CAPÍTULO V

SEGURIDAD EN CENTROS DE CÓMPUTO

ORDEN EN EL CENTRO DE CÓMPUTO

Una dirección de Sistemas de Información bien administrada debe tener y observar reglas relativas al orden y cuidado del departamento de cómputo. Los dispositivos del sistema de cómputo, los archivos magnéticos, pueden ser dañados si se manejan en forma inadecuada y eso puede traducirse en pérdidas irreparables de información o en costos muy elevados en la reconstrucción de archivos. Se deben revisar las disposiciones y reglamentos que coadyuven al mantenimiento del orden dentro del departamento de cómputo.

1. Indique la periodicidad con que se hace la limpieza del departamento de cómputo y de la cámara de aire que se encuentra abajo del piso falso si existe y los ductos de aire:
Semanalmente ( ) Quincenalmente ( )
Mensualmente ( ) Bimestralmente ( )
No hay programa ( ) Otra (especifique) ( )
2. Existe un lugar asignado a las cintas y discos magnéticos?
SI ( ) NO ( )
3. ¿Se tiene asignado un lugar especifico para papelería y utensilios de trabajo?
SI ( ) NO ( )
4. ¿Son funcionales los muebles asignados para la cintoteca y discoteca?
SI ( ) NO ( )
5. ¿Se tienen disposiciones para que se acomoden en su lugar correspondiente, después de su uso, las cintas, los discos magnéticos, la papelería, etc.?
SI ( ) NO ( )
6. Indique la periodicidad con que se limpian las unidades de cinta:
Al cambio de turno ( ) cada semana ( )
cada día ( ) otra (especificar) ( )
7. ¿Existen prohibiciones para fumar, tomar alimentos y refrescos en el departamento de cómputo?
SI ( ) NO ( )
8. ¿Se cuenta con carteles en lugares visibles que recuerdan dicha prohibición?
SI ( ) NO ( )
9. ¿Se tiene restringida la operación del sistema de cómputo al personal especializado de la Dirección de Informática?
SI ( ) NO ( )
10. Mencione los casos en que personal ajeno al departamento de operación opera el sistema de cómputo:

EVALUACIÓN DE LA CONFIGURACIÓN DEL SISTEMA DE CÓMPUTO

Los objetivos son evaluar la configuración actual tomando en consideración las aplicaciones y el nivel de uso del sistema, evaluar el grado de eficiencia con el cual el sistema operativo satisface las necesidades de la instalación y revisar las políticas seguidas por la unidad de informática en la conservación de su programoteca.

Esta sección esta orientada a:
a) Evaluar posibles cambios en el hardware a fin de nivelar el sistema de cómputo con la carga de trabajo actual o de comparar la capacidad instalada con los planes de desarrollo a mediano y lago plazo.
b) Evaluar las posibilidades de modificar el equipo para reducir el costo o bien el tiempo de proceso.
c) Evaluar la utilización de los diferentes dispositivos periféricos.

1. De acuerdo con los tiempos de utilización de cada dispositivo del sistema de cómputo, ¿existe equipo?
¿Con poco uso? SI ( ) NO ( )
¿Ocioso? SI ( ) NO ( )
¿Con capacidad superior a la necesaria? SI ( ) NO ( )
Describa cual es _____
2. ¿El equipo mencionado en el inciso anterior puede reemplazarse por otro mas lento y de menor costo?
SI ( ) NO ( )
3. Si la respuesta al inciso anterior es negativa, ¿el equipo puede ser cancelado?
SI ( ) NO ( )
4. De ser negativa la respuesta al inciso anterior, explique las causas por las que no puede ser cancelado o cambiado.
_____
5. ¿El sistema de cómputo tiene capacidad de teleproceso?
SI ( ) NO ( )
6. ¿Se utiliza la capacidad de teleproceso?
SI ( ) NO ( )
7. ¿En caso negativo, exponga los motivos por los cuales no utiliza el teleproceso?
SI ( ) NO ( )
8. ¿Cuantas terminales se tienen conectadas al sistema de cómputo?

9. ¿Se ha investigado si ese tiempo de respuesta satisface a los usuarios?
SI ( ) NO ( )
10. ¿La capacidad de memoria y de almacenamiento máximo del sistema de cómputo es suficiente
para atender el proceso por lotes y el proceso remoto?
SI ( ) NO ( )

SEGURIDAD LÓGICA Y CONFIDENCIAL

La computadora es un instrumento que estructura gran cantidad de información, la cual puede ser confidencial para individuos, empresas o instituciones, y puede ser mal utilizada o divulgada a personas que hagan mal uso de esta. También pueden ocurrir robos, fraudes o sabotajes que provoquen la destrucción total o parcial de la actividad computacional.
Esta información puede ser de suma importancia, y el no tenerla en el momento preciso puede provocar retrasos sumamente costosos. Antes esta situación, en el transcurso del siglo XX, el mundo ha sido testigo de la transformación de algunos aspectos de seguridad y de derecho.

