mínima de recursos materiales. Configuración mínima de registros vitales. Configuración mínima de equipo. Configuración mínima de personal. Configuración mínima de transporte. Configuración mínima de utilerías. Espacio mínimo de espacio oficina/industria.
FASE A LIBERAR:	Documentación de requerimientos mínimos para procesos automatizados.

5.4.1.1. **RECOLECTAR INFORMACION EXISTENTE**

Reducir el tiempo para identificar la mínima configuración requerida para procesos automatizados bajo condiciones de recuperación.

Determinar si alguna de la información requerida ha sido documentada en el pasado para otros propósitos, como puede ser:

-Planes de Emergencia.
-Listas de recursos materiales.
-Inventarios de equipo.
-Contratos de mantenimiento.
-Acuerdos para el uso de lugares externo de respaldo (off-site).
-Estrategias de respaldo usadas.
-Procedimientos de operaciones normales.
-Alguna otra información relevante.

El coordinador de la recuperación de la organización deberá asistir en la selección del personal a ser involucrado en la recolección de información.

ASIGNAR PERSONAL PARA LA RECOLECCION DE INFORMACION.

Asegurarse de que el personal asignado a la tarea este capacitado en la recolección de información, de otro modo el proceso puede ser ineficiente.

REVISAR LA RELEVANCIA DE LA INFORMACION EXISTENTE

Si se usa la documentación existente como base, asegurarse de que se encuentre actualizada: identificar la fecha de la documentación y si los procedimientos han cambiado sin que la documentación haya sido modificada.

5.4.1.2. **DETERMINAR REQUERIMIENTOS DE RECURSOS DE SOFTWARE DE APLICACION.**

Determinar el software de aplicación usado y registrar detalles sobre su uso, configuración y requerimientos de cada software.

IDENTIFICAR EL SOFTWARE INVOLUCRADO EN LOS PROCESOS CRITICOS.

Determinar el volumen y frecuencia de transacciones correspondientes a cada aplicación.

Identificar todas las entradas y salidas de cada aplicación y determinar los soportes de cada función de la organización.

Deberá ser realizada una lista completa del software usado en la organización. Incluir software de microcomputadora y de aplicaciones de red local.

DOCUMENTAR EL SOFTWARE DE APLICACION PARA LAS OPERACIONES EN CONDICIONES DE RECUPERACION.

Para cada aplicación utilizada en la operación de procesos críticos y necesarios automatizados, documentar para la recuperación la siguiente información:

-Componentes del software de aplicación, (incluyendo nombre, programa identificador, descripción, versión y fecha de la última modificación).
-Código ejecutable correspondiente.
-Nombres de archivos de librerías.
-Archivos de datos.
-Lenguaje de control de jobs.
-Contenido de tablas.
-Manuales de procedimientos.

Deberá ser incluido el número de paquetes de discos y cintas magnéticas requeridas para copias de seguridad y archivos de respaldo, los cuales son necesarios para recuperar los procesos críticos automatizados.

La documentación sobre las aplicaciones deberá también incluir calendario y tiempos como por ejemplo:

-Calendarios de frecuencia(diario, mensual, semanal).

-Disponibilidad de datos para los usuarios.
-Tiempos de Comunicación con otros sistemas.

También indicar que tipo de transporte es necesario para trasladar los respaldos de las aplicaciones a centros de almacenamiento externos.

DOCUMENTAR REQUERIMIENTOS DE SOFTWARE DE APLICACION.

Por cada aplicación a ser usada en la operación de procesos críticos automatizados en condiciones de recuperación, documentar los requerimientos mínimos de software de aplicación. Considerar lo siguiente:

- Requerimientos del hardware.
- Requerimientos de comunicaciones.
- Requerimientos de software.
- Librerías requeridas.
- Ambiente requerido de software (incluyendo capacidad, medida y facilidades de seguridad).
- Frecuencia de procesos.
- Requerimientos de respaldo.
- Programas, sistemas y uso de documentación.
- Algún recurso material especial usado.

Estimar el espacio en disco.
Para cada tipo de aplicación en línea, documentar las características de transacciones de datos incluyendo:
- Volumen diario de transacciones.
- Tiempo de transacción.

También considerar la seguridad de las aplicaciones. La mínima seguridad requerida deberá ser considerada tomando en cuenta lo siguiente:
- Bitácoras de seguridad.
- Identificadores de entrada(Login y Password).

IDENTIFICAR PROVEEDORES PARA EL SOFTWARE USADO EN CONDICIONES DE RECUPERACION.
Para cada aplicación identificar los proveedores y algún servicio de soporte o personal con experiencia en la aplicación:
- Recursos de cada aplicación.
- Detalles de contacto, incluyendo números telefónicos.
- Contratos especiales de soporte y mantenimiento.
Discutir y confirmar los requerimientos de software de aplicaciones.

5.4.1.3. DETERMINAR REQUERIMIENTOS DE RECURSOS DE TELECONUNICACIONES.

Determinar las facilidades de comunicación usadas en completar los procesos críticos automatizados para la organización, registrar detalles sobre el uso, configuración y requerimientos.

Las comunicaciones son vitales para proveer un ambiente para los procesos en condiciones de recuperación. Esta recuperación de comunicaciones es muy compleja, particularmente donde las líneas de comunicación, protocolos y otros componentes son diferentes a los usados en condiciones normales de operación.

Si las comunicaciones no pueden ser restauradas correctamente para permitir la transferencia de información con el centro de recuperación, ésta no podrá ser realizada.
Considerar cuidadosamente todos los requerimientos de comunicaciones.

IDENTIFICAR COMUNICACIONES INVOLUCRADAS EN PROCESOS CRITICOS.

Identificar cada tipo de comunicación usadas en la organización. Esto deberá incluir todas las posibles comunicaciones de voz y datos, por ejemplo teléfono, correo, fax, red y otros servicios.

DOCUMENTAR COMUNICACIONES REQUERIDAS PARA PROCESOS EN CONDICIONES DE RECUPERACION.

Documentar la mínima configuración de telecomunicaciones, asegurando que se encuentren plasmados los requerimientos extras.

Para cada comunicación a ser usada en la recuperación de procesos, documentar como es usada y la siguiente información:

- Configuración de equipo de telecomunicaciones, incluyendo multiplexores, concentradores, dispositivos de diagnóstico, módems y controladores de telecomunicaciones.
- Especfficaciones de líneas de telecomunicación incluyendo posibles consideraciones de interferencia, largas distancia, diferentes telefonos, transmisión vía sátelite y costo de transmisión.
- Descripciones de velocidad, frecuencia, amplitud de banda y números de circuito de identificación de canales de comunicación.

-Protocolos de comunicaciones usados.

-Software de comunicaciones usados, (incluyendo nombre, descripción, versión, y fecha de última modificación).

-Diagnóstico de utilerías de software.

-Un mapa de las redes de comunicación.

Esta información deberá ser documentada para todos los servicios de comunicaciones. Incluyendo servicios de teléfono, fax, redes de microcomputadoras (LAN, WAN).

La documentación deberá incluir calendarios y tiempos como:

-Calendario de frecuencia.
-Tiempos de espera.
-Tiempos de comunicación.

DOCUMENTAR REQUERIMIENTOS DE TELECOMUNICACIONES.

Para cada tipo de comunicación a ser usada, documentar los requerimientos de los componentes, considerando:

- Utilerías usadas en la conexión de cable físico.
- Utilerías usadas en diagnóstico de telecomunicaciones.
- Suministro de energía.
- Posibles orígenes de interferencia externa y medidas para prevenir cada interferencia.
- Servicios externos que pueden ser utilizados para completar las comunicaciones.
- Hardware de computadoras requerido para la comunicación.

IDENTIFICAR PROVEEDORES PARA COMUNICACIONES USADAS EN PROCESOS EN CONDICIONES DE RECUPERACION.

Para todos los equipos de comunicaciones, software y servicios usados en procesos críticos automatizados de la organización, identificar los proveedores y servicios externos ó personal con experiencia en el tipo de comunicación, así como:

-Cada dispositivo de comunicación.
-Detalles, incluyendo teléfonos.
-Detalles de contratos.
-Algunos acuerdos especiales.

Discutir y confirmar los requerimientos de comunicaciones.

5.4.1.4. DETERMINAR REQUERIMIENTOS DE RECURSOS DE SOFTWARE DE SISTEMAS.

Determinar el software de sistemas que soporta las aplicaciones usadas en la terminación de procesos críticos para la organización y registrar los detalles para su uso, configuración, y requerimientos de cada software.

Con está información se determina la configuración mínima del software requerida en la operación de procesos críticos automátizados en condiciones de recuperación.

IDENTIFICAR EL SOFTWARE INVOLUCRADO EN PROCESOS CRITICOS.
Identificar todo el software utilizado en la organización. Estimar el espacio en disco requerido para almacenar todo el software de sistemas.

Un registro completo del hardware usado en la organización deberá ser usado para asegurarse de que no exista alguna pérdida.

Considerar todas las aplicaciones soportadas, los ambientes, mainframes, minicomputadoras y microcomputadoras. Incluir software usado en las comunicaciones y utilerías requeridas para operar cada sistema.

DOCUMENTAR SOFTWARE DE SISTEMAS REQUERIDO PARA PROCESOS EN CONDICIONES DE RECUPERACION.
Un inventario de todo el software necesario para correr los procesos críticos automátizados deberá ser documentado, incluyendo:
- Configuración, sistema operativo, procesadores de transacciones, manejadores de base de datos, librerías, controladores de telecomunicaciones y compiladores.
- Parámetros del ambiente requeridos para cada aplicación.
- Software de seguridad necesario para la protección y control del acceso a los datos.
- Versiones y fechas de la última modificación.
- Aplicaciones soportadas.
- Detalles de alguna comunicación con otros sistemas.

La documentación deberá incluir calendario y tiempos.

DOCUMENTAR REQUERIMIENTOS DE SOFTWARE DE SISTEMAS.
Para cada sistema usado en la operación de procesos críticos automatizados para la organización en condiciones de recuperación, documentar los requerimientos mínimos considerando:
- Seguridad
- Requerimientos de respaldo
- Hardware
- Algún otro requerimiento especial
- Comunicaciones

IDENTIFICAR PROVEEDORES DE SOFTWARE DE SISTEMAS USADOS EN PROCESOS EN CONDICIONES DE RECUPERACION.

Para cada sistema usado en procesos críticos automatizados identificar el proveedor principal, con dos alternativos y algun servicio de soporte externo o personal con experiencia en el software de sistemas.
Para cada proveedor listar:

- El software de sistemas.
- Detalles de contactos, incluyendo teléfonos personales.
- Soporte técnico del software.
- Tiempos de espera.
- Contratos especiales.

Discutir y confirmar los requerimientos de software de sistemas.

5.4.1.5. DETERMINAR REQUERIMIENTOS DE RECURSOS MATERIALES.

Determinar los recursos materiales usados en procesos críticos automatizados de la organización, detalles sobre su uso, especfficaciones y sus requerimientos.

Identificar todas las entradas y salidas de recursos materiales consumibles usados en los procesos automatizados de la organización Considerar:

- Suministros de aplicación especfficos incluyendo formas preimpresas.
- Suministros que soportan las operaciones, incluyendo cintas magnéticas, paquetes de discos, papel stock y cinta de impresora.
- Algún requerimiento particular.

Una reserva de recursos materiales es necesaria para procesos de alta prioridad en las operaciones automatizadas. Cada reserva necesitada deberá ser definida y documentada.

Es recomendable que los stocks de reserva de recursos materiales por largos tiempos o grandes vólumenes sean almacenados en diferentes lugares.

Desde la recolección de información algunos de los recursos materiales necesarios deberán ser identificados.

IDENTIFICAR RECURSOS MATERIALES INVOLUCRADOS EN PROCESOS CRITICOS.

Revisar los pasos requeridos para cada proceso e identificar cada recurso material usado. Para cada tipo de recurso material determinar las funciones en las cuales es usado. Determinar el mfnimo de recursos materiales requeridos para soportar los procesos crfticos en condiciones de recuperación.

DOCUMENTAR LOS RECURSOS MATERIALES PARA PROCESOS EN CONDICIONES DE RECUPERACION.

Será necesario obtener información sobre la provisión, almacenamiento, y control del promedio consumible en el centro de cómputo. Esto deberá incluir documentación de cada proceso y de cada recurso material usado con la siguiente información:

- Rango y tipo de lugares de cómputo usados.
- Espacio de almacenamiento usado.
- Condiciones especiales de almacenamiento.
- Necesidades de transportación ffsica.

Identificar los lugares de stocks de reservas y documentar los procedimientos para las pruebas de cantidades suficientes y el reordenamiento de recursos materiales.

DOCUMENTAR REQUERIMIENTOS DE RECURSOS MATERIALES.

Para cada recurso material usado en la operación de procesos crfticos automatizados de la organización, documentar:

- La aplicación en la cual el recurso material es usado.
- El proceso soportado por este recurso material.

- Algún equipo involucrado directamente en la salida del recurso material usado (algún tipo de impresora).
- Precauciones de seguridad necesarias para proteger los recursos materiales.
- Requerimientos específicos de algún recurso material(numeración consecutiva).

IDENTIFICAR PROVEEDORES DE RECURSOS MATERIALES USADOS EN LOS PROCESOS EN CONDICIONES DE RECUPERACION.

Para cada recurso material registrar e identificar al proveedor principal y si es posible a dos proveedores alternativos. Para cada proveedor listar:

- Detalles de contacto incluyendo teléfonos personales.
- Costos.
- Acuerdos para lugares alternativos.
- Tiempos de espera.

Documentar detalles sobre el almacenamiento fuera de las instalaciones incluyendo tiempos de acceso.

Discutir y confirmar los requerimientos de recursos materiales.

5.4.1.6. DETERMINAR REQUERIMIENTOS DE RECURSOS DE REGISTROS VITALES.

Determinar qué registros de la organización son vitales para completar los procesos críticos de la organización y detalles sobre el almacenamiento y uso de cada registro.

La mayoría de los registros vitales involucrados en aplicaciones críticas serán aquellos almacenados en computadora. Son generalmente del tipo que no puede ser reconstruido en un corto período de tiempo. Muchos de estos requieren de un respaldo instantáneo.

Algunos registros pueden ser requeridos por asuntos legales y deben ser considerados vitales.

IDENTIFICAR REGISTROS VITALES INVOLUCRADOS EN PROCESOS CRITICOS DE LA ORGANIZACION.

Identificar todos los registros vitales almacenados para aplicaciones críticas automatizadas, esto puede incluir casos como información de deudores, información de créditos, contratos y registros de pago.

Una copia del respaldo de todos los datos vitales automatizados deberá ser almacenado en un lugar externo de respaldo(OFF SITE).

DOCUMENTAR REGISTROS VITALES REQUERIDOS PARA PROCESOS EN CONDICIONES DE RECUPERACION.

Para todos los registros vitales usados en procesos críticos automatizados de la organización, realizar una lista de los lugares en donde se encuentran para los originales y copias. Deberá ser establecida la información requerida sobre el control de cintas mágneticas y discos incluyendo:

- El número de cintas y discos para el uso de archivos específicos.
- Cómo y Dónde las cintas y discos son almacenados.
- Procedimientos para el control de movimiento de cintas y discos entre el centro de cómputo y otras áreas de almacenamiento.
- Facilidades para la localización de archivos específicos en su respectiva cinta o disco.

Clasificar los registros vitales en formas numeradas así como los documetos de entrada del software. Determinar para cada proceso el mínimo de registros vitales requeridos para soportar los procesos en condiciones de recuperación.

DOCUMENTAR LOS REQUERIMIENTOS DE REGISTROS VITALES.

Para cada tipo de registro vital, determinar algunos otros requerimientos incluyendo seguridad, ambiente y software requerido para manipular los datos.

Documentar algunos requerimientos de seguridad de los datos vitales que son requeridos legalmente.

Discutir y confirmar los requerimientos de registros vitales.

5.4.1.7. DETERMINAR REQUERIMIENTOS DE RECURSOS DE EQUIPO

Determinar todo el equipo necesario para operar procesos crfticos.

Debera ser preparada un inventario completo del equipo necesario para la operación de los procesos debe ser preparado.

La mayoría del equipo usado en las operaciones deberá ser hardware y periféricos.

IDENTIFICAR EL EQUIPO INVOLUCRADO EN LOS PROCESOS.

Deberá ser documentada información del hardware y la correspondiente configuración deberá ser documentada. Incluyendo CPUs controladores drives de disco, drives de cintas, terminales, impresoras y otros periféricos.

Considerar el ambiente de mainframe y minicomputadoras. Determinar el mfnimo de equipo requerido para soportar los procesos en condiciones de recuperación.

DOCUMENTAR EL EQUIPO REQUERIDO PARA PROCESOS EN CONDICIONES DE RECUPERACION.

Un inventario del equipo deberá formar parte del plan de recuperación, esté podrá ser usado para identificar rápidamente equipos para ser remplazados o para restaurarse.

Para cada parte del equipo incluir en el inventario:

- Descripción
- Una lista de procesos crfticos soportados por el equipo
- Las funciones del equipo
- Especificaciones incluyendo marca, número de módelo, número de serie y medidas.
- Calendario de mantenimiento y reemplazamiento de piezas.

El inventario deberá involucrar hardware y tambien documentar:

- Configuración.
- Total de espacio en disco requerido.
- Impresoras y periféricos.
- Puertos de comunicación.
- Procesadores de telecomunicaciones.
- Línea controladora y modem.
- Número de líneas.

Algunas partes del equipo pueden ser usadas en más de un proceso.

DOCUMENTAR REQUERIMIENTOS DEL EQUIPO.

Para cada equipo a ser usado en la operación de procesos crfticos automatizados en condiciones de recuperación se deberá tener una lista de requerimientos adicionales como:

- Equipo de soporte.
- Requerimientos de espacio, luz y aire acondicionado.
- Requerimientos de seguridad.
- Ambiente incluyendo (ventilación, temperatura y humedad.)

IDENTIFICAR PROVEEDORES PARA EL EQUIPO USADO PARA PROCESOS EN CONDICIONES DE RECUPERACION.

Para cada parte del equipo identificada determinar un proveedor principal y dos alternativos, listar:
- Cada pieza de equipo necesaria
- Detalles de contacto incluyendo teléfonos personales
- Tiempos de espera de recursos materiales
- Algunos otros acuerdos

Discutir y confirmar los requerimientos de equipo.

5.4.1.8. DETERMINAR REQUERIMIENTOS DE RECURSOS DE PERSONAL

Determinar el personal requerido para operar los procesos críticos automatizados de la organización, sus funciones en los procesos de su departamento.

Los departamentos críticos son compuestos del mínimo número de personal apropiado, capaz de operar los procesos y tener decisión y autoridad para organizar y conducir cada operación.

El coordinador de la operación de la organización podrá supervisar a todo el personal durante los procesos de recuperación y operaciones en condiciones de recuperación.

IDENTIFICAR AL PERSONAL INVOLUCRADO EN LOS PROCESOS CRITICOS DE LA ORGANIZACION.

Es requerida información sobre el personal de la organización, por cada individuo se deberá incluir descripciones de trabajo y detalles de contacto.

Identificar la distancia de cada persona de su casa a la organización o sitio de recuperación porque puede ser relevante.

Si están siendo considerados los procesos manuales como una alternativa de procesos automatizados, puede ser requerido personal extra para completar cada proceso.

DOCUMENTAR EL PERSONAL REQUERIDO PARA PROCESOS EN CONDICIONES DE RECUPERACION.

Determinar el personal responsable para cada proceso crítico automatizado.

Documentar las funciones de cada individuo:
- Nombre.
- Puesto.
- Descripción del Puesto.
- Detalle de contactos.
- Sus procedimientos operativos diarios.
- Problemas o dificultades.

DEFINIR COMPOSICION DE GRUPOS DE DEPARTAMENTOS CRITICOS.

Revisar los departamentos críticos requeridos y definir la composición de cada uno de los grupos del departamento. Cada grupo deberá tener un líder y un suplente definido.

Tomar en cuenta que los empleados involucrados en operaciones bajo condiciones de recuperación podrán ser requeridos para trabajos por largas horas.

DOCUMENTAR REQUERIMIENTOS DE PERSONAL DE GRUPOS DE DEPARTAMENTOS CRITICOS.

El personal identificado para operar los procesos críticos en condiciones de recuperación pueden tener requerimientos que no existen durante las operaciones normales.

Determinar la extensión de los requerimientos para el personal de recuperación como:

- Ubicación.
- Transporte.
- Seguridad.

Es necesario proveer equipo especial para empleados quienes trabajan en situaciones peligrosas.

Discutir y confirmar los requerimientos de personal.

5.4.1.9. DETERMINAR REQUERIMIENTOS DE RECURSOS DE TRANSPORTE

Identificar el tipo de transporte requerido para completar los procesos críticos automatizados de la organización.

Deberá ser preparado un inventario de vehículos alternativos.

IDENTIFICAR TRANSPORTES INVOLUCRADOS EN PROCESOS CRITICOS DE LA ORGANIZACION.

Identificar cada tipo de transporte usado en la organización.

DOCUMENTAR TRANSPORTES REQUERIDOS PARA PROCESOS EN CONDICIONES DE RECUPERACION.

Para cada vehículo a ser usado en la operación de procesos críticos, registrar lo siguiente:

- Marca, módelo y año del vehículo.
- Descripción, color, tipo de vehículo y otras características.
- Número de registro y fecha de renovación.
- Capacidad de carga.
- Gasolina apropiada.

Documentar detalles de algún servicio de transporte especial usado en la operación de procesos críticos.

DOCUMENTAR REQUERIMIENTOS DE TRANSPORTES.

Para cada vehículo usado en los procesos críticos en condiciones de recuperación documentar los requerimientos considerando:

- Almacenamiento de los vehículos por razones de seguridad.
- Medidad físicas de los vehículos.
- Personal con licencia de manejo adecuada.

IDENTIFICAR PROVEEDORES PARA TRASPORTES USADOS EN PROCESOS EN CONDICIONES DE RECUPERACION.

Identificar los proveedores para cada tipo de vehículo usado.

Documentar lugares, números de teléfono y otros detalles sobre diferentes centros de servicio para mantenimiento y recuperación.

Discutir y confirmar los requerimientos de transporte.

5.4.1.10. DETERMINAR REQUERIMIENTOS DE UTILERIAS

Determinar las utilerías necesarias para soportar los procesos críticos automatizados de la organización.

Hay muchas utilerías que soportan hardware, software, comunicaciones y personal, (como por ejemplo: teléfono y comunicaciones de datos).

Como regla general, todas las utilerías en el centro de cómputo, deberán tener el mismo nivel de protección.

IDENTIFICAR UTILERIAS INVOLUCRADAS EN PROCESOS CRITICOS.

Identificar cada tipo de utilería usadas en la organización, así como algunas especificaciones para estas utilerías.

DOCUMENTAR UTILERIAS REQUERIDAS PARA PROCESOS EN CONDICIONES DE RECUPERACION.

Documentar la configuración y recursos materiales para cada utilería usadas en la operación de procesos crfticos automatizados de la organización.

Documentar información relatando el uso de utilerías que soportan procesos crfticos automatizaqdos de la organización.

DOCUMENTAR REQUERIMIENTOS DE UTILERIAS.

Documentar algún lugar ó ambiente para las utilerías.
Algunos ejemplos de requerimientos de utilerías son:
- Unidad de aire acondicionado separada del resto de la organización.
- Tomas de aguas localizadas en la proximidad del centro de cómputo.

IDENTIFICAR PROVEEDORES DE UTILERIAS USADAS EN PROCESOS BAJO CONDICIONES DE RECUPERACION.

Identificar los proveedores de las utilerías usadas para soportar las o procesos crfticos automatizados de la organización en condiciones de recuperación.

Tambien identificar alguna alternativa de emergencia.

Discutir y confirmar los requerimientos de utilerías.

5.4.1.11. DETERMINAR REQUERIMIENTOS DE RECURSOS DE ESPACIO OFICINA/INDUSTRIA.

Determinar el espacio mfnimo requerido de oficina e industria para las operaciones de todos los procesos crfticos automatizados en condiciones de recuperación.

Basado en todos los requerimientos previos a la recuperación determinados durante está fase, el número de oficinas requeridas, el espacio necesario deberá ser determinado y documentado.

IDENTIFICAR ESPACIO OFICINA/INDUSTRIA INVOLUCRADO EN LOS PROCESOS CRITICOS DE LA ORGANIZACION.

Identificar la medida y tipo del espacio oficina e industria necesario para acomodar los requerimientos de procesos crfticos automatizados bajo condiciones de recuperación considerando:
- Número de máquinas.
- Ambiente de máquinas.

DOCUMENTAR EL ESPACIO REQUERIDO PARA OFICINA E INDUSTRIA EN PROCESOS EN CONDICIONES DE RECUPERACION

Documentar la medida de espacios comunes requeridos para ambos. oficina e industria, incluyendo el centro de procesamiento de datos.

Considerar alternativas para otros requerimientos tal como equipo usado en operaciones de oficina para reducir al mfnimo el espacio requerido.

También documentar el tipo de caracterfsticas requeridas en cada espacio tal como:
- Número y tipo de lfneas telefonicas.
- Número de personal de cada espacio.
- Requerimientos de seguridad.
- Areas especiales de almacenamiento.
- Sonido requerido para prevenir la interrupción.
- Alguna protección especial de energfa eléctrica.
- Cableado y otros requerimientos de red.

DOCUMENTAR REQUERIMIENTOS DE ESPACIO OFICINA/INDUSTRIA

En la consideración del espacio oficina/industria requerido tambien considerar accesos de seguridad a la construcción requerida en el centro de recuperación.

Discutir y confirmar requerimientos de espacio oficina/industria.

5.4.1.12 PREPARAR DOCUMENTACION DE REQUERIMIENTOS MINIMOS

Preparar la documentación como "Configuración Mfnima" requerida para las operaciones de procesos crfticos automatizados de la organización en condiciones de recuperación.

RECOLECTAR INFORMACION SOBRE LA CONFIGURACION MINIMA PARA TODOS LOS PROCESOS AUTOMATIZADOS.

Para cada tipo de requerimiento considerar la documentación para cada aplicación necesaria automatizada.

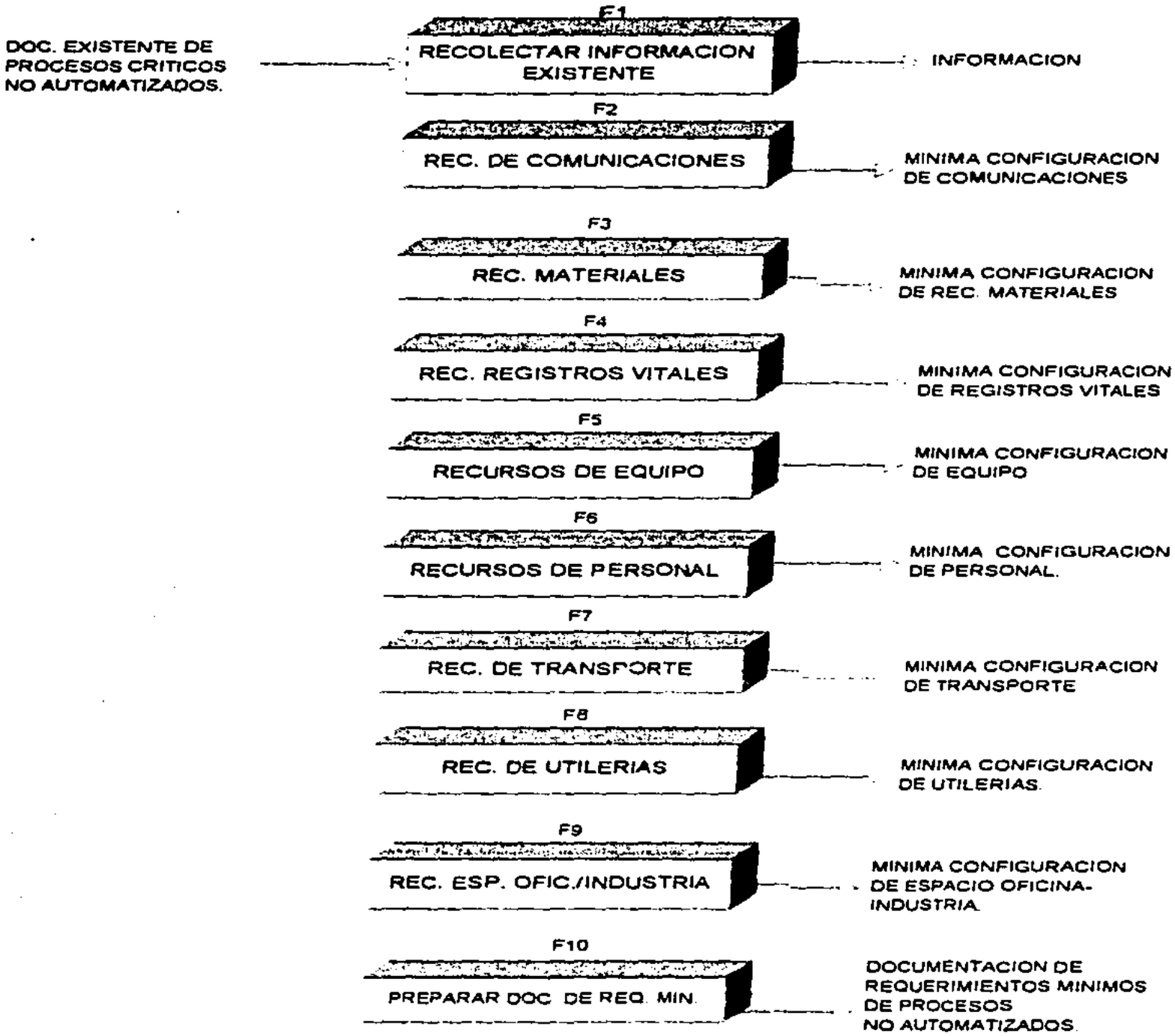
El Coordinador de la recuperación de la organización deberá revisar la información recolectada para la consistencia y determinar algunos requerimientos mfnimos de recuperación que hayan sido omitidos.

Discutir y acordar la mfnima configuración y resolver algunas dudas para seleccionar los requerimientos de configuaración mfnima. Si es necesario preparar una lista para modificaciones.

TABLA SUGERIDA DE CONTENIDO:
REQUERIMIENTOS MINIMOS

Introducción
1. Resumén de recolección de la información
2. Software de aplicación
3. Comunicaciones
4. Software de Sistemas
5. Recursos materiales
6. Registros vitales
7. Equipo
8. Personal
9. Transporte
10. Utilerfas
11. Espacio Oficina/Industria
Apendices

FASE F. RECURSOS MINIMOS DE RECUPERACION DE PROCESOS NO AUTOMATIZADOS. RELACION DE TAREAS.



5.4.2. RECURSOS MINIMOS DE RECUPERACION (PROCESOS NO AUTOMATIZADOS).

Identificar en detalle, los recursos requeridos para operar los procesos críticos no automatizados de la organización en condiciones de recuperación.

Deben ser determinados los requerimientos de recursos en condiciones de emergencia.

Hay dos fases involucradas en la recuperación de una interrupción de la organización:

- Preparación del sitio de recuperación
- Operación de procesos críticos y necesarios en condiciones de recuperación.

Verificar la fecha en que la documentación fue preparada, esto puede ser relevante si los procedimientos tienen cambios sin que la documentación sea modificada.

SUMARIO

ENTRADAS: Requerimientos existentes/Documentación de Procedimientos.
Procesos críticos y necesarios del negocio no automatizados.

TAREAS: Recolectar información existente.
Determinar requerimientos de recursos de Comunicaciones.
Determinar requerimientos de recursos materiales.
Determinar requerimientos de recursos de registros vitales.
Determinar requerimientos de recursos de equipo.
Determinar requerimientos de recursos de personal.
Determinar requerimientos de recursos de transportes.
Determinar requerimientos de recursos de utilerías.
Determinar requerimientos de recursos oficina/industria.
Preparar la documentación de requerimientos mínimos.

PRODUCTOS Información obtenida en discusiones.
Configuración mínima de comunicaciones.
Configuración mínima de recursos materiales.
Configuración mínima de registros vitales.
Configuración mínima de equipo.
Configuración mínima de personal.
Configuración mínima de transporte.
Configuración mínima de utilerías.
Configuración mínima de espacio oficina/industria.

FASE A LIBERAR: Documentación de requerimientos mínimos para procesos no automatizados.

5.4.2.1. RECOLECTAR INFORMACION EXISTENTE

Reducir el tiempo para identificar los requerimientos mínimos de configuración para procesos no automatizados en condiciones de recuperación.

Determinar si la información requerida ha sido documentada en:

- Planes de emergencia.
- Lista de recursos materiales.
- Inventario de equipos.
- Contratos de mantenimiento.

- Estrategias de respaldo usadas.
- Procedimientos en operación normal.

El coordinador de la recuperación de la organización deberá asistir en la selección del personal involucrado en la recolección de información.

ASIGNAR PERSONAL PARA LA RECOLECCION DE LA INFORMACION.

Determinar y documentar el personal apropiado, asegurarse que el personal asignado a la tarea este capacitado en la recoleción de información, de otro modo el proceso puede ser ineficiente.

REVISAR LA RELEVANCIA DE LA INFORMACION EXISTENTE.

Revisar la fecha en que la documentación fue preparada, está puede ser irrelevante si los procedimientos han cambiado sin que la documentación sea modificada.

ACORDAR SESIONES DE DISCUSION CON EL PERSONAL PARA CONFIRMAR LOS REQUERIMIENTOS MINIMOS.

Por cada requerimiento de recursos, acordar sesiones de discusión con personal apropiado, individuales o sesiones de grupo para identificar el mínimo de requerimientos para operaciones en condiciones de recuperación.

5.4.2.2. DETERMINAR REQUERIMIENTOS DE RECURSOS DE COMUNICACIONES

Determinar las facilidades de comunicación usadas en la terminación de procesos crfticos no automatizados y detalles de registros sobre el uso, configuración y requerimientos.

Las comunicaciones son vitales para proveer el ambiente recomendable para tranferir información en aplicaciones crfticas no automatizadas.

Es importante la atención a detalle de todos los requerimientos de comunicación.

La información involucrada de procesos crfticos no automatizados deberá ser documentada tal como son usadas las comunicaciones en los procesos, comunicación provista a otros sistemas o servicios y todo lo referente a entradas y salidas.

Con esta información el mínimo de facilidades de comunicaciones requeridas son determinadas.

IDENTIFICAR COMUNICACIONES INVOLUCRADAS EN PROCESO CRITICOS NO AUTOMATIZADOS.

Identificar cada tipo de comunicación usada en la organización, como telefono, correo de voz, fax, y otros servicios.

Identificar todas las entradas, salidas, el vólumen, frecuencia y los requerimientos básicos.

Con esta información determinar los procesos en los cuales las facilidades de comunicación son esenciales para soportar el proceso en condiciones de recuperación.

DOCUMENTAR COMUNICACIONES REQUERIDAS PARA PROCESOS EN CONDICIONES DE RECUPERACION

Determinar que procesos podrán requerir facilidades de comunicación en condiciones de recuperación.

Revisar que todos los requerimientos extras sean documentados, tambien considerar los efectos de fallas en las lfneas de comunicación.

Documentar la siguiente información:
- Configuración del equipo de comunicación.
- Especificaciones de lfnea de comunicación (incluyendo posibles interferencias externas y costos de transmisión).
- El número de transferencias soportadas.
- Un mapa de la red de comunicación.

Está información deberá ser documentada considerando el uso de comunicaciones vía satélite o teléfonos celulares así como incluir calendario y tiempos:
- Frecuencia (diario, semanal, mensual)
- Tiempos de espera por diferencias de tiempo internacional y restricciones de horas de servicio.
- Tiempo de comunicación con otros sistemas.

Para cada tipo de comunicación determinar que seguridad es requerida considerando:
- Protección física de cableado.
- Protección de dispositivos.
- Suministros de energía.
- Protección de accesos.
- Documentación describiendo procedimientos de servicio de comunicaciones.

DOCUMENTAR REQUERIMIENTOS DE COMUNICACIONES

Para cada tipo de comunicación usada documentar los requerimientos de los componentes considerando:

- Herramientas usadas en la conexión física de cables
- Utilerías usadas en diagnósticos de comunicaciones
- Posibles orígenes de interferencia externa y medidas para prevenirla.

Considerar el acceso requerido para operaciones en condiciones de recuperación en estos servicios.

IDENTIFICAR PROVEDORES DE COMUNICACIONES USADOS EN PROCESOS EN CONDICIONES DE RECUPERACION.

Para todos los equipos de comunicación y servicios usados en procesos críticos no automatizados de la organización, identificar los proveedores y dos alternativas posibles así como servicios de soporte externo y personal con experiencia en las comunicaciones, por cada proveedor listar:
- Cada dispositivo de comunicación o servicio.
- Detalle de contactos incluyendo teléfonos personales.
- Soporte técnico relativo a comunicaciones.
- Teléfono de la compañía, teléfono de emergencia y detalles del contrato.
- Otros proveedores del equipo de comunicaciones.
- Contactos para aprobación del tendido de cables y servicios de conexión.

ACORDAR SESIONES DE DISCUSION CON EL PERSONAL PARA CONFIRMAR LOS REQUERIMIENTOS MINIMOS.

Por cada requerimiento de recursos, acordar sesiones de discusión con personal apropiado, individuales o sesiones de grupo para identificar el mínimo de requerimientos para operaciones en condiciones de recuperación.

5.4.2.3. DETERMINAR REQUERIMIENTOS DE RECURSOS MATERIALES

Determinar recursos materiales esenciales para completar los procesos críticos no automatizados y registrar detalles sobre sus especificaciones y requerimientos.

Considerar una reserva de recursos materiales necesaria para procesos prioritarios, la cual deberá ser definida y documentada.

Con esta información recolectada identificar los recursos materiales involucrados en la operación de procesos no automatizados.

IDENTIFICAR RECURSOS MATERIALES INVOLUCRADOS EN PROCESOS CRITICOS NO AUTOMATIZADOS DE LA ORGANIZACION.

Identificar todos los recursos materiales usados en todos los procesos no automatizados de la organización.

Para cada recurso material determinar la función de la organización en la cual es usado.

DOCUMENTAR RECURSOS MATERIALES REQUERIDOS PARA PROCESOS EN CONDICIONES DE RECUPERACION.

Obtener información documentando la provisión de almacenamiento y control de estos recursos materiales.

Está documentación deberá incluir en que proceso es usado cada recurso material, incluyendo la siguiente información:

- Espacio de almacenamiento usado.
- Condiciones especiales de almacenamiento.
- Necesidades ffsicas de transportación.

Para cada recurso material documentar donde son localizados los stocks de reserva y como pueden ser accesados. Documentar los procedimientos para regular las cantidades, los cuales pueden tener un tiempo máximo de almacenamiento.

La documentación sobre proveedores deberá incluir:

1. Tiempos de espera para nuevas ordenes
2. Fecha de suministro normal
3. Vólumenes de consumibles usados en cada proceso y la frecuencia con la cual son usados
4. Máxima espera aceptable de un proveedor

DOCUMENTAR REQUERIMIENTOS DE RECURSOS MATERIALES

Por cada recurso material usado en la operación de procesos crfticos no automatizados en condiciones de recuperación, documentar:

- El proceso soportado por el recurso material.
- Los pasos particulares de un proceso en el cual el recurso material es usado.
- Precauciones de seguridad necesarias para proteger el recurso material almacenado.
- Requerimientos especfficos de algún recurso material.

IDENTIFICAR PROVEEDORES DE RECURSOS MATERIALES USADOS EN PROCESOS BAJO CONDICIONES DE RECUPERACION

Para cada recurso material registrado identificar el proveedor principal y dos alternativos si es posible, por cada uno listar:

- Detalles de contacto, incluyendo teléfonos personales.
- Costos.
- Detalles del contrato.
- Tiempos de espera.

ACORDAR SESIONES DE DISCUSION CON EL PERSONAL PARA CONFIRMAR LOS REQUERIMIENTOS MINIMOS.

Por cada requerimiento de recursos, acordar sesiones de discusión con personal apropiado, individuales o sesiones de grupo para identificar el mínimo de requerimientos para operaciones en condiciones de recuperación.

5.4.2.4. DETERMINAR REQUERIMIENTOS DE RECURSOS DE REGISTROS VITALES

Determinar que registros de la organización son vitales para completar los procesos críticos no automatizados de la organización, y detalles sobre el almacenamiento y uso de cada registro.

Los registros vitales son generalmente del tipo que no pueden ser reconstruidos en un corto período de tiempo. Muchos de estos registros pueden requerir respaldo instantáneo y períodicos almacenamientos externos a la organización.

IDENTIFICAR REGISTROS VITALES INCOLUCRADOS EN PROCESOS CRITICOS DE LA ORGANIZACION.

Identificar todos los registros vitales almacenados en todos los procesos críticos no automatizados considerando cuidadosamente los pasos en cada proceso.

Una copia del respaldo de todos los registros vitales no automatizados debe ser almacendo en un lugar externo (off-site).

DOCUMENTAR REGISTROS VITALES REQUERIDOS PARA PROCESOS EN CONDICIONES DE RECUPERACION.

Por cada registro vital incluir detalles del lugar de almacenamiento externo (off-site) y como pueden ser accesados los registros.

Con esta información determinar el mínimo de registros vitales requeridos para soportar el proceso bajo condiciones de recuperación. Por cada registro vital documentar:

- Descripción.
- Procesos soportados por los registros.
- Lugar usual de registros vitales.

DOCUMENTAR REQUERIMIENTOS DE REGISTROS VITALES

Por cada registro vital documentar algún otro requerimiento incluyendo:

- Precauciones de seguridad necesarias
- Requerimientos de ambiente
- Espacio requerido de almacenamiento
- Equipo requerido para hacer uso de los registros vitales.

ACORDAR SESIONES DE DISCUSION CON EL PERSONAL PARA CONFIRMAR LOS REQUERIMIENTOS MINIMOS.

Por cada requerimiento de recursos, acordar sesiones de discusión con personal apropiado, individuales o sesiones de grupo para identificar el mínimo de requerimientos para operaciones en condiciones de recuperación.

5.4.2.5. DETERMINAR REQUERIMIENTOS DE RECURSOS DE EQUIPO

Determinar que equipo es necesario para la recuperación de procesos críticos no automatizados, incluyendo configuración del equipo y recursos materiales.

Preparar un inventario completo del equipo necesario para soportar los procesos no automatizados.

Por cada pieza de equipo involucrada obtener información sobre las especfficaciones, calendario de mantenimiento, utilerías, recursos materiales, y requerimientos de ambiente para ser documentados.

IDENTIFICAR EL EQUIPO INVOLUCRADO EN PROCESOS CRITICOS DE LA ORGANIZACION.

Revisar los pasos requeridos en la operación de cada proceso crítico no automatizado de la organización y considerar cada pieza de equipo usado.

Con está información determinar el mínimo de equipo requerido para soportar los procesos en condiciones de recuperación.

DOCUMENTAR EL EQUIPO REQUERIDO PARA PROCESOS EN CONDICIONES DE RECUPERACION

Preparar un inventario del equipo involucrado en la recuperación, esté inventario formará parte del plan.