En la actualidad y principalmente en las computadoras personales, se ha dado otro factor que hay que considerar el llamado ""virus" de las computadoras, el cual aunque tiene diferentes intenciones se encuentra principalmente para paquetes que son copiados sin autorización ("piratas") y borra toda la información que se tiene en un disco.
Al auditar los sistemas se debe tener cuidado que no se tengan copias "piratas" o bien que, al conectarnos en red con otras computadoras, no exista la posibilidad de transmisión del virus.

El uso inadecuado de la computadora comienza desde la utilización de tiempo de máquina para usos ajenos de la organización, la copia de programas para fines de comercialización sin reportar los derechos de autor hasta el acceso por vía telefónica a bases de datos a fin de modificar la información con propósitos fraudulentos.
Un método eficaz para proteger sistemas de computación es el software de control de acceso. Dicho simplemente, los paquetes de control de acceso protegen contra el acceso no autorizado, pues piden del usuario una contraseña antes de permitirle el acceso a información confidencial. Dichos paquetes han sido populares desde hace muchos años en el mundo de las computadoras grandes, y los principales proveedores ponen a disposición de clientes algunos de estos paquetes.

El sistema integral de seguridad debe comprender:

- Elementos administrativos
- Definición de una política de seguridad
- Organización y división de responsabilidades
- Seguridad física y contra catástrofes (incendio, terremotos, etc.)
- Prácticas de seguridad del personal
- Elementos técnicos y procedimientos
- Sistemas de seguridad (de equipos y de sistemas, incluyendo todos los elementos, tanto redes como terminales.
- Aplicación de los sistemas de seguridad, incluyendo datos y archivos
- El papel de los auditores, tanto internos como externos
- Planeación de programas de desastre y su prueba.

Se debe evaluar el nivel de riesgo que puede tener la información para poder hacer un adecuado estudio costo/beneficio entre el costo por pérdida de información y el costo de un sistema de seguridad, para lo cual se debe considerar lo siguiente:

- Clasificar la instalación en términos de riesgo (alto, mediano, pequeño).
- Identificar aquellas aplicaciones que tengan un alto riesgo.
- Cuantificar el impacto en el caso de suspensión del servicio en aquellas aplicaciones con un alto riesgo.
- Formular las medidas de seguridad necesarias dependiendo del nivel de seguridad que se requiera.
- La justificación del costo de implantar las medidas de seguridad para poder clasificar el riesgo e identificar las aplicaciones de alto riesgo, se debe preguntar lo siguiente:
    - Que sucedería si no se puede usar el sistema?
    - Si la contestación es que no se podría seguir trabajando, esto nos sitúa en un sistema de alto riego.
- La siguiente pregunta es:
    - ¿Que implicaciones tiene el que no se obtenga el sistema y cuanto tiempo podríamos estar sin utilizarlo?
    - ¿Existe un procedimiento alterno y que problemas nos ocasionaría?
    - ¿Que se ha hecho para un caso de emergencia?

Una vez que se ha definido, el grado de riesgo, hay que elaborar una lista de los sistemas con las medias preventivas que se deben tomar, así como las correctivas en caso de desastre señalándole a cada uno su prioridad.
Hay que tener mucho cuidado con la información que sale de la oficina, su utilización y que sea borrada al momento de dejar la instalación que está dando respaldo.

Para clasificar la instalación en términos de riesgo se debe:

- Clasificar los datos, información y programas que contienen información confidencial que tenga un alto valor dentro del mercado de competencia de una organización, e información que sea de difícil recuperación.
- Identificar aquella información que tenga un gran costo financiero en caso de pérdida o bien puede provocar un gran impacto en la toma de decisiones.
- Determinar la información que tenga una gran pérdida en la organización y, consecuentemente, puedan provocar hasta la posibilidad de que no pueda sobrevivir sin esa información.

Para cuantificar el riesgo es necesario que se efectúen entrevistas con los altos niveles administrativos que sean directamente afectados por la suspensión en el procesamiento y que cuantifiquen el impacto que les puede causar este tipo de situaciones.

Para evaluar las medidas de seguridad se debe:

- Especificar la aplicación, los programas y archivos.
- Las medidas en caso de desastre, pérdida total, abuso y los planes necesarios.
- Las prioridades que se deben tomar en cuanto a las acciones a corto y largo plazo.

- En cuanto a la división del trabajo se debe evaluar que se tomen las siguientes precauciones, las cuales dependerán del riesgo que tenga la información y del tipo y tamaño de la organización.
    - El personal que prepara la información no debe tener acceso a la operación.
    - Los análisis y programadores no deben tener acceso al área de operaciones y viceversa.
    - Los operadores no deben tener acceso restringido a las librerías ni a los lugares donde se tengan los archivos almacenados; es importante separar las funciones de librería y de operación.
    - Los operadores no deben ser los únicos que tengan el control sobre los trabajos procesados y no deben hacer las correcciones a los errores detectados.

Al implantar sistemas de seguridad puede, reducirse la flexibilidad en el trabajo, pero no debe reducir la eficiencia.

SEGURIDAD FÍSICA

El objetivo es establecer políticas, procedimientos y prácticas para evitar las interrupciones prolongadas del servicio de procesamiento de datos, información debido a contingencias como incendio, inundaciones, huelgas, disturbios, sabotaje, etc. y continuar en medio de emergencia hasta que sea restaurado el servicio completo.
Entre las precauciones que se deben revisar están:

- Los ductos del aire acondicionado deben estar limpios, ya que son una de las principales causas del polvo y se habrá de contar con detectores de humo que indiquen la posible presencia de fuego.
- En las instalaciones de alto riesgo se debe tener equipo de fuente no interrumpible, tanto en la computadora como en la red y los equipos de teleproceso.
- En cuanto a los extintores, se debe revisar en número de estos, su capacidad, fácil acceso, peso y tipo de producto que utilizan. Es muy frecuente que se tengan los extintores, pero puede suceder que no se encuentren recargados o bien que sean de difícil acceso de un peso tal que sea difícil utilizarlos.
- Esto es común en lugares donde se encuentran trabajando hombres y mujeres y los extintores están a tal altura o con un peso tan grande que una mujer no puede utilizarlos.
- Otro de los problemas es la utilización de extintores inadecuados que pueden provocar mayor perjuicio a las máquinas (extintores líquidos) o que producen gases tóxicos.
- También se debe ver si el personal sabe usar los equipos contra incendio y si ha habido prácticas en cuanto a su uso.
- Se debe verificar que existan suficientes salidas de emergencia y que estén debidamente controladas para evitar robos por medio de estas salidas.
- Los materiales mas peligrosos son las cintas magnéticas que al quemarse, producen gases tóxicos y el papel carbón que es altamente inflamable.

Tomando en cuenta lo anterior se elaboro el siguiente cuestionario:
1. ¿Se han adoptado medidas de seguridad en el departamento de sistemas de información?
SI ( ) NO ( )
2. ¿Existen una persona responsable de la seguridad?
SI ( ) NO ( )
3. ¿Se ha dividido la responsabilidad para tener un mejor control de la seguridad?
SI ( ) NO ( )
4. ¿Existe personal de vigilancia en la institución?
SI ( ) NO ( )
5. ¿La vigilancia se contrata?
a) Directamente ( )
b) Por medio de empresas que venden ese servicio ( )
6. ¿Existe una clara definición de funciones entre los puestos clave?
SI ( ) NO ( )
7. ¿Se investiga a los vigilantes cuando son contratados directamente?
SI ( ) NO ( )
8. ¿Se controla el trabajo fuera de horario?
SI ( ) NO ( )
9. ¿Se registran las acciones de los operadores para evitar que realicen algunas pruebas que puedan dañar los sistemas?.
SI ( ) NO ( )
10. ¿Existe vigilancia en el departamento de cómputo las 24 horas?
SI ( ) NO ( )
11. ¿Existe vigilancia a la entrada del departamento de cómputo las 24 horas?
a) Vigilante? ( )
b) Recepcionista? ( )
c) Tarjeta de control de acceso ? ( )
d) Nadie? ( )
12. ¿Se permite el acceso a los archivos y programas a los programadores, analistas y operadores?
SI ( ) NO ( )
13. Se ha instruido a estas personas sobre que medidas tomar en caso de que alguien pretenda entrar sin autorización?
SI ( ) NO ( )
14. El edificio donde se encuentra la computadora esta situado a salvo de:
a) Inundación? ( )
b) Terremoto? ( )
c) Fuego? ( )
d) Sabotaje? ( )
15. El centro de cómputo tiene salida al exterior al exterior?
SI ( ) NO ( )
16. Describa brevemente la construcción del centro de cómputo, de preferencia proporcionando planos y material con que construido y equipo (muebles, sillas etc.) dentro del centro.
17. ¿Existe control en el acceso a este cuarto?
a) Por identificación personal? ( )
b) Por tarjeta magnética? ( )