Por cada tipo de equipo incluido en el inventario considerar:
- Descripción del equipo.
- Una lista de procesos crfticos en las que se usa.
- Las funciones del equipo en los procesos.
- Especfficaciones incluyendo marca, número de serie, modelo, medida y algunas caracterfsticas especiales.
- Cumplimiento de requerimientos del gobierno.
- Calendario de mantenimiento.

Algunas partes del equipo pueden ser usadas en más de un proceso crftico.

DOCUMENTAR REQUERIMIENTOS DEL EQUIPO.

Para el equipo a ser usado en la recuperación de procesos crfticos no automatizados en condiciones de recuperación, también hacer una lista de adicionales como:

-Equipo de soporte.
-Suministros de mantenimiento.
-Espacio requerido.
-Requerimientos de ambiente.
-Precauciones de seguridad requerida.

IDENTIFICAR PROVEEDORES PARA EL EQUIPO USADO EN PROCESOS EN CONDICIONES DE RECUPERACION.

Para cada parte del equipo identificado para uso en la operación de procesos crfticos no automatizados en condiciones de recuperación, identificar un proveedor principal y dos alternativos si es posible. Por cada proveedor listar:

-Cada pieza de equipo suministrada
-Detalles de contacto, incluyendo teléfonos personales.
-Tiempos de espera.
-Detalles de contratos.
-Algunos acuerdos especiales.

Se deberá incluir una lista de transportes especiales requeridos para mover el equipo.

ACORDAR SESIONES DE DISCUSION CON EL PERSONAL PARA CONFIRMAR LOS REQUERIMIENTOS MINIMOS.

Por cada requerimiento de recursos, acordar sesiones de discusión con personal apropiado, individuales o sesiones de grupo para identificar el mínimo de requerimientos para operaciones en condiciones de recuperación.

5.4.2.6 DETERMINAR REQUERIMIENTOS DE RECURSOS DE PERSONAL

Determinar el personal que es requerido para operar los procesos críticos no automatizados, sus funciones en los procesos y la composición de los departamentos críticos.

Deberá ser documentada información general de cada persona involucrada en la operación de procesos no automatizados de la organización, sus descripciones, responsabilidades y detalles de contactos.

Con esta información determinar el personal a ser involucrado en la recuperación de procesos críticos y necesarios no automatizados en el evento de desastre.

Sugerir departamentos críticos que deberán ser definidos. Deberán estar compuestos del número mínimo de gente apropiada capaz de operar los procesos críticos no automatizados en condiciones de recuperación.

IDENTIFICAR PERSONAL INVOLUCRADO EN PROCESOS CRITICOS DE LA ORGANIZACION.

Requerir información sobre el personal de la organización es requerida, por cada individuo incluir descripción y detalles de contacto.

Recordar que la distancia de cada persona de su casa al lugar de recuperación puede ser relevante.

Identificar el personal en cada departamento durante operaciones normales, e identificar las funciones que ellos realizarán.

DOCUMENTAR PERSONAL REQUERIDO PARA PROCESOS EN CONDICIONES DE RECUPERACION.

Identificar qué personal está involucrado en la operación de procesos críticos no automatizados y cuales son esenciales para la recuperación considerando sus responsabilidades.

Determinar a la persona responsable para la operación de recuperación de cada proceso.

Por cada persona identificada como involucrada en el soporte de la operación de procesos críticos no automatizados, registrar lo siguiente:

-Nombre
-Descripción del puesto.
-Detalles de contacto.

Elaborar una lista del personal requerido para realizar operaciones de recuperación y las funciones que ellos completarán.

La recuperación de equipo sofisticado puede requerir asistencia técnica. Indicar que pasos deben ser completados por el personal en la organización y cuales requieren personal externo de soporte.

Documentar nombres, teléfonos y funciones del personal de soporte técnico.

DEFINIR COMPOSICION DE DEPARTAMENTOS CRITICOS.

Los departamentos críticos son definidos en la fase de procesos críticos en la etapa de Análisis del Impacto en la Organización, de acuerdo con los procesos críticos de la organización relatados por cada departamento.

Con el personal identificado para la operación de procesos críticos y necesarios no automatizados, definir la composición de cada departamento crítico. Cada equipo deberá tener un líder y un suplente definido. Estos departamentos críticos podrán ser revisados durante la etapa de preparación del plan, prueba y mantenimiento. Por cada grupo identificar lo siguiente:

-Personal alternativo identificado por miembros principales.
-Números telefónicos personales y domicilio.

DOCUMENTAR REQUERIMIENTOS DE PERSONAL DE RECUPERACION.

El personal involucrado en la operación de procesos crfticos no automatizados en condiciones de recuperación, puede tener requerimientos que no son responsabilidad del empleado en condiciones normales de operación. Determinar requerimientos del personal de recuperación como:

-Ubicación.
-Transporte.
-Seguridad.

ACORDAR SESIONES DE DISCUSION CON EL PERSONAL PARA CONFIRMAR LOS REQUERIMIENTOS MINIMOS.

Por cada requerimiento de recursos, acordar sesiones de discusión con personal apropiado, individuales o sesiones de grupo para identificar el mfnimo de requerimientos para operaciones en condiciones de recuperación.

5.4.2.7 DETERMINAR REQUERIMIENTOS DE RECURSOS DE TRANSPORTE.

Identificar el tipo de transporte requerido para completar procesos crfticos no automatizados de la organización.

Preparar un inventario de vehículos requeridos para la recuperación, incluyendo alternativas.

IDENTIFICAR TRANSPORTES INVOLUCRADOS EN PROCESOS CRITICOS DE LA ORGANIZACION.

Por cada proceso crftico no automatizado identificar el tipo de transporte usado hasta terminar el proceso.

Estos vehículos y servicios de transportación deberán ser incluidos en el inventario de vehículos.

DOCUMENTAR TRANSPORTES REQUERIDOS PARA LOS PROCESOS EN CONDICIONES DE RECUPERACION.

Por cada vehículo usado en la operación de procesos crfticos no automatizados en condiciones de recuperación, registrar lo siguiente:

-Marca del vehículo, modelo, año de fabricación.
-Descripción del vehículo, color, tipo y otras caracterfsticas.
-Número de registro y fecha de renovación.
-Número de motor
-Tipo apropiado de gasolina.
-Capacidad de carga.

DOCUMENTAR REQUERIMIENTOS DE TRANSPORTES DE RECUPERACION.

Por cada vehículo usado en proceso crfticos no automatizados en condiciones de recuperación, documentar los requerimientos de estos vehículos incluyendo:

-Estacionamiento para los vehículos, por razones de seguridad.
-Medidas físicas de los vehículos.
-Personal con licencia de manejo apropiada.

IDENTIFICAR PROVEEDORES PARA LOS TRANSPORTES USADOS EN PROCESOS EN CONDICIONES DE RECUPERACION.

Para todos los tipos de vehículos usados en procesos crfticos no automatizados y durante la recuperación, identificar proveedor para cada vehículo.

Documentar lugares, números de contacto y otros detalles sobre centros de servicio donde los diferentes vehículos son mantenidos y reparados.

También documentar contacto y detalles de contrato de los servicios de transporte.

ACORDAR SESIONES DE DISCUSION CON EL PERSONAL PARA CONFIRMAR LOS REQUERIMIENTOS MINIMOS.

Por cada requerimiento de recursos, acordar sesiones de discusión con personal apropiado, individuales o sesiones de grupo para identificar el mínimo de requerimientos para operaciones en condiciones de recuperación.

5.4.2.8 DETERMINAR REQUERIMIENTOS DE RECURSOS DE ESPACIO OFICINA/INDUSTRIA.

Determinar el mínimo de espacio requerido para oficina/industria en las operaciones de los procesos críticos no automatizados de la organización en condiciones de recuperación.

Basados en todos los requerimientos de recuperación previamente determinados durante esta fase, determinar y documentar el número de oficinas, espacio general de oficina y algún espacio industrial requerido.

Esto podrá asistir en la selección de un apropiado sitio de recuperación.

Esto deberá incluir espacio para vehículos, planta de manufactura y otros requerimientos que son necesarios.

IDENTIFICAR ESPACIO OFICINA/INDUSTRIA INVOLUCRADO EN PROCESOS CRITICOS DE LA ORGANIZACION.

Identificar la medida y tipo de espacio oficina/industria necesario para acomodar cada requerimiento definido previamente de los procesos críticos no automatizados, considerar:

-Número de personal.
-Cantidad de muebles de oficina(incluyendo escritorios, sillas y gabinetes).
-Cantidad y medidas de máquinas.
-Ambiente requerido para las máquinas.

DOCUMENTAR ESPACIO OFICINA/INDUSTRIA REQUERIDO PARA PROCESOS EN CONDICIONES DE RECUPERACION.

Documentar la medida y número de espacios comunes requeridos para propósitos de oficina e industria.

Considerar alternativas para otros requerimientos tal como equipo usado en operaciones de oficina para reducir el espacio mínimo requerido.

También documentar las facilidades requeridas en cada espacio como:

-Cantidad de personal por cada espacio.
-Areas de almacenamiento.
-Alguna área para protección de energía ó requerimientos de suministro.
-Otras áreas generales de almacenamiento.

DOCUMENTAR REQUERIMIENTOS DE RECUPERACION ESPACIO OFICINA/INDUSTRIA.

Al considerar el espacio oficina/industria requerido, también considerar los accesos a las instalaciones y seguridad requerida en la recuperación del sitio.

ACORDAR SESIONES DE DISCUSION CON EL PERSONAL PARA CONFIRMAR LOS REQUERIMIENTOS MINIMOS.

Por cada requerimiento de recursos, acordar sesiones de discusión con personal apropiado, individuales o sesiones de grupo para identificar el mínimo de requerimientos para operaciones en condiciones de recuperación.

5.4.2.10 PREPARAR DOCUMENTACION DE REQUERIMIENTOS MINIMOS.

Actualizar los documentos registrando los requerimientos mínimos para la recuperación de todos los procesos críticos no automatizados de la organización.

En esta fase los requerimientos de cada proceso crítico no automatizado tienen que ser considerados. Es necesario combinar estos requerimientos para producir una "configuración mínima". Toda la información recolectada en las tareas de esta fase es utilizada y documentada.

Esta configuración mínima para procesos críticos y necesarios del negocio no automatizados es entonces combinada con la especificada en la fase previa.

RECOLECTAR INFORMACION SOBRE CONFIGURACION MINIMA PARA TODOS LOS PROCESOS CRITICOS DE LA ORGANIZACION.

Combinar las declaraciones de requerimientos mínimos preparados para procesos críticos automatizados y los procesos no automatizados por cada tipo de requerimiento para proveer una configuración mínima para todos los procesos críticos de la organización.

Discutir y acordar declaraciones de la configuración mínima especificada para procesos críticos no automatizados.

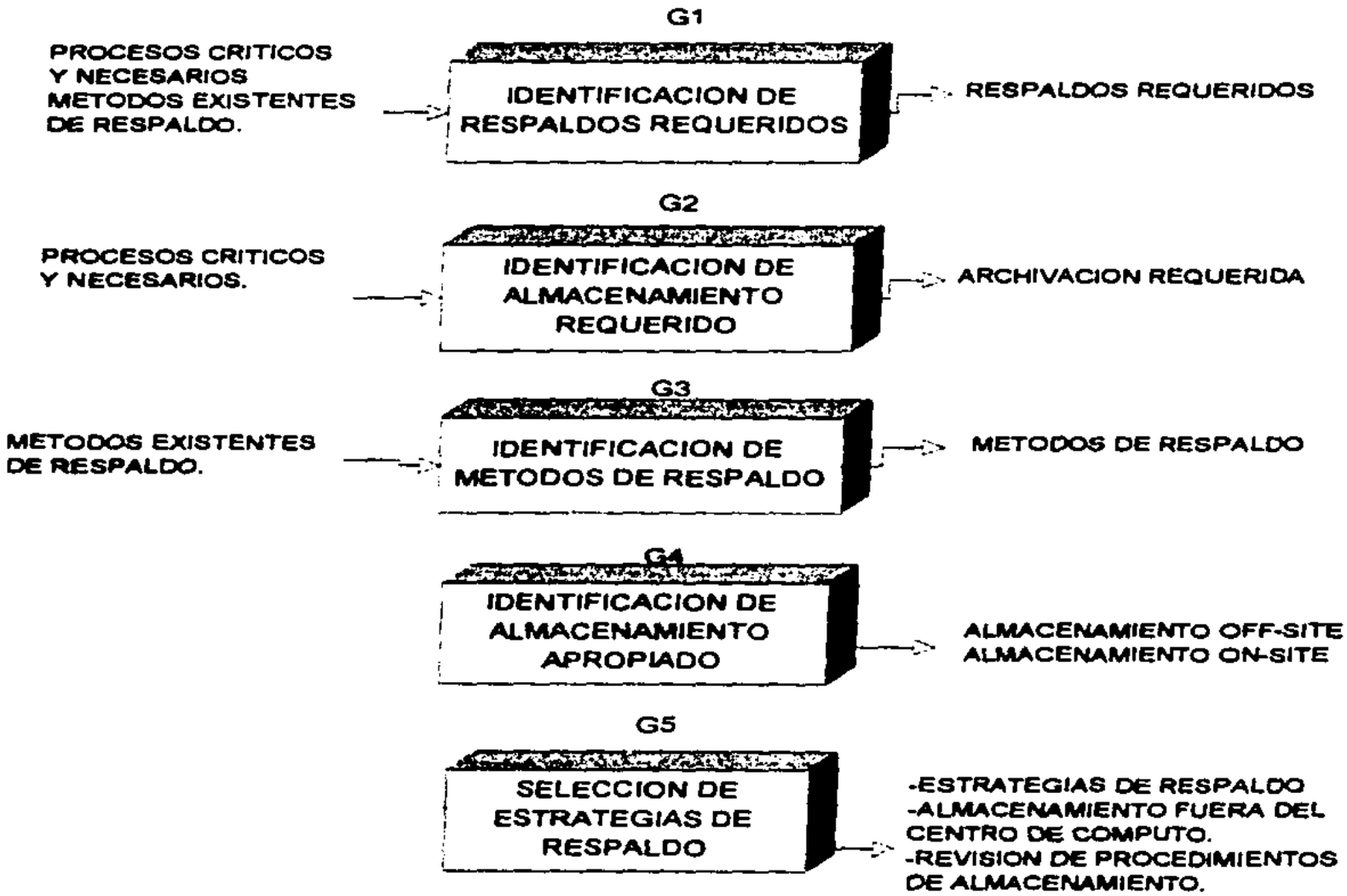
Resolver algunas dudas. El Coordinador de la Recuperación de la Organización deberá acordar con el Gerente los requerimientos de la configuración mínima.

Acordar la mínima configuración para todos los procesos críticos automatizados y no automatizados.

TABLA SUGERIDA DE CONTENIDOS.
DOCUMENTACION DE REQUERIMIENTOS MINIMOS.

Introducción.
1. Resumen de la recolección de información.
2. Aplicaciones de software.
3. Comunicaciones.
4. Software de sistemas
5. Recursos materiales.
6. Registros vitales.
7. Equipo.
8. Personal.
9. Transporte.
10. Utilerías.
11. Espacio Oficina/Industria.
Apendices.

FASE G. ESTRATEGIAS DE RESPALDO.
RELACION DE TAREAS.



5.4.3 ESTRATEGIAS DE RESPALDOS.

Para considerar la alternativa de Respaldo de Datos, seleccionar lugares apropiados que sirvan como almacenes y determinar la frecuencia y contenido de los respaldos.

La clave para una buena recuperación de operaciones de la organización depende de tener copias adecuadas de datos relevantes, programas de cómputo y documentación.

No importa que tan sofisticada sea la estrategia de recuperación, si la organización no puede recuperar los datos y el ambiente de operación en el momento de desastre, la recuperación fallará.

Los requerimientos mínimos de recuperación necesitan de respaldos. En esta fase, el respaldo de los procesos de la organización evaluados como necesarios durante la etapa de Análisis del Impacto en la Organización, deberán ser incluidos.

La selección de una estrategia de respaldo debe tomar en cuenta el almacenamiento dentro y fuera del centro de cómputo, frecuencia de respaldos, número de respaldos requeridos, capacidad de almacenamiento, responsabilidad del respaldo y mantener una adecuada documentación.

La cantidad de tiempo que la información es guardada, puede ser dictado por regulación legal ó de acuerdo a requerimientos de la organización. Estos deberán ser investigados prioritariamente para la selección de una estrategia de respaldo.

El número de copias de datos y el tiempo que éstas son guardadas puede ser determinado por la importancia para la organización y el costo para conservar la información.

Los respaldos pueden ser usados para recuperar un Sistema después de la falla del mismo. El respaldo, no es únicamente concerniente a datos, tamboén para recuperar las operaciones del sistema, programas y utilerias.

Como los datos son generalmente conservados por un largo periodo de tiempo, la configuración del hardware y el software en la organización puede ser cambiada antes que los datos sean requeridos otra vez. Deberá ser documentada la información sobre los datos, incluyendo la configuración específica del hardware y versión del Sistema Operativo, librerías y otros archivos aplicables a el software que procesa los datos en ese momento.

La apropiada estrategia de respaldo deberá ser relacionada en el final de esta fase:

SUMARIO

ENTRADAS	Procesos Críticos y necesarios de la organización. Métodos existentes de Respaldo.
TAREAS	Identificación de respaldos requeridos. Identificación de almacenamiento requerido. Identificación de Métodos de Respaldo. Identificación de Almacenamiento apropiado. Selección de estrategias de Respaldo.
FASE A LIBERAR:	Estrategias de Respaldo. Almacenamiento fuera del Centro de cómputo. Revisión de Procedimientos de Almacenamiento.

5.4.3.1. IDENTIFICACION DE RESPALDOS REQUERIDOS.

Identificar cuales aspectos son necesarios en el proceso de la Organización para ser respaldados con cierta regularidad. Que forma de respaldos, elegir la frecuencia y números de respaldos y el nivel de seguridad a ser mantenidos sobre estos respaldos.

Los respaldos pueden ser requeridos para numerosas razones los cuales pueden ser: la provisión para recuperación de datos, requerimientos legales, requerimientos de contabilidad, políticas de la Compañía.

En un evento de falla completa del Sistema, los respaldos de datos podrán solo ser usados si el ambiente de software en el cual corren puede ser reconstruído.

Hay software de aplicaciones y de sistemas, librerías, utilerías y otros archivos relevantes que pueden también ser respaldados, preparar documentación con detalles de los pasos requeridos para recuperar los sistemas.

ESTABLECER UN PROCESO DE CLASIFICACION DE DATOS.

Establecer un Criterio de clasificación de datos como críticos, necesarios y opcionales. El Coordinador de Recuperación de la Organización deberá obtener asistencia de los auditores y otras áreas en la Organización con una visión de los datos.

Las definiciones usadas en la determinación de importantes y necesarias funciones de la Organización son:

- Críticos: esenciales para la sobrevivencia de la Organización.
- Necesarios: esenciales para mantener las funciones críticas de la Organización.
- Opcionales: no críticos para las funciones de la Organización.

Una sugerencia para extender el criterio basado en estas definiciones:
CRITICO. Información requerida por la ley y para recuperación de procesos críticos de la organización.

NECESARIOS. Información usada en recuperación de procesos necesarios que soportan a los procesos criticos.

OPCIONAL. Información que puede ser fácilmente reemplazada y duplicada.

El documento de criterios de respaldo deberá ser incluido como parte de la sección de estrategias de respaldo de el Plan de Contingencias.

IDENTIFICACION DE RESPALDOS REQUERIDOS POR PROCESOS AUTOMATIZADOS.

Basados en la identificación de procesos críticos automatizados, sus prioridades, desde el Análisis del Impacto en la Organización y los requerimientos de cada aplicación determinar cuales aplicaciones de datos serán respaldadas.

Los respaldos dentro y fuera de la organización son usados para diferentes propósitos. La Documentación para levantar respaldos es requerida y considerada necesaria para completar las operaciones de restauración.

IDENTIFICAR RESPALDOS REQUERIDOS PARA PROCESOS NO AUTOMATIZADOS.

Basados en la identificación de procesos críticos no automatizados y sus prioridades desde el análisis de impacto en la organización y los requerimientos de cada proceso determinar los aspectos de los procesos a respaldar.

El Plan de Contingencias y desastres deberá ser copiado y almacenado fuera de la Organización.

DETERMINAR LA FRECUENCIA DE TIEMPO DE LOS RESPALDOS REQUERIDOS.

Basados en la naturaleza de respaldo requerido determinar cuantos de los componentes de un proceso necesitan ser respaldados.

Los datos de los procesos automatizadas podrán requerir respaldos frecuentes, diariamente, incluyendo archivos de control, modificaciones de accesos, cambios de password, estados de procesos y otra información asociada que se altera simultáneamente con el estado de los datos. El software, utilerías y librerías pueden no cambiar tan frecuentemente y pueden requerir de respaldos menos frecuentes.

DETERMINAR LA SEGURIDAD REQUERIDA DE LOS RESPALDOS.

Los respaldos son tan valiosos como los datos contenidos en el sistema mismo. Hay pruebas de Seguridad que deben ser puestas en práctica para asegurar que el acceso a los respaldos es restringido, particularmente si los datos son fácilmente releibles o con la posibilidad de ser usados con software comercial.

Cada cinta o diskette deberá ser asignado a un propósito particular, para cada uno de estos determinar la medida de los mismos sobre lecturas/escrituras y registrar fecha.

DISCUTIR Y CONFIRMAR LOS REQUERIMIENTOS DE RESPALDOS IDENTIFICADOS, ASI COMO LOS RECURSOS ASOCIADOS Y LA FRECUENCIA.

Esta información deberá ser incluida en el Plan de Contingencias (DCP), como uno de los procedimientos en la fase de preparación del plan.

5.4.3.2 IDENTIFICAR ALMACENAMIENTO REQUERIDO

Identificar aspectos de los Procesos criticos de la Organización, los cuales deben ser archivados y almacenados, forma de almacenamiento, la frecuencia y el número de copias requeridas de archivos y el nivel de seguridad a ser mantenido sobre estos.

El tiempo que los datos son almacenados, puede ser dictado por regulación legal, o requerimientos de la Organización. El número de respaldos y el tiempo que estos son guardados, deberá ser evaluado de acuerdo al costo y a la carga de información.

IDENTIFICAR ALMACENAMIENTO REQUERIDO PARA PROCESOS AUTOMATIZADOS.

Basados en la identificación de procesos críticos y sus prioridades desde el Análisis del Impacto en la Organización y los requerimientos de cada proceso, determinar cuales elementos del sistema deberán ser archivados, incluyendo aplicaciones y software de sistema, utilerías y librerías.

IDENTIFICAR ALMACENAMIENTO REQUERIDO PARA PROCESOS NO AUTOMATIZADOS.

Determinar los aspectos de los Procesos a ser archivados.

Considerar almacenamiento microficha o información basada en papel para ahorrar espacio de almacenamiento.

DETERMINAR FRECUENCIA DE ALMACENAMIENTO.

Mientras cada componente del sistema como aplicaciones y software no cambie frecuentemente, se recomiendan respaldos de una forma regular y no frecuente.

Los datos del sistema y software deberán ser archivados cada vez que estos cambian.

DETERMINAR NUMERO DE COPIAS REQUERIDAS.

Deacuerdo con la naturaleza de la información, determinar cuantas copias de la información a archivar son requeridas.

DETERMINAR SEGURIDAD REQUERIDA.

La seguridad necesaria deberá ser estrictamente controlada.

Para asegurar la integridad de los datos, un control sobre el tiempo de uso deberá ser puesto en práctica. Para cada archivo en cinta o diskette determinar la longitud ocupada y registrar la fecha.

DISCUTIR Y CONFIRMAR EL ALMACENAMIENTO REQUERIDO Y RECURSOS ASOCIADOS, ASI COMO LA FRECUENCIA.

Esta información deberá ser incorporada en el Plan de Contingencias (DCP), como uno de los procedimientos en la Fase de Preparación del Plan.

5.4.3.3 IDENTIFICAR METODOS DE RESPALDOS POSIBLES.

Identificar todos los posibles métodos de respaldo y archivación para la Organización, para los procesos criticos.

El rango de posibles alternativas es dependiente de muchos factores, incluyendo hardware usado, cantidad de información a ser almacenada y la frecuencia.

Hay numerosas alternativas para la creación y almacenamiento de copias de información no automatizada. Esto incluye algunos como microficha, fotocopiado y copias al carbón. Cuando se evalúen alternativas de respaldo deben ser considerados los siguientes 5 factores:

1. Capacidad,
2. Compatibilidad,
3. Costo,
4. Tiempo de Preparación, y
5. Cooperatividad del personal.

IDENTIFICACION DE METODOS EXISTENTES DE RESPALDOS DE DATOS.

Revisar la información proporcionada por los gerentes de departamentos. Estos Métodos existentes pueden implementarse y coordinarse como estrategias de respaldo.

DETERMINAR POSIBLES METODOS DE RESPALDO DE PROCESOS AUTOMATIZADOS.

Para procesos automatizados (mainframe), el más comün de los respaldos es la cinta. Las cintas almacenan una gran cantidad de información.

Hay otras alternativas de respaldo como espejo, almacenamiento en compact disk, diskette, disco duro removible y otras tecnologías.

Cada uno de estos métodos deberá ser evaluado considerando: capacidad de dispositivo, compatibilidad con el sistema existente, el hardware, tiempo de preparación y costo requerido del dispositivo.

DETERMINAR POSIBLES METODOS DE RESPALDO EN PROCESOS NO AUTOMATIZADOS.

En estos casos la recuperación de información almacenada es generalmente de más tiempo consumido.

Algunos de los Métodos son almacenamiento en micro ficha, scaneo y fotocopiado.

Cada alternativa deberá ser evaluada considerando capacidad, compatibilidad, cooperatividad, tiempo de preparación y costo.

5.4.3.4 IDENTIFICAR POSIBILIDAD DE ALMACENAMIENTOS APROPIADOS.

Determinar la localización apropiada de almacenamiento en la organización (on-site) y fuera de la organización (off-site) por corto y largo tiempo, así como el ambiente requerido basado en el tipo de respaldo.
Debe considerarse un segundo respaldo fuera de la organización (off-site) para evitar que se vea afectado por un desastre.

DETERMINAR AMBIENTE REQUERIDO PARA RESPALDOS DE PROCESOS Y ARCHIVOS AUTOMATIZADOS.
Considerar requerimientos de ambiente para el respaldo, por ejemplo: el almacenamiento de cintas en la oficina puede ser dañado, después de unas pocas semanas por la temperatura, donde no existe aire acondicionado, así como si están expuestos a mucho sol,similarmente niveles de alta humedad pueden destruir el óxido contenido en la cinta.

IDENTIFICAR ALMACENAMIENTO POSIBLE EN LA ORGANIZACION (ON-SITE).
Cada tipo de respaldo identificado deberá ser apropiado para algún tipo de información de otro modo este no podrá ser considerado.

Listar las características en ventajas y desventajas incluyendo los diferentes tipos de respaldo.
Documentar los tipos de respaldo identificados, ambiente y otros controles de almacenamiento.

IDENTIFICAR APROPIADOS Y POSIBLES ALMACENAMIENTOS FUERA DE LA ORGANIZACION (OFF-SITE).
En el caso de una recuperación crítica donde el área local es dañada (un respaldo localizado cerca es mas apropiado). En el caso de un desastre regional un respaldo localizado a larga distancia es mas apropiado.

Otra razón para mantener 2 copias de respaldo fuera de la organización (off-site) es para minimizar riesgos de pérdida en el camino.
Hay dos tipos de posibilidad comercial para facilitar el almacenamiento fuera de la organización (off-site):

- Existen los provistos por bancos y compañías de almacenamiento.
  Estas no son recomendadas por no contar con un ambiente especial, tienen limitadas horas de acceso y el espacio posible es limitado.
- Otras organizaciones específicas de almacenamiento.
  Tiene apropiado ambiente, accesibilidad y espacio.

Discutir y confirmar la apropiada Posibilidad de almacenamiento.

5.4.3.5. SELECCIONAR ESTRATEGIAS DE RESPALDO.

Determinar el más apropiado procedimiento de respaldo para la Organización.

REVISION DE REGLAS DICTADAS.
Las reglas, tanto legales como estándares de la Industria deben ser consideradas.

SELECCION DEL APROPIADO ALMACENAMIENTO EN LA ORGANIZACION (ON-SITE).

Documentar las características de cada almacenamiento on-site:

- Localización Física,
- Información a ser respaldada,
- Frecuencia de uso,
- Seguridad y controles de ambiente,
- Volumen del respaldo, y
- Formato de Respaldo.

EVALUAR ALMACENAMIENTOS FUERA DE LA ORGANIZACION (OFF-SITE).

En cada Evaluación considerar:

- Recuperación: Facilidad para la operación.
- Seguridad: Debe existir buena seguridad física, bloques de control, paredes reforzadas y contenido de dispositivos de mantenimiento para control de acceso, monitores las 24 Hrs. del día, el edificio no deberá llamar la atención o ser compartido con otro negocio.
  Deberá tener personal de seguridad capaz, así como controles del personal como: identificaciones con foto, password, fechas de nacimiento, etc.
  Estas características deberán ser regularmente aprobadas.
- Control de Ambiente: Es necesario para almacenar microfilms y cintas magnéticas las cuales son sensitivas a la temperatura y control de humedad. Extremados niveles pueden destruir información. Incluir detectores de humo, fuego, agua, etc.
- Transporte: Control sobre el transporte usado. Los vehículos deberán tener alarma, los cuales detectaran la entrada ilegal.

SELECCIONAR FRECUENCIA DE RESPALDO Y ALMACENAMIENTO.

Determinar la frecuencia requerida, para la creación y almacenamiento de archivos. Preparar un calendario indicando tiempos de respaldo.

DETERMINAR RESPONSABILIDADES DE RESPALDO.

Determinar quien es el responsable por cada respaldo y proceso de almacenamiento.

La Organización debe de responsabilizar a las personas apropiadas para respaldar la información.

DOCUMENTACION SELECCIONADA PARA PROCEDIMIENTOS DE RESPALDO.

Deberán existir procedimientos de prueba sobre respaldos.

Los procedimientos deberán ser desarrollados para asegurar los respaldos que pudieran tener cambios.

Los procedimientos deberán asegurar que los respaldos sean confiables, para que los datos archivados puedan ser recuperados, aún si el ambiente en el cual fueron creados no es el original. Consecuentemente al archivar datos se deberá incluir documentación indicando la configuración y tiempo en que se hizo la copia.

ESTABLECER Y AGREGAR PROCEDIMIENTOS PARA REVISIONES PERIODICAS DE ALMACENAMIENTO FUERA DE LA ORGANIZACION (OFF-SITE).

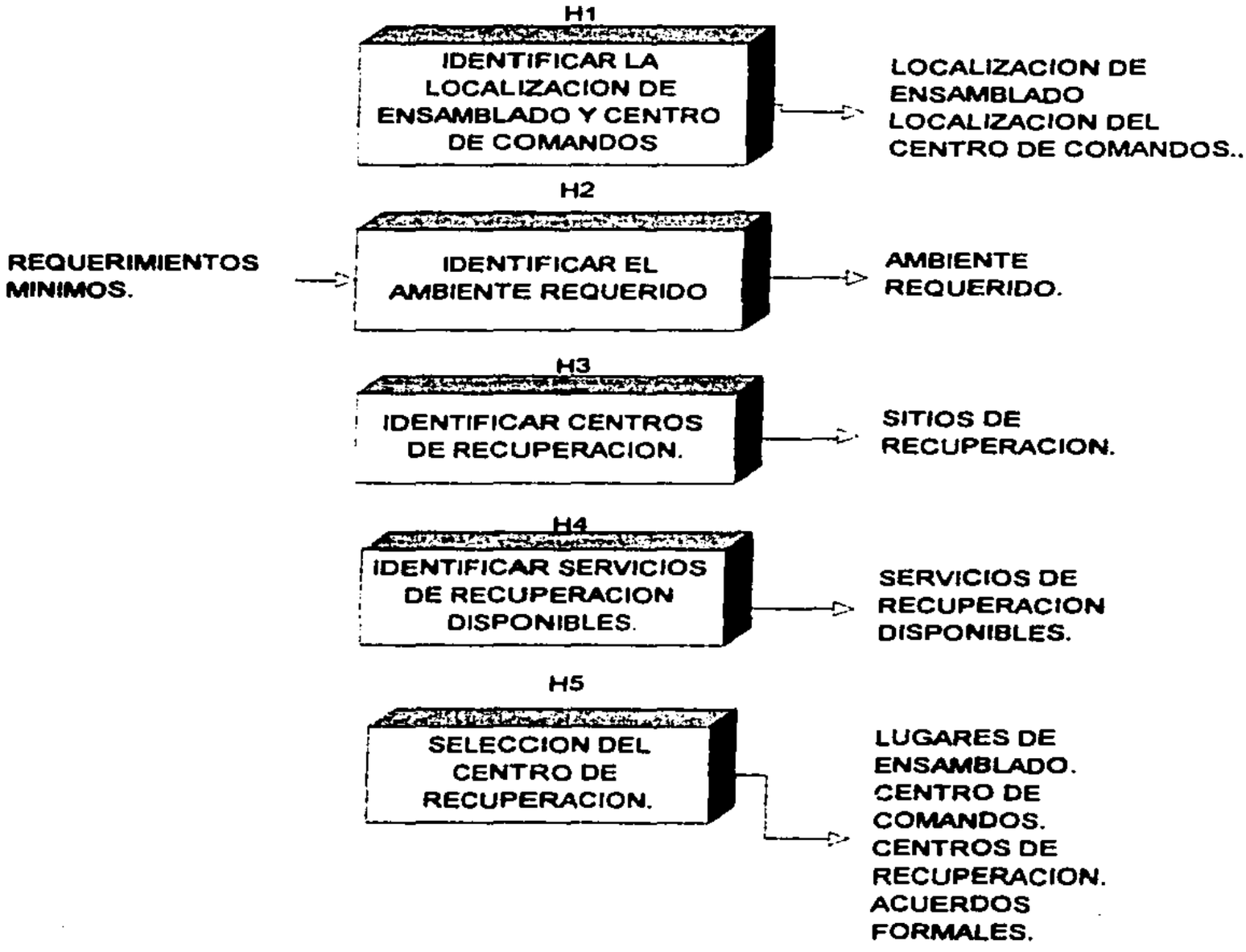
Dependiendo de la velocidad con que suceden los cambios en la Organización una revisión de almacenamiento fuera de la organización (off-site) deberá ser realizada de cada 2 a 6 meses.

Este procedimiento deberá incorporar una revisión de:

- PROCEDIMIENTOS DEL PROVEEDOR. Checar los Procedimientos de almacenamiento, rotación de cintas, desarrollo de calendarios incluyendo tiempo de emergencia posible.
  Para completar, inspeccionar la situación financiera del proveedor y la opinión de la organización sobre los estándares de servicios de almacenamiento off-site.

- PROGRAMAS INTERNOS. Este puede ser determinado por discusiones con los miembros de la Organización. Este deberá incluir ejemplos de información para almacenamiento off-site, para checar si el criterio de clasificación de datos ha sido el especificado.

FASE H. CENTROS DE RECUPERACION
RELACION DE TAREAS.



5.4.4 CENTROS DE RECUPERACIÓN.

Identificar todos los centros de recuperación fuera de la organización y seleccionar un lugar de recuperación primario y alternativo.

Los Centros de Recuperación Primarios deberán ser apropiados para las operaciones cuando suceda un desastre local de grandes proporciones, en el cual otro sitio es requerido para continuar procesando. La selección del tipo de centro de Recuperación podrá ser influenciada por el tiempo máximo que la organización puede interrumpir de los procesos criticos y el costo del centro de recuperación

Una recuperación deberá ser controlada, incluyendo la configuración y uso de los centros de recuperación. Por consiguiente deberá ser establecido un lugar independiente separado desde el cual las operaciones de recuperación puedan ser dirigidas.

El centro de recuperación deberá tener servicios apropiados y espacio para permitir el restablecimiento a las operaciones normales, en una nueva localización.

Las opciones para centros de recuperación son clasificadas en:

- Centros de Cómputo alternativos(Hot-site)
- Centros de Cómputo móviles (Cold-site),
- Acuerdos Recíprocos con otros Centros de Cómputo.

La recuperación de comunicaciones es extremadamente importante para el restablecimiento de procesos automatizados.

La selección de estrategias podrá depender del tiempo límite para la recuperación de la organización, su costo y el tiempo requerido para restablecer las operaciones normales.

5.4.4.1. IDENTIFICAR LA LOCALIZACION DEL ENSAMBLADO Y CENTRO DE COMANDOS.

Identificar centros apropiados para la recuperación en caso de desastre y el centro desde el cual la recuperación de operaciones podrá ser controlada.

Todo el personal deberá tener funciones a realizar cuando suceda un desastre.

IDENTIFICAR REQUERIMIENTOS PARA LA LOCALIZACION DEL ENSAMBLADO.

La localización del centro de ensamblado a una distancia corta del sitio original, pero lo suficientemente lejos para proteger a los empleados del peligro. Y este deberá ser lo suficientemente grande para albergar a todos los empleados.

Las puertas de Salida del centro deberán tener una localización alternativa y deberá contar con teléfonos.

IDENTIFICAR POSIBLES SITIOS DE ENSAMBLADO DE INSTALACIONES.

Identificar todos los posibles sitios para ensamblado en el área inmediata alrededor del lugar original.

Algunos ejemplos son:

- Estaciones Públicas de Transporte(como de tren, autobús, avión o metro).
- Lobby de un Hotel.
- Edificio cercano.
- Lote de Estacionamiento.
- Reservado.

Donde sea apropiado, inferir detalles preliminares en los servicios y características deseables para cada lugar.

IDENTIFICAR REQUERIMIENTOS DEL CENTRO DE COMANDOS.

Las operaciones de Recuperación son dirigidas desde el Centro de comandos comenzando inmediatamente la primer tarea del Plan de Contingencias. El centro deberá tener facilidades como teléfono, fax y de comunicación. Considerar requerimientos especiales de telecomunicaciones.

IDENTIFICAR POSIBLES SITIOS PARA EL CENTRO DE COMANDOS.

Identificar todos los sitios posibles para el centro de comandos en un evento local o regional de desastre.

Para desastres locales, el centro de comando deberá ser un sitio que usa una diferente línea de teléfono.

El centro de comandos deberá ser localizado entre el lugar original y el sitio de recuperación o en el sitio de recuperación.

Si el desastre regional ocurre, el centro de comando deberá ser localizado cerca del sitio de recuperación . El centro de comandos no deberá instalarse en una casa, ni en el área de desastre. Se recomienda en un hotel o motel ó en oficinas rentadas ó en sala de conferencias en otra compañía propietaria.

5.4.4.2.IDENTIFICAR EL AMBIENTE REQUERIDO.

Determinar requerimientos de ambiente para procesos crfticos de la organización.

Considerar el espacio requerido para oficinas, vehículos de transporte, equipo de computadora, máquinas y almacenes establecidos.

IDENTIFICAR EL ESPACIO REQUERIDO.

Identificar el espacio requerido, considerando espacio para oficinas, área de trabajo industrial, área de microcomputadoras, área de mainframe, área general administrativa, vehículos de transporte, maquinarfa y almacenes establecidos. Tomar en cuenta el espacio oficina/industria requerido, establecido en la fase de requerimientos mínimos.

IDENTIFICAR REQUERIMIENTOS DE COMUNICACIONES.

La perdida de las comunicaciones es muy importante para algunas empresas.

Los servicios de comunicaciones pueden ser redes de área local, transferencia de datos y modem.

IDENTIFICAR REQUERIMIENTOS ESPECIALES DE LOS PROCESOS CRITICOS DE LA ORGANIZACION RELATIVOS A SISTEMAS.

Identificar los requerimientos especiales de los procesos criticos de la Organización como: aire acondicionado, líneas de comunicación, reguladores de poder, sistema de supresión de fuego, sistema de enfriamiento.

DETERMINAR EL MINIMO DE REQUERIMIENTOS DE CONFIGURACION.

En la determinación de la configuración requerida para un centro de recuperación revisar los requerimientos mínimos:

- El número de usuarios necesarios para completar las tareas de recuperación, indicando el número de terminales e impresoras y otros periféricos requeridos.
- Entradas y salidas de procesos criticos,indicando

secuencias de proceso básicos y tiempos requeridos.
- Algún hardware especial.
- Otros requerimientos.

IDENTIFICAR REQUERIMIENTOS DE SEGURIDAD.

Identificar características de seguridad requeridas para todos los procesos, para ser implemantados durante la recuperación. Puede incluir personal de seguridad, protección física, así como medidas de reducción de riesgos.

Discutir y acordar los requerimientos de ambiente.

5.4.4.3 IDENTIFICAR CENTROS DE RECUPERACION.

Identificar los lugares apropiados para recuperación, donde los procesos puedan ser restablecidos.

Este centro deberá tener espacio para oficinas conteniendo apropiadas comunicaciones, cableado y otros requerimientos.

Este deberá permitir recuperar los procesos criticos de la organización en un evento de desastre.

DETERMINAR AREAS APROPIADAS PARA EL CENTRO DE RECUPERACION.

Determinar áreas apropiadas en eventos de desastre locales y regionales.

Determinar distancias del lugar original al centro de recuperación.

Sobre un mapa dibujar un círculo alrededor del lugar original para determinar la distancia necesaria en cada tipo de desastre.

El centro de recuperación primario será para desastres locales de grandes proporciones, donde es requerido continuar procesando en una área cercana.

Una de las áreas alternativas deberá ser para la recuperación en un desastre regional, donde el centro de recuperación primario no podrá ser usado. Este centro deberá estar en otra región.

Existe otra área alternativa para recuperaciones de un desastre menor. Este puede ser recuperado en un área de trabajo de la misma organización, pero en otro piso.

IDENTIFICAR POSIBLES CENTROS DE RECUPERACION.

Identificar centros para recuperación tomando en cuenta distancias de desastre local y regional.

Evaluar costos para la selección de un centro de recuperación, si seleccionamos varias alternativas en el momento del desastre se necesitará preparar los requerimientos y contando con un sólo centro previamente evaluar su mantenimiento hasta el momento del desastre.

5.4.4.4 IDENTIFICAR SERVICIOS DE RECUPERACION DISPONIBLES.

Identificar todos los servicios disponibles de recuperación para procesos automatizados, que se necesiten como requerimientos en la Organización.

La configuración para recuperación puede requerir mucho menos procesamiento y capacidad de almacenamiento que durante las operaciones normales.

Hay numerosos y diferentes tipos de servicios para la recuperación de procesos automatizados.

Existen servicios de recuperación en donde, el tiempo es grande pero el costo es menor. El mas común de estos es el centro de cómputo móvil (cold-site) donde un cuarto de cómputo es ensamblado, pero el hardware tiene que ser instalado en el momento de recuperación.

Es común un centro de cómputo alternativo (hot-site) para ser usado por un corto período de tiempo. Es conveniente para la organización usar sus propios recursos para mantener un centro de cómpuyo alternativo (hot-site) o un centro de cómputo móvil (cold-site) para proveer centros de recuperación propios.

IDENTIFICAR CENTROS DENTRO DE LA ORGANIZACION PARA RECUPERACION.

Si la Organización tiene numerosas instalaciones de computadoras. Es posible que distribuya la carga de trabajo de un sitio a otro en un evento de desastre.

Identificar si la Organización tiene algún sitio basado en las consideraciones siguientes:

- Una configuración compatible,
- Suficiente capacidad para soportar procesos extras.
- Personal para completar el Procesamiento y que pueda temporalmente ser transferido, para ayudar en los procesamientos requeridos de recuperación.
- La habilidad necesaria para distribuir los procesos del negocio en múltiples sitios o si estos pueden ser completados en un solo sitio.

IDENTIFICAR UN CENTRO DE COMPUTO ALTERNATIVO (HOT-SITE POSIBLE).

Un hot-site es un Centro de Computo que deberá estar listo en caso de desastre.

Los hot-sites son comercialmente posibles, el costo de este depende de el costo del hardware, espacio de piso requerido, requerimientos de comunicaciones y sustitución de servicios; pero el costo es generalmente alto.

Identificar algún servicio posible de hot-site en un lugar apropiado como alternativa primaria para centro de recuperación.

IDENTIFICAR CENTROS DE COMPUTO CON SERVICIOS DE COMPARTIDOS.

Este consiste en el servicio compartido de un centro de cómputo para muchas organizaciones.Esta opción no es recomendada, pues no puede ser ensamblada cerca. Cuando el desastre ocurre, el Servicio compartido puede no tener capacidad suficiente.

IDENTIFICAR CENTROS DE COMPUTO MOVILES (COLD-SITE POSIBLES).

Los centros de cóputo móviles son provisionales, construidos considerando todos los requerimientos de ambiente.

Cuando un desastre es declarado, la configuración es transportada al lugar elegido por el cliente.

Esto es posible para tener el hardware instalado en línea con la configuración predefinida por el cliente, centro de cómputo alternativo móvil(hot-site).

Este es un costo alternativo pero requiere una gran área para el estacionamiento de la unidad móvil. Notar que los procedimientos de recuperación pueden no estar probados con esta opción.

IDENTIFICAR SERVICIOS COLD-SITE POSIBLES.

Un cold-site es un sitio que tiene el ambiente apropiado para las computadoras pero sin equipo. En un desastre debe instalarse el hardware.

El tiempo de recuperación es obviamente mas largo con un cold-site que con un hot-site donde el hardware ha sido instalado previamente. Notar que los procedimientos de recuperación no pueden ser probados con esta alternativa.

IDENTIFICAR ACUERDOS RECIPROCOS CON OTROS CENTROS DE COMPUTO.

Consiste en un acuerdo con otra Organización que tiene una plataforma compatible y con capacidad. Ambas organizaciones pueden tener la necesidad de un sitio de respaldo y que sirva para procesamiento, cuando ocurre un desastre en la otra Organización.

Un Contrato de Acuerdos para ambas organizaciones deberá incluir lo siguiente:

- Definición de desastre.
- El tiempo de Procesamiento necesario.
- Explicar los recursos necesarios.
- Responsables de la operación.
- Si las líneas de comunicaciones y el equipo podrá ser utilizado.
- Horarios para la recuperación.
- Acuerdos para la notificación de cambios en la configuración.,
- El tiempo de espera entre la declaración del desastre y el acceso al Centro de Computo alternativo.

Esta forma de protección contra el desastre es generalmente no recomendado, pues el desastre puede ser de ambas al unir sus resultados.

5.4.4.5 SELECCION DEL CENTRO DE RECUPERACION.

Seleccionar la alternativa de ensamblado del Centro de Comandos y del Centro de Recuperación.

En esta tarea, las posibilidades de sitios a ser usados deben ser previamente identificadas.

Para cada sitio conocer los requerimientos, facilidades, conveniencia, justificación del costo y prácticas de uso que deberán ser consideradas.

El Coordinador de Recuperación de la Organización deberá realizar la evaluación y selección de Centros de Recuperación en conjunción con el Departamento de Procesamiento de datos.

Cada selección será discutida y acordada.

SELECCION DEL LUGAR DE ENSAMBLADO PARA LA RECUPERACION.

Todos los detalles deberán ser checados para asegurar la accesibilidad a el lugar y la provisión de servicios. Por ejemplo: el uso de teléfonos en el momento del desastre.

SELECCION DEL LUGAR DEL CENTRO DE COMANDOS.

Asegurarse de las facilidades seleccionadas para el propósito y si algún acuerdo formal es requerido. Asegurar el espacio requerido y saber si los servicios funcionan.

SELECCION DEL CENTRO DE RECUPERACION.

Deberá tener una línea diferente de teléfono y de energía eléctrica.

Acordar una inspección física del sitio. El Coordinador de Recuperación de la Organización puede ser acompañado por un experto en sistemas y un auditor.

-Determinar que el equipo puede ser usado en una emergencia.
-Determinar que tan grande puede ser declarado un desastre.

-Asegurar que puede ser usado por el tiempo estimado para la recuperación de procesos.
-Discutir los requerimientos de la organización con el propietario de cada sitio.
-Negociar un tentativo costo y condiciones.
-Evaluar el sitio y seleccionar el más apropiado como primario y alternativo para usarlo como centro de recuperación.

SELECCIONAR EL TIPO DE CENTROS DE RECUPERACION.

Seleccionar el tipo de sitio como primario y alternativo para cada estrategia, considerando:
-Tiempo de procesos críticos de la organización.
-Rango de servicios ofrecidos.
-Calidad de servicios ofrecidos.
-Costo.
-Lugar.

EVALUAR EL CENTRO DE RECUPERACION SELECCIONADO.

El Coordinador de la recuperación de la Organización, ó un miembro del Departamento de Procesamiento de Datos, deberá seguir una serie de pasos para evaluar el centro de recuperación seleccionado.

Los pasos listados se refieren específicamente a la evaluación de centros de cómputo alternativos(hot-site), pero puntos similares se aplican a cada tipo de servicio:

-La persona involucrada en la evaluación deberá tener un conocimiento detallado del mínimo hardware y sistema operativo requerido para procesos de recuperación.

-Preparar una lista de software y hardware del sistema requerido durante la operación, también si es necesario para las procesos de la organización, requerir de transferencia de datos entre lugares, detallando requerimientos de comunicaciones.

-El Coordinador de la Recuperación de la Organización deberá tener un representante de mercado quién requerirá información sobre la configuración mínima de la organización, respaldos, necesidad de comunicaciones y otros requerimientos.

REVISAR LA ESTRATEGIA DE RESPALDO.

En algunos casos, la selección de un particular Tipo de sitio de recuperación puede afectar el Método de Respaldo. La transferencia de transacciones al hot-site puede ocurrir frecuentemente como un Método de Respaldo.

SELECCIONAR UN CENTRO DE RECUPERACION PRIMARIO Y ALTERNATIVO.

Seleccionar dos alternativas de centros de recuperación a ser usados en eventos de desastre.

Seleccionar uno como primario evaluado previamente.

El coordinador de recuperación de la Organización deberá discutir con el gerente la selección del lugar de recuperación.

ACUERDOS DEL CENTRO DE RECUPERACION.

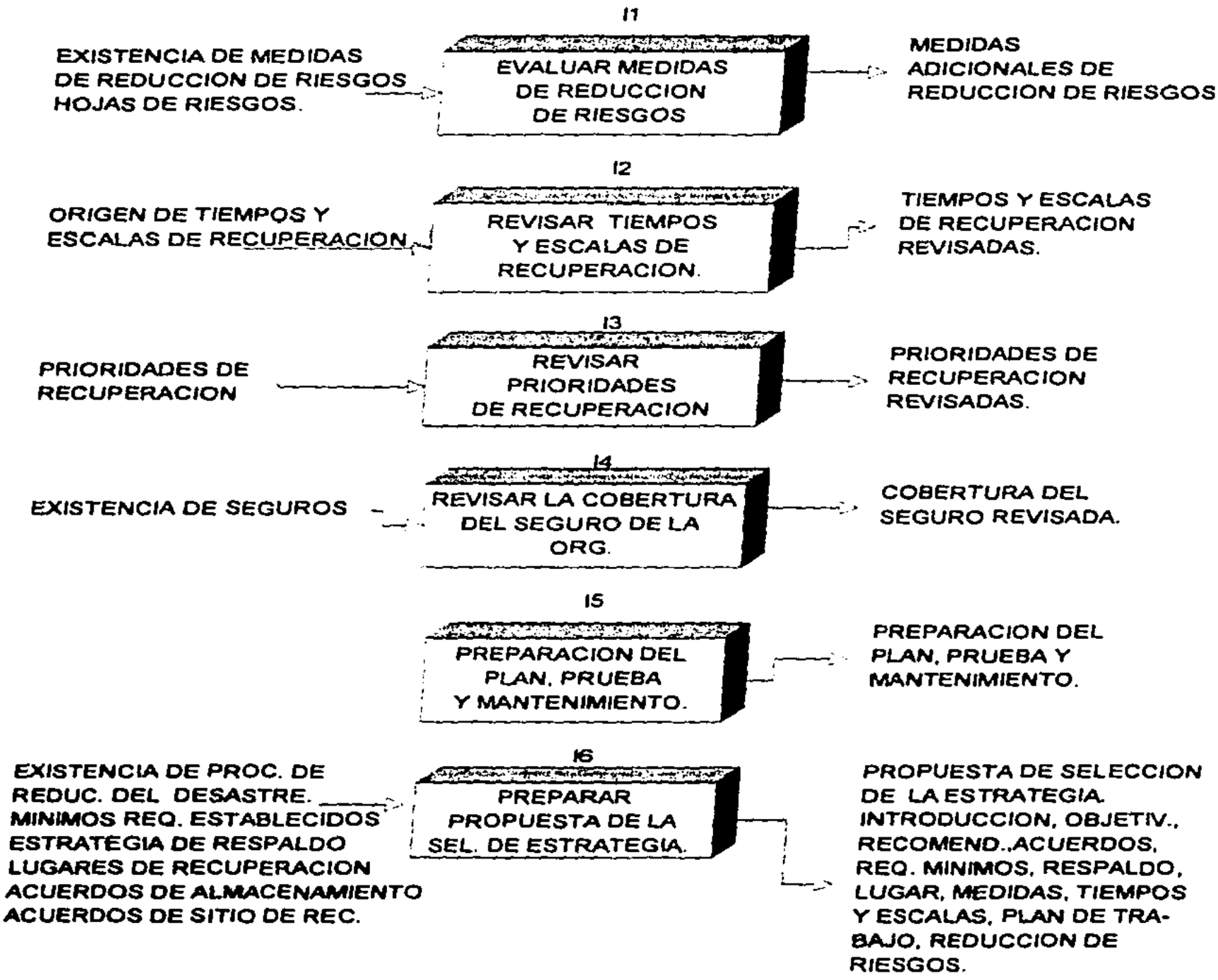
El Gerente deberá ser responsable de finalizar los acuerdos y el contrato deberá tomar efecto en el momento en que se inicien los procedimientos de recuperación en el lugar.

Los contratos deberán ser revisado para asegurar que todo es completamente entendido.

Por ejemplo en un contrato de un centro de cómputo alternativo (hot-site) el Coordinador de Recuperación de la Organización deberá revisar los siguientes puntos:

-Definición de un desastre.
-La posibilidad de suplir la configuración base del equipo.
-Las horas establecidas para prueba del suscriptor y el costo por hora exedida.
-La energía electrica utilizada en la declaración de un desastre.
-La energía electrica utilizada por el uso del hot-site durante la recuperación.
-Honorarios del proveedor por la asistencia en el Plan de Contingencias del cliente.
-El conocimiento de recursos suficientes cuando un desastre severo es declarado al mismo tiempo por diferentes suscriptores.
-El número máximo de suscriptores permitidos.
-El tiempo máximo que un suscriptor puede usar las facilidades de recuperación en un evento de desastre.
-El aviso a los suscriptores de un incremento de precio, con anticipación.
-La descripción de cambios en el equipo por efectos significativos en la configuración, deberán ser notificados por el suscriptor con anticipación.

FASE I. CURSO DE ACCION
RELACION DE TAREAS.



5.4.5 CURSO DE ACCION.

Formular posibles situaciones de desastre de desastre, estrategias de plan de recuperación y después de una evaluación, seleccionar el más apropiado y obtener la aprobación para proceder con el plan de preparación, mantenimiento y pruebas.

Basarse en los requerimientos y lugares de recuperación seleccionados.
Deberán ser evaluadas las medidas de reducción de riesgos existentes.
Es desarrollado y acordado un plan de trabajo con el gerente.
Es preparada una propuesta, la cual combina el trabajo en las fases de selección de la estrategia para la presentación al Gerente. Esta propuesta incluye:

- -Un Resumen de los acuerdos existentes para la recuperación del desastre.
- -Acuerdos y Procedimientos de Respaldo.
- -Opciones de Planeación para la recuperación de un desastre
- -Cambios a las medidas de reducción de riesgo, prioridades de recuperación y escalas de tiempo, cobertura del seguro.
- -La seleccción de la estrategia de Planeación en la recuperación del desastre.
- -Un plan de preparación, mantenimiento y pruebas.

5.4.5.1. EVALUAR MEDIDAS DE REDUCCION DE RIESGOS.

Revisar las medidas existentes de Reducción de Riesgos, evaluar y recomendar medidas adicionales.

Usando la Información preparada en la etapa de Análisis del Impacto en la Organización, revisar las medidas de reducción del riesgo.

Estas medidas de reducción del riesgo son justificadas y acordadas para su implementación

IDENTIFICAR CONSECUENCIAS DE ALTOS RIESGOS.
Identificar que todos los riesgos de la organización y evaluar su costo.

IDENTIFICAR MEDIDAS ADICIONALES DE REDUCCION DEL RIESGO.
Basados en el potencial de alto riesgo de la Organización, identificar medidas relevantes de reducción del riesgo para reducir la exposición a ese daño.
Por ejemplo: El apagado de switches puede ser localizado en las salidas del centro de cómputo para apagarlos. Esto es particularmente importante si el agua ó el fuego amenazan el centro.

Otras medidas de reducción del riesgo incluyen controles incorporados dentro del proceso normal como:

-Controles sobre el desarrollo del software:
- Controles de acceso lógico.
- Librerías de Transferencia.
- Control de cambios.
- Recuperación/Respaldo.

-Controles de Auditoría:
- Reportes.
- Bitácoras de Auditoría.
- Reportes de violación de acceso.
- Estadísticas generales(como totales y sumatorias).
- Procedimientos para pruebas.

PREPARACION DE ANALISIS DE JUSTIFICACION

Preparar un análisis del costo de la interrupción y el costo de la implementación de las medidas de reducción del riesgo identificadas a través de discusiones con los proveedores.

MEDIDAS DE REDUCCION DE RIESGO RECOMENDADAS.

Identificar una medida para cada exposición al riesgo, la cual sea aconsejable, efectiva y no muy costosa.

Tener en mente que mientras se desarrollan los procedimientos del Plan de Contingencias, la adopción de medidas adicionales de reducción del riesgo puede provocar nuevos procedimientos de operaciones y alteraciones al trabajo practicado, el cual puede ser incorporado en el Plan.

Discutir algunas recomendaciones de medidas adicionales de reducción del riesgo, cubriendo el impacto del riesgo y un análisis de justificación del costo.

5.4.5.2 REVISAR TIEMPOS Y ESCALAS DE RECUPERACION.

Revisar las escalas de tiempo tomando en consideración los requerimientos mínimos para la recuperación, las estrategias de respaldo y los lugares de recuperación seleccionados.

Habrá diferentes escalas de tiempo de recuperación estimadas para cada unidad de desastre local ó regional, así como tambien los requerimientos son diferentes.

Las escalas de tiempo deberán ser estimadas para la recuperación de ambas condiciones, emergencia y operación normal.

REVISAR ESCALAS DE TIEMPOS DE RECUPERACION.

Desde el desarrollo del Análisis del Impacto en la Organización, tener las escalas de tiempo de cada proceso critico de la organización.

Hacer un calendario, comenzando en el momento en que el desastre tiene lugar y cada proceso de la organización debe ser restaurado indicando en el calendario el tiempo para la recuperación operando en condiciones de emergencia.

DISCUTIR Y ACORDAR REVISAR LAS ESCALAS DE TIEMPO DE RECUPERACION.

El Coordinador de la Recuperación de la Organización deberá proveer información al gerente relacionando lo usado en la revisión de las escalas de tiempo de recuperación y la explicación de alguna alteración a los mismos.

Obtener la aprobación del Gerente.

5.4.5.3 REVISAR PRIORIDADES DE RECUPERACION.

Revisar las prioridades usando información sobre escalas de tiempo y medidas de reducción de riesgos.

Las prioridades de recuperación son estimadas en la etapa de Análisis del Impacto de la Organización, considerando la pérdida de un proceso en la organización. Son revisados considerando el mínimo de requerimientos de recuperación documentados en esta etapa.

Pueden existir diferentes prioridades, dependiendo del momento en que se interrumpe la organización.

Es importante el orden de las prioridades para la recuperación, lo mismo en un desastre local que regional, en operación de emergencia, que en operación normal, pero el orden de las prioridades será diferente.

Revisar las prioridades documentadas en el desarrollo del Análisis del Impacto de la Organización usando el calendario y las escalas de tiempo de recuperación desarrolladas en la tarea anterior.

REVISAR PRIORIDADES DE RECUPERACION NECESARIAS.

En los procesos donde se determine una alta prioridad de recuperación, considerar las medidas de reducción del riesgo u otras medidas para efectuar una rápida recuperación.

Discutir y acordar la revisión de las prioridades de recuperación.

El Coordinador de la Recuperación de la Organización deberá realizar una revisión de las prioridades de recuperación y medidas adicionales recomendadas con el gerente.

5.4.5.4 REVISAR LA COBERTURA DEL SEGURO DE LA ORGANIZACION.

Asegurar un apropiado nivel de cobertura del Seguro de la Organización.

La etapa de Análisis del Impacto de la Organización provee un resumen de la cobertura de los seguros existentes. Tomando en cuenta estas consideraciones podrán ser implementadas algunas medidas de reducción del riesgo. Las opciones de todo tipo de seguro de la organización, son revisadas para identificar alguna cobertura extra del seguro. Algunas compañías de Seguro ofrecen descuentos por la instalación de cierta medida de reducción del riesgo ó por la implementación del Plan de Contingencias.

El seguro podrá asistir en el financiamiento de las operaciones de recuperación pero no es un sustituto para los procedimientos de recuperación de la organización.

ACUERDO PARA LA INSPECCION DEL LUGAR POR EL REPRESENTANTE DE LA ASEGURADORA.

El Coordinador de la Recuperación de la Organización deberá acompañar a cada representante y discutir los requisitos señalando algunas áreas específicas a ser inspeccionadas.

El representante de la aseguradora deberá preparar un reporte explicando los procedimientos a seguir durante algún evento de interrupción.

REVISION GENERAL DE LA COBERTURA DEL SEGURO.

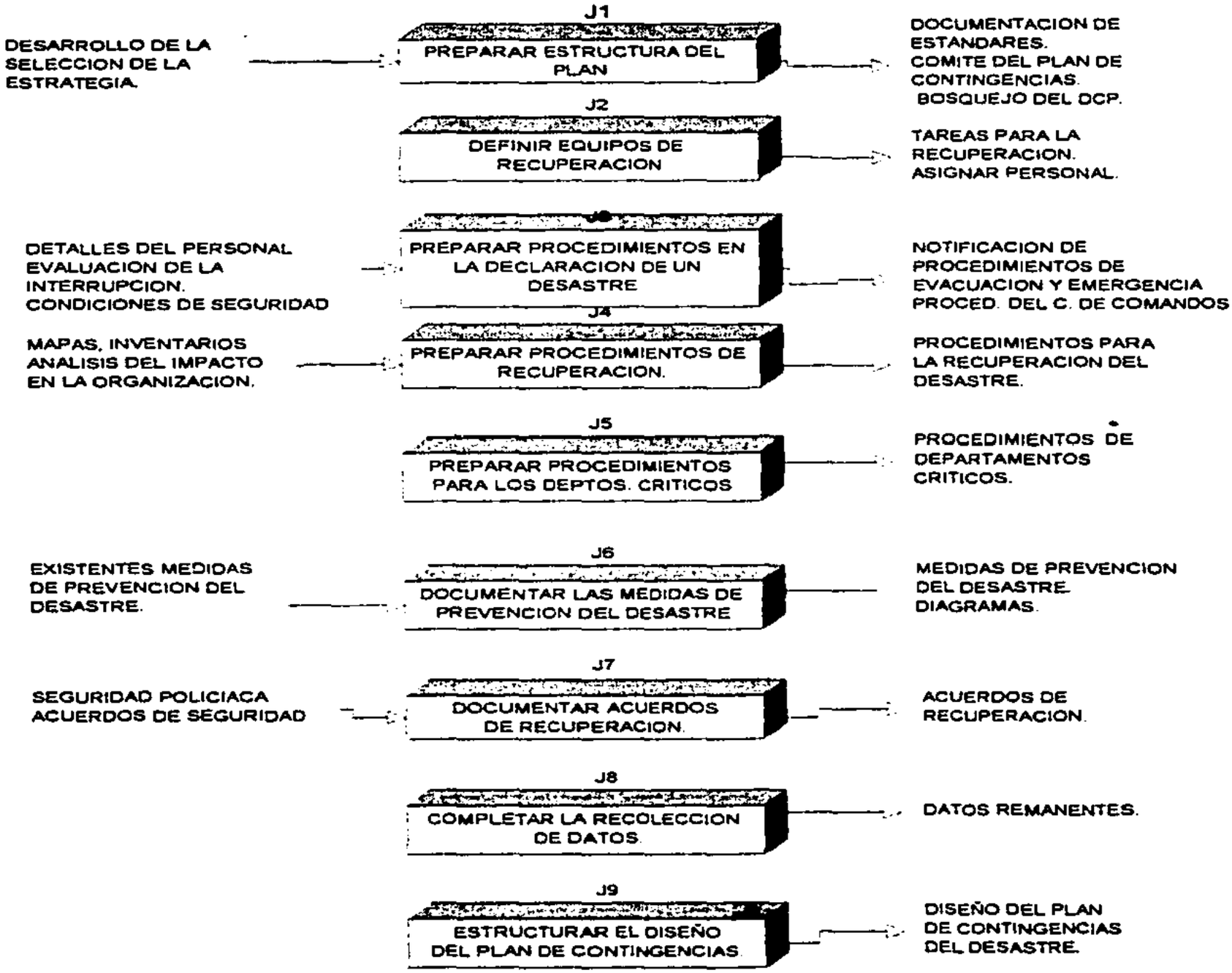
Considerar medidas de reducción del riesgo adicionales para ser implementadas, en el Plan de Contingencias.

REVISAR LA COBERTURA DEL SEGURO DONDE SEA NECESARIO.

La Organización deberá ser responsable de la selección final de la cobertura del Seguro y el acuerdo para revisiones cuando sea necesario.

El Coordinador de la recuperación de la Organización deberá acordar alguna revisión de la cobertura del Seguro con el Gerente.

FASE J. PREPARACION DEL PLAN.
RELACION DE TAREAS.



5.4.5.5 PREPARACION DEL PLAN, PRUEBA Y MANTENIMIENTO.

Definir una preparación del Plan, prueba y etapa de mantenimiento el cual sirve como una utilería de planeación y mecanismo de control para asegurar que el Plan de Contingencias es desarrollado y probado de una apropiada manera y oportunamente.

Identificar tareas como objetivos en la práctica del Plan de Contingencias.
Estimar recursos requeridos para completar cada tarea y llevar a cabo el Plan de Contingencias.
El Coordinador de la Recuperación de la Organización deberá preparar un estimado de tiempo requerido en conjunción con otros miembros del proyecto expertos en las tareas de Preparación, prueba y mantenimiento del Plan.
El Coordinador deberá también ser responsable de informar a la gente del tiempo estimado para el proyecto, así como de la supervisión de ese personal.

ESTIMAR RECURSOS ADICIONALES DE PERSONAL REQUERIDOS PARA LA PREPARACION DE LOS PROCEDIMIENTOS DEL PLAN DE CONTINGENCIAS.

Asignar personas como responsables para la documentación y revisión de los procedimientos del Plan de Contingencias.
Considerar lo siguiente:
-Personal requerido para revisar procedimientos.
-Personal requerido para documentar procedimientos no incluidos en manuales existentes.
-Personal requerido para dar formato a todos los procedimientos.

ESTIMAR RECURSOS ADICIONALES DE PERSONAL REQUERIDOS PARA OPERACIONES DURANTE EL DESARROLLO DEL PLAN Y PRUEBAS.

Durante la preparación del Plan y períódos de prueba, pueden ser requeridos recursos de personal adicionales para continuar con las operaciones normales. Revisar las opciones posibles como ayuda temporal, tiempo extra ó traslado de trabajo a otro lugar.

PREPARAR CALENDARIO DE TIEMPOS
Considerar:
1. Fechas del calendario para tareas prioritarias de el desarrollo, mantenimiento y prueba de los procedimientos del Plan de Contingencias.
2. Calendarizar períódos de trabajo.
3. Niveles jerarquicos para cada tarea del calendario.
4. Planes de Vacaciones.
5. Capacitación.
6. Calendarización de pruebas.
7. Posibilidad de lugares de recuperación.

PREPARACION DEL PLAN, MANTENIMIENTO Y ETAPA DE PRUEBAS.

Incluir lo siguiente:
1. Calendario de tiempos.
2. Recursos de personal estimados.
3. Impacto en la Organización.

Discutir y obtener aprobación del contenido del Plan.

5.4.5.6 PREPARAR LA SELECCION DE LA ESTRATEGIA

Proveer información al gerente para obtener la aprobación de las selecciones y recomendaciones con la autorización para proceder.

PROPUESTA DE SELECCION DE LA ESTRATEGIA.
Incluir en el documento:

1. Un bosquejo del trabajo realizado.
2. Propósitos y objetivos de la selección de la estrategia.
3. Recomendaciones y selecciones.
4. Acuerdos existentes para la recuperación.
5. Requerimientos mínimos de recuperación para procesos crfticos y necesarias de la organización automatizados y no automatizados.
6. Opciones de estrategia de respaldo.
7. Opciones de lugares de recuperación.
8. Recomendaciones adicionales a las medidas de reducción del riesgo, asociar justificación del costo.
9. Revisiones hechas a las prioridades de recuperación y escalas de tiempo de recuperación.
10. Revisiones a la cobertura del Seguro de la organización, incluyendo cambios.
11. Otras consideraciones.
12. Un Plan de Trabajo detallado para la preparación del Plan, mantenimiento y etapa de prueba del proyecto.
13. Conteniendo Apendices detallados de la información resumida.

REVISAR LA ETAPA DE LA SELECCION DE LA ESTRATEGIA.
La revisión de la selección de la estrategia deberá enfocarse a:

-Exactitud en lo estimado en el Plan.
-Satisfacer los objetivos del Plan.
-Claridad para la presentación del Plan.

PRESENTAR Y DISCUTIR LA SELECCION DE LA ESTRATEGIA.
Discutir todas las selecciones y recomendaciones con el Gerente, ındicando claramente los diferentes componentes de la selección de la estrategia. El Coordinador deterá demostrar al Gerente como las estrategias seleccionadas cubren los requerimientos de la Organización.

Obtener aprobación de la estrategia seleccionada y la autorización para proceder.

PUNTO FORMAL DE APROBACION.

CONTENIDO SUGERIDO DE LA TABLA
SELECCION DE LA ESTRATEGIA.
Introducción.

1. Propósitos y objetivos de la Selección de la Estrategia.
2. Recomendaciones.
3. Existencia de acuerdos para la recuperación.
4. Requerimientos mínimos de recuperación.
5. Opciones de estartegia de respaldo.
6. Opciones de lugares de recuperación.
7. Medidas adicionales de reducción del riesgo.
8. Revisiones de prioridades de recuperación y escalas de tiempo.
9. Revisiones de la cobertura del Seguro de la Organización.
10. Acuerdos formales.
11. Otras consideraciones.
12. Preparación del Plan, mantenimiento y etapa de prueba.

5.5 PREPARACION DEL PLAN, PRUEBA Y MANTENIMIENTO.

Un Plan de Contingencias deberá incluir procedimientos a seguir para continuar las operaciones bajo una adecuada protección y seguridad cuando suceda una interrupción.

En esta etapa son desarrollados, probados y establecidos procedimientos de mantenimiento del plan.
Cuando el Plan es terminado debe ser probado y revisado, para que en el momento del desastre no se sigan estrategias incorrectas.

El Plan por sí mismo deberá contener un calendario para pruebas del plan y mantenimiento y deberá proporcionar detalles de objetivos de pruebas y procedimientos.
El contenido del plan de Contingencias relata información de procesos críticos y necesarios de la organización únicamente.

5.5.1 PREPARACION DEL PLAN.

Preparar un diseño del Plan de Contingencia con información previamente recolectada y documentando procedimientos específicos de recuperación del desastre.

Un Plan de Contingencias debe contener toda la información necesaria para recuperar los procesos de la Organización en un desastre.
La información contenida en el Plan de Contingencias debe ser comprensiva, simple para entenderse y con una estructura de secciones fácilmente localizables.
El Plan deberá contener como mínimo:

1. Una sección introductoria anotando el objetivo y el criterio usado para determinar el momento en que el Plan de Recuperación deberá ser usado.
2. Una sección que contenga los pasos a seguir inmediatamente después de que el desastre ocurre.
3. Los procedimientos necesarios para recuperar las operaciones de los procesos críticos para la organización.
4. Responsabilidades, tareas de todas las áreas para la recuperación del desastre.
5. Responsabilidades, personal y tareas para departamentos críticos.
6. Información sobre las medidas de prevención del desastre implementadas y su uso.
7. Información sobre acuerdos hechos para la recuperación antes de que el desastre ocurra.
8. Anexos con listas de inventario, listas de contactos, mapas, diagramas y otros detalles.

Mucha de la información incluida en el Plan de Contingencias es confidencial, por ejemplo números telefónicos y direcciones, detalles de medidas de seguridad, procedimientos de operación y controles.
Una copia original del Plan deberá ser guardada en un lugar externo (off-site) conteniendo toda la información de Recuperación de la Organización. Otras copias completas serán entregadas a otros miembros del equipo de Recuperación si se considera apropiado.

Todas las otras copias del Plan de Contingencias serán distribuidas excluyendo secciones que contienen información no apropiada.

SUMARIO

ENTRADAS	Selección de la Estrategia Detalles del Personal Evaluación de la Interrupción Condiciones de Seguridad Análisis del Impacto en la Organización Mapas e Inventarios Medidas existentes de Prevención del Desastre Seguros.
TAREAS	Preparar la estructura del Plan Definir equipos de recuperación Preparar procedimientos en la declaración de un desastre. Preparar procedimientos de recuperación Preparar procedimientos para los Departamentos críticos Documentar medidas de prevención del desastre. Documentar acuerdos de recuperación Completar recolección de datos. Estructurar el diseño del Plan de Contingencias.
PRODUCTOS	Documentación de Estándares Comité del Plan Bosquejo del Plan de Contingencias Tareas para la recuperación y asignar personal Notificación de Procedimientos Proc. de Emergencia/Evacuación Proc. del Centro de Comandos Proc. para la recuperación del Desastre Proc. en Departamentos críticos Medidas de Prevención del desastre Diagramas Acuerdos de Recuperación

FASE
A LIBERAR: Diseño del Plan de contingencias del Desastre.

5.5.1.1 PREPARAR LA ESTRUCTURA DEL PLAN

Preparar el material introductorio para el Plan de Contingencias que informa las acciones a ejecutarse, el inicio a realizar y un resumen del contenido del Plan.

El diseño del Plan de Contingencias es muy importante, este deberá establecer bases para ser desarrolladas durante el plan.
El Plan debe documentarse en un formato fácil de leer.
En una situación de desastre, únicamente algunas secciones del Plan podrán ser requeridas y debe ser estructurado de una manera que puedan ser encontradas fácilmente.
La información cambiante debe estar en secciones separadas.

ESTABLECER ESTANDARES DE DOCUMENTACION DEL PLAN DE CONTINGENCIAS.
Los estándares de documentación del Plan de Contingencias deberán basarse en:
-Numeración y nombres convencionales.
-Sección de texto y anexos.
-Secciones Fijas y Obligatorias.
-Medida de la página

-Procesadores de palabras/gráficos/(software en general).
-Responsabilidad para su publicación.

La información incluida en el Plan, deberá ser dividida en secciones pequeñas y lógicas. Cada sección deberá contener información únicamente sobre un solo tópico.

Numerar las secciones y subsecciones. El contenido del Plan deberá ser comprensivo usando terminología simple y concisa.

La información es necesaria para una situación de desastre, particularmente para responder a los procedimientos de emergencia.

Mostrar estándares de documentación al Gerente y obtener su aprobación.

PREPARAR EL OBJETIVO DEL PLAN.

El objetivo del Plan de recuperación deberá indicar como el plan puede ser usado para efectos de recuperación de operaciones críticas de la organización durante un desastre.

DOCUMENTAR EL ALCANCE DEL PLAN.

El alcance del plan define bajo que situaciones es diseñado para ser usado. El alcance deberá también definir la magnitud del evento. El alcance es basado en el valor de las operaciones necesarias para la organización, costo de los procedimientos desarrollados, el presupuesto otorgado para el proyecto y en otras consideraciones específicas de la organización.

CRITERIO PARA DETERMINAR UN DESASTRE.

El criterio para declarar un desastre podrá ser determinado por el Coordinador de Recuperación de la Organización y los equipos de recuperación.

El criterio para determinar un desastre podrá ser basado en el financiero e intangible impacto de una pérdida de procesos críticos de la organización y el costo e impacto de las estrategias de recuperación implementadas.

PREPARAR INTRODUCCION DEL PLAN.

Preparar una introducción del plan explicando razones de desarrollo del Plan de Contingencias y presentando su estructura del plan.

DETERMINAR EQUIPOS DE RECUPERACION REQUERIDOS

Cada equipo de recuperación deberá ser responsable de una área en particular para el proceso de recuperación y encargarse de completar una tarea específica para la recuperación.

Determinar en conjunción con el Coordinador de Recuperación de la Organización y el Gerente, cuales equipos de recuperación son requeridos. Documentar la estructura y composición de cada equipo.

Sugerencias de equipos de recuperación a incluir:

EQUIPO/LUGAR	RESPONSABILIDADES
-Equipo de Recuperació de la organización (Centro de Comandos)	Declarar desastre, preparar calendario de la recuperación, coordinar la recuperación, relaciones públicas, aspectos financieros y legales, reportar al Gerente.

-Equipo de Salvamento y Daños

-Equipo de Facilidades
Documentar daños, preparar estimados sobre reparaciones, coordinar reparaciones y reinstalaciones, reportar al equipo de Recuperación de la Organización.

-Equipo de Hardware
Evaluar los daños al Hardware, preparar estimados para reparaciones, coordinar reparaciones y reportar al equipo de recuperación de la organización.

-Equipo de Registros
Evaluar daños a los registros, salvar y establecer ambiente de registros donde sea posible, preparar estimados para restauración de registros, coordinar restauración de registros y reportar al equipo de recuperación de la organización.

-Equipo de Almacenamiento(off-site).
Coordinar carga de respaldos externos (off-site) y su manejo, reportar el equipo de recuperación de la organización.

-Equipo de Recuperación del Centro de Computo

-Equipo de Hardware
Preparar alternativas del hardware, preparar calendario de procesos, sistemas operativos y niveles de emergencia, reportar al Equipo de Recuperación de la organización.

-Equipo de Software
Restaurar ambientes del software de sistemas y software de aplicaciones, reportar al equipo de recuperación de la organización.

-Equipo de Comunicación
Coordinar comunicaciones locales y largas distancias, monitoreo de red, reportar al Equipo de Recuperación de la organización.

-Equipo de Recuperación de Soporte en el Sitio de Recuperación.

-Equipo de Tranporte
Coordinar el transporte usado y requerimientos para recuperar el lugar,
reportar al equipo de Servicios

-Equipo de Hardware
Coordinar la instalación y preparación de del hardware, reportar al Equipo de Recuperación de la organización.

-Equipo de Datos
Actualizar datos por lo ocurrido, reportar al Equipo de Recuperación de la organización.

-Equipo de Servicios
Organizar comunicación entre grupos de recuperación, servicio al cliente, acomodación, soporte admvo., reportar al Equipo de Recuperación de la organización.

-Equipo de Suministros
Coordinar recuperación de suministros, monitoreo de costos, reportar al Equipo de Recuperación de la organización.

-Equipo de Operaciones
Coordinar la seguridad, registro de tiempos del personal.

-Equipo de Departamentos Críticos
Coordinar y completar tareas relatando la operación de procesos específicos de la organización en condiciones de recuperación, reportar al Equipo de Recuperación.

. Todos los equipos podrán tomar parte en las tareas de la reubicación en el momento de la recuperación desde el sitio normal de operaciones a un nuevo sitio listo para ocuparse.
En pequeñas organizaciones, cada equipo puede ser de una persona.

ESTABLECER EL COMITE DE PLANEACION DE RECUPERACION DEL DESASTRE
El Coordinador de la recuperación de la organización en conjunción con el gerente deberá seleccionar personal para formar un comité para la recuperación.

PREPARAR EL BOSQUEJO DEL PLAN.

Establecer las secciones a ser incluidas en el Plan. La información incluida en el Plan deberá ser dividida en pequeñas y secciones lógicas y cada sección deberá contener información únicamente de un tópico. numerar las secciones indicadas y las sub-secciones.
Una lista alfabética del contenido deberá ser incluida en el plan.

REVISAR INFORMACION RECOLECTADA.

La información recolectada. incluyendo los procedimientos del plan, debe ser documentada para que las acciones de recuperación puedan ser tomadas.

TABLA SUGERIDA DE CONTENIDOS DEL PLAN DE CONTINGENCIAS.

-Introducción
-Objetivo del Plan
-Alcance
-Criterio de desastre
-Lista de distribución del Plan.
Procedimientos en la declaración de un desastre.
-Notificación(Contactos de emergencia)
-Ensamblado(Mapas)
-Daños.
-Declaración del desastre.
-Centro de Comandos.
-Responsabilidad en Emergencia (Contactos con servicios de emergencia)

Procedimientos de Recuperación
-Determinar plan de recuperación.
-Notificar el sitio de recuperación.
-Notificar el almacén externo (off-site).
-Notificar equipos de recuperación.
-Establecer centro de comandos.
-Notificar compañía de seguros. (cobertura)
Equipos de Recuperación
-Equipo de Coordinación.
-Coordinador de la Recuperación.
-Equipo de la Recuperación del Desastre.
-Equipos de Departamentos críticos.
-Por cada equipo describir responsabilidades.
Medidas de Prevención del Desastre.
Acuerdos de Recuperación. (Copias del Contrato)
-Estrategias de Respaldo.
-Sitio de recuperación.
-Cobertura del Seguro.
Plan. Prueba y Mantenimiento
-Riesgos
-Plan de Prueba (Calendario de Prueba)
-Plan de Mantenimiento.

5.5.1.2 DEFINIR EQUIPOS DE RECUPERACION.

Determinar la ayuda y especificar responsabilidades de cada equipo de recuperación.

Cada equipo de recuperación tiene responsabilidades y tareas específicas para completar la parte de las operaciones de recuperación.

Existen 2 fases para la recuperación de la interrupción de la organización:
-La recuperación para hacer posible que los procesos continuen.
-La operación de procesos críticos de la organización en condiciones de recuperación.

Hay 2 grupos de equipos:

Los equipos que completan las operaciones de recuperación.

Los equipos de departamentos críticos que completan las operaciones de los procesos criticos de la organización bajo condiciones de recuperación después de que los equipos de recuperación del desastre han completado la preparación de el sitio de recuperación.

ASIGNAR TAREAS PARA EQUIPOS DE RECUPERACION.

Definir las tareas específicas a ser completadas durante la recuperación y asignar estas tareas a los equipos de recuperación del desastre. El equipo de recuperación de la organización deberá ser responsable de la coordinación y monitoreo de todas las tareas de recuperación y de informar al gerente durante los procesos de recuperación.

DEFINIR UNA LISTA DE HABILIDADES PARA CADA EQUIPO DE RECUPERACION.

Para cada equipo de recuperación fotocopilar una lista de conocimientos técnicos y habilidades requeridas para las tareas asignadas a cada equipo.

DETERMINAR JEFES DE EQUIPO DE RECUPERACION.

Un jefe de equipo deberá tener la experiencia técnica para entender, supervisar y completar los procedimientos de recuperación asignados a cada equipo incluyendo la preparación de reportes de avance y el monitoreo de costos incurridos por cada equipo.

En conjunción con el Coordinador de recuperación de la organización

y el comité de planeación de recuperación del desastre, asignar un jefe alternativo de cada equipo definido.

El jefe alternativo deberá ser guía del equipo si el primer jefe no puede por alguna razón en el momento del desastre.

DETERMINAR EL PERSONAL DEL EQUIPO DE RECUPERACION.

Los miembros del equipo obviamente necesitan tener las habilidades técnicas requeridas para completar las tareas asignadas al equipo de recuperación.

El criterio de selección más importante es elegir individuos adecuados para soportar una situación de crisis.

El Gerente de departamento y el jefe deberán tener considerable influencia en esta decisión.

Algunos puntos que deberán ser considerados en la evaluación del personal:

-Características. Una persona quien requiere de supervisión exseciva o es indecisa no es buena elección en una situación de desastre. Así como alguien que no puede comunicar sus ideas ó bien que caresca sin conocimientos técnicos.

-Distancia a su casa. Empleados que viven a una gran distancia del lugar de trabajo puede no ser la mejor opción para el personal del equipo de recuperación del desastre.

Verificar la actitud de esos empleados para dejar su casa durante/después de que un desastre ha ocurrido. Los empleados involucrados en las operaciones de recuperación podrán ser requeridos para trabajar largas horas durante el desastre.

ACORDAR LA SELECCION DEL EQUIPO DE RECUPERACION.

El Coordinador de la Recuperación de la organización deberá presentar al gerente las razones de la selección u omisión de algún individuo en los equipos de recuperación del desastre. Discutir y obtener aprobación.

5.5.1.3 PROCEDIMIENTOS EN LA DECLARACION DE UN DESASTRE.

Preparar procedimientos, detallando tareas y asignando responsabilidades durante el desastre.

En una crisis el Coordinador de la Recuperación de la organización deberá ser informado inmediatamente.

La comunicación es escencial para controlar una situación de desastre y poder ayudar a organizar. Son necesarios y esenciales los procedimientos de evacuación.

Notificar todo lo apropiado a los jefes de equipos de recuperación quienes a su vez deberán contactarse con los miembros de su equipo.

PREPARAR PROCEDIMIENTOS DE NOTIFICACION.

La secuencia de notificación es organizada en una estructura "arbol". El coordinador de la Recuperación de la organización es la primera persona a ser contactada en un evento de emergencia.

Es responsabilidad del Coordinador el notificar a los servicios de emergencia apropiados.

Una lista de contactos de emergencia con números telefónicos de sus miembros deberá ser preparada como parte de un procedimiento de notificación e incluida en el Plan de Contingencias.

-Primer punto de contacto. En todos los casos de crisis el Coordinador de Recuperación de la organización deberá ser el primer punto de contacto y de no encontrarse, se deberá tener un número teléfonico de un contacto alternativo.

-Servicios de emergencia. La persona quien descubre la situación del desastre deberá contactar los apropiados servicios de emergencia. Dependiendo de la naturaleza del desastre estos pueden ser:

-Departamento de bomberos.
-Departamento de policía.
-Ambulancia y/o Hospital.
-Mantenimientos de aire acondicionado.
-Autoridades.
-Servicio de seguridad.
-Compañía de telefonos.

-Equipo de Recuperación de la organización. El coordinador deberá asegurar todas las medidas de prevención posibles ha ser tomadas por el equipo de recuperación.

-Declarado el Desastre. Si un desastre es declarado por el equipo de recuperación de la organización deberán notificar a los jefes del equipo de recuperación ó a sus suplentes si los primeros no se encuentran. El equipo de recuperación de la organización también deberá notificar:

-El lugar del centro de comandos si el original no puede ser usado para dirigir las operaciones de recuperación.
-Algunos lugares de almacenamiento off-site para guardar respaldos.
-Centro de Cómputo alternativos (hot-sites) si el original hardware no puede ser usado.
-El lugar de recuperación si el original no puede ser usado para operaciones de recuperación.

PREPARAR PROCEDIMIENTOS DE EVACUACION.

Cuando un desastre ocurre, algunas personas deberán ser evacuadas. Switchs de poder deberán ser localizados en el centro de cómputo, esto es particularmente importante ya que el agua ó el fuego pueden afectar circuitos eléctricos.

Una ó varias gentes serán responsables para llevar a cabo estos procedimientos.

Esta gente deberá tener responsabilidades especfficas en una evacuación y suficiente habilidad.

Documentar los procedimientos de evacuación.

PREPARAR PROCEDIMIENTOS DE EVALUACION DEL DESASTRE.

El equipo de recuperación de la organización deberá hacer una inspección preliminar de las condiciones, utilerías, hardware, software, aplicaciones, registros y otros equipos disponibles vitales para las operaciones de la organización.

Se deberá determinar la magnitud del desastre para que este sea declarado y que el plan de recuperación sea invocado.

Uno de los factores decisivos a tomar en cuenta es el tiempo de interrupción de las operaciones en una situación de desastre.

Si un desastre es declarado, el daño deberá ser reportado.

El equipo de recuperación de la organización deberá entonces preparar un calendario de tareas a ser realizadas. Este calendario indicará la secuencia de eventos y el tiempo estimado para cada tarea.

Documentar los procedimientos de avaluación del desastre.

PREPARAR PROCEDIMIENTOS DEL CENTRO DE COMANDOS.

Preparar un grupo de estándares de procedimientos detallados para notificar el lugar centro de comandos y ya que este servirá como centro de control de operaciones para la recuperación.

Estos procedimientos deberán incluir un mapa del lugar.

PREPARAR PROCEDIMIENTOS Y RESPONSABILIDADES EN CASO DE EMERGENCIA.

Preparar procedimientos detallados para la inmediata respuesta a emergencia, como:

-Amenaza de bomba
-Derrames químicos.
-Temblores
-Exposición al fuego
-Inundaciones
-Tornados
-Sobrecargas.

unir toda la información sobre servicios de emergencia.

Como los siguientes.

-Bomberos
-Departamento de policía.
-Ambulancia y/o hospital
-Aire acondicionado.
-Autoridades
-Servicio de seguridad
-Compañía de luz
-Compañía de teléfono.

Asegurar que más de un nombre y número telefónico de emergencia sea documentado.

Discutir y confirmar los procedimientos de declaración del desastre.

5.5.1.4 PREPARAR PROCEDIMIENTOS PARA LOS EQUIPO DE RECUPERACION.

Preparar procedimientos que describan en detalle las tareas requeridas para recuperar procesos críticos de la organización.

Cada equipo deberá tener comprensivos procedimientos preparados indicando los pasos a ser tomados para recuperar los procesos críticos de la organización.

Una descripción de responsabilidades, tareas y la secuencia de estas deberá ser documentada por cada equipo.

Puede ser necesario preparar dos grupos de procedimientos de recuperación donde más de una estrategia de recuperación puede ser seleccionada.

IDENTIFICAR RESPONSABILIDADES PARA LA PREPARACION DE LOS PROCEDIMIENTOS DEL EQUIPO DE RECUPERACION.

Es recomendable que un número de individuos sea seleccionado para preparar los procedimientos del equipo de recuperación del desastre.

En conjunción con las recomendaciones del Coordinador de la recuperación de la organización, identificar a los individuos responsables para realizar los procedimientos de recuperación.

Discutir los siguientes puntos con cada individuo seleccionado para preparar los procedimientos del equipo de recuperación:

-Estándares de documentación incluyendo la numeración y secciones de la estructura requerida.
-El nivel de detalle requerido.
-El propósito del contenido.
-Un límite de la información requerida.

Cuando los procedimientos del equipo de recuperación son terminados, un miembro del equipo de recuperación de la organización deberá revisar los procedimientos para asegurar:

-Que todas las tareas involucradas en el proceso de recuperación esten incluidas.

-Que el flujo de información sea claro entre las tareas.
-Que los estándares de documentación y la estructura hayan sido seguidos.

PREPARAR DIAGRAMA DE FLUJO DE LAS TAREAS.

Preparar un diagrama de flujo que indique las tareas de recuperación a ser realizadas durante el desastre y su secuencia correcta.

La presentación de una gráfica de las tareas involucradas en la recuperación ayuda en la interpretación de las mismas.

PREPARAR PROCEDIMIENTOS DEL EQUIPO DE RECUPERACION DE LA ORGANIZACION.

El equipo de recuperación de la organización es responsable de la coordinación, así como de la declaración del desastre, de preparar un calendario de recuperación, relaciones públicas legales, consideraciones financieras y monitoreos sobre el progreso de otros equipos. Así mismo será responsable de reportar al gerente del avance de la recuperación.

Preparar instrucciones detalladas de las responsabilidades del equipo de recuperación de la organización y los pasos a tomar durante el desastre.

PREPARAR PROCEDIMIENTOS PARA LA RECUPERACION DE RECURSOS.

Estos equipos son responsables de la evaluación de los daños para la recuperación de los posibles recursos.

La decisión de reparación ó preparación de un nuevo recurso debe ser responsabilidad del coordinador de la recuperación de la organización.

El límite de tiempo de recuperación puede ser basado en el costo, y debe ser tomada la decisión lo más pronto posible después de que ocurre el desastre.

La documentación deberá incluir: reportes y evidencia en fotografías hasta donde sea posible.

Información adicional puede también ser obtenida de los servicios de emergencia oficial, como el departamento de bomberos, policía y otro personal de emergencia.

Los registros que puedan ser salvados son una parte importante de los procedimientos de recuperación.

PREPARAR PROCEDIMIENTOS PARA EL EQUIPO DE ALMACENAMIENTO FUERA DE LA ORGANIZACION (OFF-SITE).

El equipo de almacenamiento fuera de la organización (off-site) es responsable de la coordinación de sus respaldos.

También deberá acordar que respaldos serán tomados del lugar de almacenamiento fuera de la organización (off-site) y transportados al sitio de recuperación, deberá asegurarse de que sean mantenidas copias adecuadas.

PREPARAR PROCEDIMIENTOS PARA EL EQUIPO DE RECUPERACION DE COMPUTADORAS.

El equipo debe contar con: hardware, software y comunicaciones.

Son responsables de la preparación y prueba de hardware alternativo, sistemas de restauración y software de aplicación, además del reestablecimiento interno, local y larga distancia de comunicaciones en el centro de recuperación.

Incluir procesos de controles y condiciones de integridad en la base de datos.

Estos equipos deben tener especificaciones de configuración, software, respaldos de datos y estrategias de prueba.

PREPARAR PROCEDIMIENTOS PARA EL EQUIPO DE USUARIOS DE LOS PROCESOS CRITICOS.

El uso del centro de recuperación es donde los procesos críticos de la organización podrán ser procesados hasta que una alternativa pueda ser localizada y establecida para reinstalarlos al estado original.

Los equipos sugeridos son de transporte, hardware de datos, de

servicios administrativos, suplente y de operaciones.
Estos son el soporte de las operaciones en el centro de recuperación.
Deberá ser preparado un calendario de operaciones en condiciones de recuperación, detallando las necesidades diarias, semanales y mensuales.
El equipo de servicios administrativos será responsable de periódicos y contactos con los empleados no involucrados en las operaciones de recuperación. También deberá hacerse cargo de la distribución del personal cerca de los centros de recuperación, los métodos de pago, contabilidad de la compañía y el transporte entre los sitios de recuperación.
Preparar instrucciones detalladas sobre las responsabilidades del equipo de usuarios de procesos criticos y las tareas a realizar en el momento de desastre y durante las operaciones de recuperación. Algunas consideraciones específicas son:

-Software de aplicación:
Preparar instrucciones detalladas para restaurar cada aplicación.
Esta documentación deberá incluir:
- -Una lista del software y soporte utilizado.
- -Especificaciones técnicas.
- -Especificar la instalación de aplicaciones y sus instrucciones de recuperación.
- -Especificar la carga de bases de datos y sus instrucciones de recuperación.
- -Checar la integridad para asegurar que el sistema es estable.

Si es necesaria la reconstrucción de una Base de Datos en ese caso lo siguiente deberá ser realizado:
- -El software de la base de datos deberá ser usado para confirmar la integridad de la base de datos interna.
- -Deberán ser generados reportes de control para confirmar la integridad de datos.
- -Deberá ser identificado el punto de corte de la última transacción completa identificada.
- -Deberán ser cuidadosamente checados los primeros procedimientos y reportes.

Indicar que pasos pueden ser realizados por personal interno y cuales requieren de un soporte externo.

-Comunicaciones.
Documentar los pasos requeridos para la recuperación de las comunicaciones que soportan los procesos criticos de la organización basados en computadora.
Preparar instrucciones detalladas para restaurar las comunicaciones. Esta documentación deberá incluir:
- -Una lista de software de utilerías y soporte que necesiten las operaciones.
- -La combinación de cable de comunicaciones, dispositivos, software, servicios externos e interfases requeridas.
- -Especificar instalación de dispositivos de comunicaciones y procedimientos de recuperación de la configuración.
- -Especificar software de comunicaciones y procedimientos de recuperación.
- -Checar la integridad para asegurar las comunicaciones.
- -Algunas provisiones de respaldo.

-Software de Sistemas
Documentar los pasos requeridos para la recuperación de sistemas que soportan los procesos criticos de la organización basados en computadora.
Por cada sistema documentar que respaldos son necesarios,

incluyendo la medida de los respaldos para la recuperación por:
-Fallas de hardware
-Fallas en algún sistema.
-Fallas en una porción del sistema.
Deberá también incluir el número de paquetes de discos dedicadas y cintas magnéticas requeridas, copias de seguridad, archivos que necesitan ser removidos después de proceso.
Preparar instrucciones detalladas para restaurar cada sistema. Esta documentación deberá incluir:
-Pasos para la carga de respaldos fuera de la organización (off-site) y el software de los sistemas.
-Especificaciones técnicas.
-La secuencia de carga de los sistemas y software de soporte.
-Especificar las instrucciones de recuperación.
-Integridad validada para asegurar que el sistema es completo y estable.

-Recursos Materiales
Documentar los pasos requeridos para recuperar recursos materiales usados en procesos críticos.
Preparar una lista de todos los recursos materiales necesarios.

-Registros vitales.
Documentar los pasos requeridos para recuperar los registros vitales usados en los procesos criticos de la organización.

-Equipo
Documentar algunos pasos requeridos para la recuperación del equipo, en la cual debe ser incluida una lista de algún transporte especial requerido para mover el equipo.
Documentar alternativas de equipo ó procesos manuales que pueden ser usados incluyendo hardware para conducir las operaciones de emergencia de un proceso.
Documentar el personal requerido para compeltar las operaciones de recuperación, puede necesitarse asistencia técnica y detalles sobre personal de soporte externo.

-Transporte
Incluir:
-Procedimientos y algún staff asignado para completar la transferencia del respaldc desde el almacén.
-Medidas alternativas de recolección y preparación de datos y distribución de salidas.
-Reemplazamientos por fallas de transmisión.
-Provisiones para servicio de correo
-Provisiones para obtener vehículos a trasnportación requerida.
-Recursos alternativos de vehículos o transportes en el evento de la pérdida de vehículos durante el desastre.

-Utilerías
Deberán ser documentados los pasos a seguir para restaurar utilerías, incluir:
-Procedimientos de recuperación.
-Contactos con nombres y números telefonicos.
-Tiempos mínimos de recuperación para cada utilería.
-Datos relevantes del lugar, si las utilerías son instaladas en un sitio alternativo.
-Configuraciones requeridas.

DETERMINAR RECURSOS USADOS EXCLUSIVAMENTE EN LA RECUPERACION DE PROCESOS CRITICOS AUTOMATIZADOS.

Definir todos los recursos usados en la recuperación de procesos críticos automatizados de la organización.

Considerar todos los pasos involucrados en las operaciones de recuperación. Para cada paso considerar que recursos son requeridos en las siguientes áreas:

-Software, Aplicaciones y Software de sistemas.
-Comunicaciones.
-Recursos Materiales
-Registros, incluyendo datos basados en computadora.
-Equipo, incluyendo configuración y transporte.
-Personal
-Transporte requerido por cada recurso.
-Utilerías.
-Espacio oficina/industria.
-Suministros para cada requerimiento.

Muchos de estos requerimientos pueden duplicar los recursos requeridos para operar los procesos criticos automatizados en condiciones de recuperación como fue determinado en la etapa de la selección de la estrategia.

DETERMINAR RECURSOS USADOS EXCLUSIVAMENTE EN LA RECUPERACION DE PROCESOS CRITICOS NO AUTOMATIZADOS DE LA ORGANIZACION.

Definir todos los recursos usados en la recuperación de procesos críticos no automatizados de la organización.

Considerar todos los pasos involucrados en la recuperación de operaciones.Para cada paso considerar que recursos son requeridos:

-Recursos Materiales
-Registro vitales
-Equipo, incluyendo configuración y transporte.
-Personal incluyendo las funciones.
-Transporte requerido para cada recurso.
-Utilerías
-Espacio oficina/industria
-Suministros para cada requerimiento.

Muchos de estos requerimientos pueden duplicar los recursos requeridos para operar los procesos críticos no automatizados de la organización en condiciones de recuperación como están determinadas en la etapa de la selección de la estrategia.

Discutir y confirmar el equipo de recuperación, procedimientos y requerimientos.

5.5.1.5 PREPARAR PROCEDIMIENTOS PARA LOS DEPARTAMENTOS CRITICOS.

Preparar procedimientos que describan en detalle las tareas requeridas para operar procesos críticos de la organización en condiciones de recuperación.

Los procedimientos preparados para equipos de departamentos críticos contienen instrucciones para la operación de procesos críticos de la organización en condiciones de recuperación.

Cada tarea deberá ser asignada como una responsabilidad a una persona del grupo.

IDENTIFICAR RESPONSABLES PARA LA PREPARACION DE PROCEDIMIENTOS PARA LOS GRUPOS DE DEPARTAMENTOS CRITICOS.

De los individuos que son involucrados en la operación de procesos críticos en condiciones de recuperación deberá ser seleccionado alguno para preparar procedimientos para grupos de departamentos críticos.

Distribuir las tareas de preparación de procedimientos a este personal, podrá servir para numerosos propósitos:

-La documentación de procedimientos deberá ser completada rápidamente por la familiaridad con los procesos.
-Todos los detalles relevantes son documentados.
-Incluyendo aspectos usados infrecuentemente.
-Apropiado uso de documentación existente.

Identificar a los individuos apropiados como responsables para completar secciones de procedimientos. Miembros del equipo de recuperación de la organización en conjunción con el gerente de cada deparatamento deberá asistir en esta selección.

Discutir con cada individuo seleccionado para preparar porciones de los procedimientos del departamento crítico como los siguientes:

-Documentación incluyendo estándares, la numeración y tipo de sección en la estructura requerida.
-El nivel de detalle requerido.
-El propósito del contenido.

Cuando los procedimientos del departamento crítico son determinados, el gerente de cada departamento deberá revisar los procedimientos para asegurar que:

-Todas las tareas envueltas en el proceso son incluidas.
-El flujo de la información sea claro entre las tareas.
-Los estandares de documentación y estructura han sido seguidos.

PREPARAR PROCEDIMIENTOS DEL DEPARTAMENTO CRITICO.

En una situación de desastre, son restablecidos cada equipo y los usuario en el sitio de recuperación preparados para operar los procesos críticos de la organización comenzando así la recuperación.

Los grupos que operan estos procesos podrán usar la documentación preparada.

Preparar instrucciones detalladas sobre responsabilidades de los grupos de departamentos críticos y los pasos que ellos tomarán durante las operaciones de recuperación, estas instrucciones incluirán referencias a manuales y procesos normales del usuario.

Discutir y confirmar los procedimientos de los departamentos criticos.

5.5.1.6 DOCUMENTAR MEDIDAS DE PREVENCION DEL DESASTRE.

Documentar la implantación de medidas de prevención del desastre e instrucciones para uso normal y de emergencia.

Deberá ser documentada la existencia y operación de medidas de prevención del desastre en la organización.

Un gran paso en la prevención del desastre es instalar medidas para reducir el riesgo.

La existencia de medidas de prevención del desastre son documentadas en detalle, incluyendo sus lugares, información sobre su propósito e instrucciones para su uso. El Coordinador de la recuperación de la organización deberá ser responsable de asegurar la inclusión de medidas de algún riesgo adicional que son evaluados durante el período en que el Plan de Contingencia está siendo preparado.

DOCUMENTAR INSTRUCCIONES PARA EL USO DE MEDIDAS EXISTENTE DE PREVENCION DEL DESASTRE.

Documentar las medidas de seguridad existentes en el lugar e instrucciones relatando su uso.
Deberá incluir:
-Seguridad física
-Asistencia médica
-Prevención de fuego
-Limpieza general en el centro de procesamiento de datos, mantenimiento.
-Ambiente
-Medidas de protección del software con passwords y otros.
-Protección de comunicaciones
-Medidas de control para la estructura del desarrollo de software.

PREPARAR DIAGRAMAS PARA FACILITAR EL DESARROLLO
Preparar un diagrama del centro de procesamiento de datos a escala incluyendo salidas, entradas, direcciones y métodos de abrir puertas, equipo, poder y líneas de comunicación, switches de emergencia, transformadores de poder y switchs de alarma.
Usar este diagrama como una base y preparar diagramas separados mostrando los lugares de medidas específicas de prevención del desastre.Por ejemplo extinguidores.
Cada diagrama será familiarizado con el personal

Discutir y confirmar las medidas de prevención del desastre.

5.5.1.7 **DOCUMENTAR ACUERDOS DE RECUPERACION**

Documentar acuerdos existentes de recuperación incluyendo calendarios y requerimientos.

Incluir la estrategia de respaldo adoptada, para equipo de computo y el uso, cobertura del seguro.

DOCUMENTAR ESTRATEGIAS DE RESPALDO
Incluir lugares de almacenamiento dentro y fuera de la organización así como una copia de los calendarios de respaldos.

DOCUMENTAR ACUERDOS DEL SITIO DE RECUPERACION
Incluir un resumen de los puntos acordados . Asegurar la notificaión de procedimientos requeridos y mapas de los lugares con direcciones específicas.

DOCUMENTAR LA COBERTURA DEL SEGURO
Incluir copia de los contratos con aseguradoras, preparar documentación de los puntos de seguridad. Procedimientos incluidos como parte de la covertura del seguro.

DOCUMENTAR REGISTROS SALVADOS
Documentar los registros recuperados.

Discutir y confirmar los acuerdos de recuperación.

5.5.1.8 **COMPLETAR LA RECOLECCION DE INFORMACION.**
Revisar los datos recolectados para la inclusión en el plan de contingencias del desastre.

IDENTIFICAR ALGUN REMANENTE DE DATOS NECESARIOS.

Identificar información la cual no ha sido recolectado. Identificar algún procedimiento ó requerimiento que ha sido implementado o alterado al preparar el Plan de Contingencia.

5.5.1.9 ELABORACION DEL BORRADOR DEL PLAN DE CONTINGENCIAS.

Recolectar toda la información del borrador del Plan de Contingencias.

El borrador del Plan de Contingencias es revisado para asegurar secuencia de secciones, deberá ser después de discutido con el gerente.

REUNIR TODA LA INFORMACION DENTRO DEL PLAN DE CONTINGENCIAS.

Acomodar toda la información preparada para el Plan de Contingencias en el orden especifícado. El Plan deberá contener referencias de documentación existente.

VERIFICAR EL CONTENIDO Y CONSISTENCIA DEL PLAN DE CONTINGENCIAS.

Miembros del equipo de recuperación de la organización deberán revisar todos los procedimientos y alguna otra información preparada para su inclusión en el Plan de Contingencias para asegurar que:

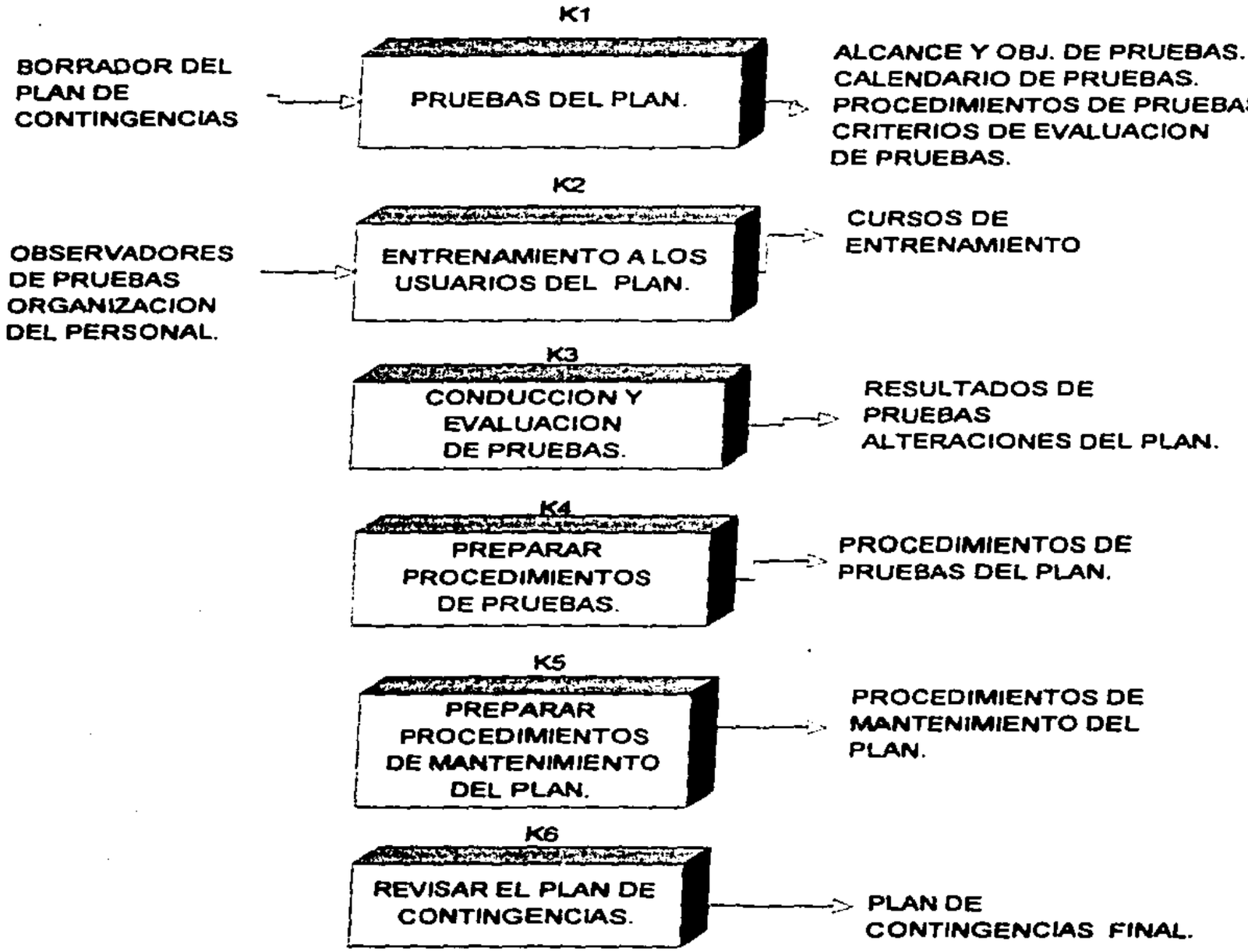
-Estándares de documentación y estructura hayan sido incluidos.
-El nivel requerido de detalle sea incluido.
-El flujo de información sea considerado
-La información sea integrada comprensible y consistente.

REVISAR Y DISCUTIR EL PLAN DE CONTINGENCIAS.

Leer el plan. Asegurar el flujo apropiado desde una sección a la siguiente y revisar toda la información relevante incluida para el evento del desastre.

Discutir el Plan de Contingencias con el comité de planeación de recuperación de la organización y obtener su aprobación.

FASE K. PRUEBA Y MANTENIMIENTO DEL PLAN
RELACION DE TAREAS.



5.5.2 PRUEBA Y MANTENIMIENTO DEL PLAN.

Verificar que el Plan de Contingencias sirva para recuperar los procesos críticos de la organización después de que estos hayan sido interrumpidos.

Durante la prueba del plan el coordinador de la recuperación de la organización coordina las pruebas de todos los aspectos del plan.

Estas pruebas son necesarias para asegurar que el plan este completo antes de ser usado en una situación de desastre.

SUMARIO	
ENTRADAS:	Borrador del Plan de Contingencias. Observadores de pruebas. Organización del personal.
TAREAS:	Pruebas del plan. Entrenamiento a los usuarios del plan. Conducción y evaluación de pruebas. Preparar procedimientos de pruebas. Preparar procedimientos de mantenimiento del plan. Revisar el Plan de Contingencias.
PRODUCTOS:	Alcance y objetivos de pruebas. Calendario de pruebas. Procedimientos de pruebas. Criterio de evaluación de pruebas. Cursos de entrenamiento. Resultados de pruebas. Alteraciones del plan. Procedimientos de mantenimiento del Plan.
FASE A LIBERAR:	Plan de contingencias final.

5.5.2.1 PRUEBAS DEL PLAN

Idear procedimientos de prueba para evaluar el Plan de Contingencias identificando y describiendo todas las tareas involucradas en la recuperación de procesos críticos de la organización.

Las pruebas pueden consistir en:
-Determinar la eficiencia del plan.
-Obtener tiempos estimados durante las operaciones de recuperación.
-Entrenamiento requerido en situaciones de crisis.

Cada aspecto del Plan de Contingencias deberá ser probado como parte de el proceso de recuperación.

DETERMINAR ALCANCE DE LAS PRUEBAS.

Una prueba puede afectar únicamente un proceso crítico de la organización ó un paso de las tareas de recuperación, las pruebas pueden ser desarrolladas alternadamente para evaluar todos los procedimientos de recuperación.

Cuando se determine el alcance de cada prueba, considerar el costo de los recursos requeridos para realizar la misma.

DETERMINAR OBJETIVOS DE LAS PRUEBAS.

Para cada prueba determinar objetivos. Como los siguientes:

- Confirmar tiempos estimados para procesos de recuperación.
- Verificar que el desarrollo es aceptable con configuraciones específicas de recuperación.
- Verificar la exactitud del Plan de Contingencias en cuanto a:
  - Arbol de notificación.
  - Facilidad de almacenamiento fuera de la organización (off-site).
  - Evaluación del sitio de recuperación.
  - Que los procedimientos sean prácticos para dar respuesta en casos de emergencia.
  - Requerimientos de recursos mínimos.
  - Estrategias de respaldos.
  - Documentar procedimientos de recuperación.
  - Documentar procesos críticos.

DETERMINAR METODO DE PRUEBAS.

Las pruebas pueden ser conducidas en una situación pasiva ó activa:
-Pasiva es conducir la prueba "como si" el desastre hubiera ocurrido.
-Activa es donde el desastre es simulado con sus condiciones.

Por cada prueba seleccionada deben ser elegidos los métodos más apropiados para asegurar el mínimo de interrupción de las operaciones.

DEFINIR CONDICIONES DE PRUEBA.

Por cada prueba, definir las condiciones. Por ejemplo en alguna prueba definir condiciones específicas comopuede ser que el coordinador de la recuperación no pueda ser localizado.

PLANEAR Y DOCUMENTAR PROCEDIMIENTOS DE PRUEBA.

Planear y detallar los procedimientos a seguir para conducir las pruebas verificando los resultados esperados.

Los procedimientos de pruebas deberán ser referidos a las secciones del Plan de Contingencias donde estan documentados procedimientos de recuperación

ESTABLECER CALENDARIOS DE PRUEBAS.

Preparar calendario detallando el tiempo de pruebas. En la preparación considerar cargas de procesos, vacaciones y otros eventos.

Presentar los detalles de las pruebas y obtener aprobación al diseño de las mismas.

5.5.2.2 **ENTRENAR A LOS USUARIOS DEL PLAN.**

Entrenar a todo el personal a responder a una emergencia siguiendo los procedimientos del Plan de Contingencias.

Entrenar para la evacuación y para el uso de las medidas de prevención de un desastre.

El propósito e importancia del Plan de Contingencias deberá ser presentado a todo el personal para incrementar sus conocimientos ante un desastre.

ESTIMAR EL NUMERO DE GENTE A SER CAPACITADA EN CADA GRUPO.

Determinar el número de personas de cada grupo a ser capacitado, la metodología para la capacitación, recursos requeridos, número de sesiones y/o tiempo requerido.

Todo el personal debe ser notificado para seguir procedimientos.

IDENTIFICAR TOPICOS DE ENTRENAMIENTO.

Identificar los tópicos específicos a ser cubiertos en cada sesión. Basados en los tipos de sesiones necesarias, sus niveles y sus actividades, identificar las clases de entrenamiento a preparar.
Incluir lo siguiente:

-Nombre del curso.
-Requisitos y propósito del curso.
-Audiencia.
-Número estimado de sesiones.
-Número estimado de participantes por sesión.

DETERMINAR LAS TECNICAS DE ENTRENAMIENTO A SER EMPLEADAS.

Considerar como será la capacitación a presentar y quién la impartirá, incluyendo:

-Sesiones de salón conducidas por un instructor.
-Sesiones de salón conducidas por jefes de departamentos.
-El nivel del empleado en la organización.
-Practicar el aprendizaje.

PREPARAR EL CONTENIDO DEL CURSO Y EL CALENDARIO.

Indicar lo siguiente:
-Secuencia de presentación.
-Tiempo estimado por tipo de sesión.
-Tiempo anticipado para ejcutar los cursos.

DETERMINAR SECUENCIA Y CONTENIDO POR CADA TOPICO.

Cada sesión deberá cubrir un tópico lógico y completo ó grupo de tópicos. No deberá haber más de dos tópicos diferentes por sesión.

PREPARAR MATERIALES DE CAPACITACION.

Estos materiales pueden ser preparados de acuerdo a la estructura de la sesión. Estos pueden ser:

-Partes de los procedimientos relevantes del Plan de Contingencias.
-Cartas del comité.
-Copias.
-Ejemplos.
-Lecturas relevantes.
-Guías ó calendarios para actividades individuales y de grupo.
-Hojas para tomar nota.

CALENDARIO Y CONDUCCION DE LA CAPACITACION POR EL INSTRUCTOR.

Preparar el calendario considerando:

-Un lugar para el curso.
-Audio-Visual y otros equipos disponibles.
-Preparación y distribución del material del curso.

EVALUAR Y MODIFICAR EL PROGRAM DE CAPACITACION COMO SEA NECESARIO.

Observar la reacción del participante al curso y evaluar al instructor sobre la presentación y materiales, si es necesario modificar el curso.

DEFINIR RESPONSABILIDADES PARA LA PRESENTACION Y MANTENIMIENTO DE LOS CURSOS Y MATERIALES.

El Coordinador de la recuperación de la organización deberá ser responsable de la asignación de tareas relacionadas para la presentación y mantenimiento del curso.

5.5.2.3 PRUEBAS DE DIRECCION Y EVALUACION.

Probar el Plan de Contingencias y evaluar la exactitud del plan, así como sus resultados.
En la evaluación de los resultados de las pruebas,los participantes deberán involucrar una sesión de discusión en grupo.
Los resultados de la prueba deberán ser comparados con los objetivos predefinidos en la prueba.

NOTIFICAR AL PERSONAL INVOLUCRADO EN EL CALENDARIO DE PRUEBAS.

Las pruebas del Plan de Contingencias deberán ser conducidas con un número de observadores quienes pueden registrar todas las desviaciones desde los procedimientos de recuperación documentados.
Por cada prueba, notificar a los participantes y observadores del tiempo, lugar y expectativas.
También es apropiado informar a los participantes de la naturaleza de la pruebas y los objetivos.

CONDUCIR Y DOCUMENTAR PRUEBAS.
Conducir las pruebas planeadas para evitar desviaciones.
Asegurarse de que el equipo de recuperación se familiarize con todos los procedimientos relatados en el plan.

ARCHIVO DE RESULTADOS DE PRUEBAS.
Documentar todas las pruebas en un archivo. Este es usado durante auditorías para indicar que las pruebas del Plan de Contingencias han sido realizadas.
Alguna evidencia por alteraciones requeridas deberá ser incluida. Cada prueba deberá ser identificada por número y nombre.

5.5.2.4 PREPARAR PROCEDIMIENTOS DEL PLAN DE PRUEBAS

Preparar procedimientos para su incorporación dentro del Plan de Contingencias. Los tipos de prueba, frecuencia y procedimientos detallando los pasos a ser tomados para documentar.

DETERMINAR FRECUENCIA DE PRUEBAS A SER CONDUCIDAS.
Determinar cuales pruebas del Plan de Contingencias son incluidas sobre una base regular, (evacuación y procedimientos de ensamble).
Determinar cada cuando las pruebas serán conducidas, puede ser cada cuatro años ó en años alternativos.

Prepara calendario de pruebas.

DOCUNENTAR PROCEDIMIENTOS DE PRUEBAS.
Preparar procedimientos detallados de pruebas describiendo como conducirlas y evaluar los resultados.

Documentar el método por el cual las pruebas son diseñadas. Preparar procedimientos de pruebas estructurados para su incorporaciónen el Plan de Contingencias.

5.5.2.5 PREPARAR PROCEDIMIENTOS DEL PLAN DE MANTENIMIENTO

Preparar procedimientos para incluirse en el Plan de Contingencias.
Los pasos involucrados en el mantenimiento del Plan de Contingencias deberán ser documentados, incluyendo alguna aprobación.
Cada que existe una alteración ó cambio al Plan de Contingencias debe ser notificado y todas las copias deben ser modificadas y distribuidas y el procedimiento anterior debe ser destruido para asegurar que no exista confusión.

PREPARAR CALENDARIO PARA REVISIONES REGULARES DEL PLAN DE CONTINGENCIAS POR EL COORDINADOR DE LA RECUPERACION DE LA ORGANIZACION.
El coordinador de la recuperación de la organización deberá revisar el Plan de Contingencias regularmente para el mantenimiento requerido.
El material referenciado en el Plan de Contingecias para cada operación manual, deberá ser revisado periódicamente. Es importante que las aplicaciones automatizadas y el software de recuperación sea revisado, para asegurar los cambios en la configuración que han sido incorporados.

PREPARAR PROCEDIMIENTOS DE INCORPORACION DE ALTERACIONES AL PLAN DE CONTINGENCIAS.
Las alteraciones deberán ser incorporadas en el Plan de Contingencias. El coordinador de la recuperación de la organización deberá presentar las alteraciones para su aprobación. Discutir el mejor método de notificación.

DETERMINAR LA LISTA DE DISTRIBUCION DEL PLAN DE CONTINGENCIAS.
Cada copia del Plan de Contingencias que es distribuida, debe ser expedida bajo un código de identificación. Esto podrá asegurar que todas las copias son modificadas y expedidas, haciendo responsable a un empleado.

Las secciones confidenciales del Plan de Contingencia deberán únicamente ser incluidos en copias para el gerente.
Las otras copias deberán ser expedidas sin estas secciones.

También considerar la producción de todas las copias del Plan de Contingencias en papel colorido que no es generalmente usado en la organización y que sea difícil de fotocopiar.
El Coordinador de la recuperación de la organización será responsable de lo recibido por cada individuo.

5.5.2.6 REVISAR EL PLAN DE CONTINGENCIAS

Completar el Plan de Contingencias original.
El borrador inicial del Plan de Contingencias fue preparado basado en información obtenida durante las dos etapas previas.

REVISAR EL BORRADOR DEL PLAN DE CONTINGENCIAS DE ACUERDO CON LOS RESULTADOS DE LAS PRUEBAS.

Basado en las alteraciones requeridas documentadas, como resultado de las pruebas, modificar el borrador inicial del Plan de Contingencias.

INCORPORAR PROCEDIMIENTOS DE PRUEBA EN EL PLAN DE CONTINGENCIAS.
Incluir los procedimientos de prueba preparados en el Plan de Contingencias como una sección separada. Esta deberá incluir calendarios de prueba.

REVISION FINAL DEL PLAN DE CONTINGENCIA CON EL GERENTE.
El Plan de Contingencias final es completado, presentarlo al gerente, discutirlo.

DISTRIBUCION DE COPIAS DEL PLAN DE CONTINGENCIAS ORIGINAL FORMAL.
Distribuir copias del Plan de Contingencias de acuerdo a la lista de destribución.
Asegurar que una copia en disco duro ó en diskkete este almacenada fuera de la organización.

PUNTO DE APROBACION FORMAL.

CONCLUSIONES

Una vez que hemos evaluado las diferentes opciones para la recuperación, el Plan de Contingencias es la mejor opción, ya que permite conocer las deficiencias de la organización y sus principales amenazas. Este disminuye los costos de recuperación y ayuda a una eficiente puesta en marcha de la organización.

Después de haber planteado una metodología para la creación y puesta en marcha de un Plan de Contingencias, podemos recomendar lo siguiente para auditarlo:

La información del plan de contingencias deberá ser completa y precisa

El personal involucrado deberá estar capacitado para la recuperación.

El Plan de Contingencias se deberá encontrar almacenado en más de un lugar.

Las copias distribuidas deberán ser constantemente actualizadas.

Se debe actualizar el Plan de Contigencias por lo menos cada año.

El plan deberá ser probado mínimo una vez al año.

El Plan de Contingencias deberá ser probado con los procedimientos más críticos para la organización.

El usuario deberá ser involucrado en el desarrollo de los procedimientos de contingencia de su departamento.

El usuario deberá contemplar cuánto tiempo puede estar sin un sistema automatizado.

Identificar todas las aplicaciones críticas

Verificar que sean efectivos los procedimientos documentados:
a) Minuciosos
b) Exactos
c) Comprensibles

El Plan deberá detallar los grados de desastre.

El plan deberá contener acciones específicas para cada uno de los grados de desastre.

El Plan deberá contener los números telefónicos de aquellas personas que han sido incluidas para su aplicación.

El plan deberá contener contactos de emergencia con los proveedores requeridos.

Mencionar el nombre de la persona que estaría a cargo de la puesta en marcha del plan, en caso de desastre.

Cada persona involucrada en la responsabilidad de un desastre deberá contar con una copia del plan.

Cada persona involucrada en la puesta en marcha del plan deberá estar capacitada y tener las habilidades para desarrollar su función en el momento en que sea requerido.

Deberá mencionar un lugar alternativo al propio para el momento de la contingencia.

El plan de contingencias deberá tomar en cuenta:

a) Edificio
b) Ventilación (aire acondicionado)
c) Fuente de poder ininterruptible
d) Personal
e) Comunicaciones
f) Seguridad
g) Hardware y software

Los usuarios deberán estar de acuerdo en mantener los costos de recuperación.

Los usuarios deberán tener preparado su propio plan de contingencias, detallando las prioridades para ser restauradas.

La alta gerencia debe darse cuenta de la importancia del plan de contingencias.

La cobertura del seguro deberá ser acorde con los requerimientos contemplados en el plan de contingencias.

En caso de que se tenga un acuerdo entre dos organizaciones para proporcionarse ayuda mutua:
Se deberá encontrar por escrito el acuerdo.
Se deberá revisar constantemente que ambos sistemas sean compatibles.

En caso de que se cuente con un Centro de cómputo básico:
Contemplar a que distancia se encuentra.
Qué tiempo tomará obtener el equipo de hardware adecuado, e instalarlo.

En caso de que se tenga contemplado un centro de respaldo de emergencia:
Verificar que la cobertura del contrato es suficiente
Contemplar cuánto tiempo se tardará en instalarse el centro.

Si existe un centro de cómputo propio en caso de desastre:
Se deberá revisar la carga de trabajo para el centro auxiliar y no debera ser crftica.
Contemplar si cuenta con suficientes lfneas telefónicas.

BIBLIOGRAFIA.

1) LIC. JOSE ANTONIO ECHENIQUE
AUDITORIA EN INFORMATICA
McGRAW HILL

2) RON WEBER
EDP AUDITING, CONCEPTUAL FUNDATIONS AND PRACTICE
SECOND EDITION 1988. PAG.9-11

3) MAIR WILLIAM C. WOOD DONALD R. KEAGLE DAVIS W.
COMPUTER CONTROL & AUDIT
INSTITUTE OF INTERNAL AUDITORS
USA 1978, PAG. 17

4) SYSTEM MANAGEMENT METHODOLOGY
DISASTER CONTINGENCY PLANINIG OVERVIEW AND BASELINE
VERSION 1.0
1992 PRICE WATERHOUSE

5) THE INSTITUTE OF INTERNAL AUDITORS RESEARCH FOUNDATION
MODULO 9. SECURITY
INTERNATIONAL BUSINESS MACHINES CORPORATION
1991

6) EDP
CONTROLS AND AUDITING
SECOND EDITION
W. THOMAS PORTER
TAUCHE ROSS
WILLIAM E. PERRY
INSTITUTE OF INTERNAL AUDITORS

7) CONTINGENCY PLANING
BROADBENT D.
NCC PUBLICATIONS 1980

8) COMPUTER SEGURITY: A MANAGEMENT AUDITING APPROACH
AMACOM, 1980
ENGER, NORMAN L. Y HOWERTON

9) COMPUTER FRAUD AND COUNTERMEASURES
KRAUSS, LEONAD Y MACGATIAN AILEEN
PRENYICE HALL 1979

10) COMPUTER SEGURITY: RISK ANALYSIS AND CONTROL
NCC PUBLICATIONS

11) SQUIRES .T. COMPUTER SEGURITY: THE PERSONNEL
ASPECT, NCC PUBLICATIONS. 1980

12) SEGURIDAD DE CENTROS DE COMPUTO
POLITICAS Y PROCEDIMIENTOS
EDITORIAL TRILLAS
LEONARD H.FINE
2DA. EDICION JUNIO DE 1990

13) INFORMATICA PRESENTE Y FUTURO
DONALD H. SANDERS
MC. GRAW HILL