c) por claves verbales? ( )
d) Otras? ( )
18. ¿Son controladas las visitas y demostraciones en el centro de cómputo?
SI ( ) NO ( )
19. ¿Se registra el acceso al departamento de cómputo de personas ajenas a la dirección de informática?
SI ( ) NO ( )
20. ¿Se vigilan la moral y comportamiento del personal de la dirección de informática con el fin de mantener una buena imagen y evitar un posible fraude?
SI ( ) NO ( )
21. ¿Existe alarma para
a) Detectar fuego (calor o humo) en forma automática? ( )
b) Avisar en forma manual la presencia del fuego? ( )
c) Detectar una fuga de agua? ( )
d) Detectar magnéticos? ( )
e) No existe ( )
22. ¿Estas alarmas están
a) En el departamento de cómputo? ( )
b) En la cintoteca y discoteca? ( )
23. ¿Existe alarma para detectar condiciones anormales del ambiente?
a) En el departamento de cómputo? ( )
b) En la cintoteca y discoteca? ( )
c) En otros lados ( )
24. ¿La alarma es perfectamente audible?
SI ( ) NO ( )
25.¿Esta alarma también está conectada
a) Al puesto de guardias? ( )
b) A la estación de Bomberos? ( )
c) A ningún otro lado? ( )
Otro_____
26. Existen extintores de fuego
a) Manuales? ( )
b) Automáticos? ( )
c) No existen ( )
27. ¿Se ha adiestrado el personal en el manejo de los extintores?
SI ( ) NO ( )
28. ¿Los extintores, manuales o automáticos a base de

TIPO	SI	NO
a) Agua,	( )	( )
b) Gas?	( )	( )
c) Otros	( )	( )

29. ¿Se revisa de acuerdo con el proveedor el funcionamiento de los extintores?
SI ( ) NO ( )
30. ¿Si es que existen extintores automáticos son activador por detectores automáticos de fuego?
SI ( ) NO ( )

31. ¿Si los extintores automáticos son a base de agua ¿Se han tomado medidas para evitar que el agua cause mas daño que el fuego?
SI ( ) NO ( )
32. ¿Si los extintores automáticos son a base de gas, ¿Se ha tomado medidas para evitar que el gas cause mas daño que el fuego?
SI ( ) NO ( )
33. ¿Existe un lapso de tiempo suficiente, antes de que funcionen los extintores automáticos para que el personal
a) Corte la acción de los extintores por
tratarse de falsas alarmas? SI ( ) NO ( )
b) Pueda cortar la energía Eléctrica SI ( ) NO ( )
c) Pueda abandonar el local sin peligro
de intoxicación SI ( ) NO ( )
d) Es inmediata su acción? SI ( ) NO ( )
34. ¿Los interruptores de energía están debidamente protegidos, etiquetados y sin obstáculos para alcanzarlos?
SI ( ) NO ( )
35. ¿Saben que hacer los operadores del departamento de cómputo, en caso de que ocurra una emergencia ocasionado por fuego?
SI ( ) NO ( )
36. ¿El personal ajeno a operación sabe que hacer en el caso de una emergencia (incendio)?
SI ( ) NO ( )
37. ¿Existe salida de emergencia?
SI ( ) NO ( )
38. ¿Esta puerta solo es posible abrirla:
a) Desde el interior ? ( )
b) Desde el exterior ? ( )
c) Ambos Lados ( )
39. ¿Se revisa frecuentemente que no esté abierta o descompuesta la cerradura de esta puerta y de las ventanas, si es que existen?
SI ( ) NO ( )
40. ¿Se ha adiestrado a todo el personal en la forma en que se deben desalojar las instalaciones en caso de emergencia?
SI ( ) NO ( )
41. ¿Se ha tomado medidas para minimizar la posibilidad de fuego:
a) Evitando artículos inflamables
en el departamento de cómputo? ( )
b) Prohibiendo fumar a los operadores
en el interior? ( )
c) Vigilando y manteniendo el
sistema eléctrico? ( )
d) No se ha previsto ( )
42. ¿Se ha prohibido a los operadores el consumo de alimentos y bebidas en el interior del departamento de cómputo para evitar daños al equipo?
SI ( ) NO ( )
43. ¿Se limpia con frecuencia el polvo acumulado debajo del piso falso si existe?
SI ( ) NO ( )

44. ¿Se controla el acceso y préstamo en la
a) Discoteca? ( )
b) Cintoteca? ( )
c) Programoteca? ( )
45. Explique la forma como se ha clasificado la información vital, esencial, no esencial etc.
46. ¿Se cuenta con copias de los archivos en lugar distinto al de la computadora?
SI ( ) NO ( )
47. Explique la forma en que están protegidas físicamente estas copias (bóveda, cajas de seguridad etc.) que garantice su integridad en caso de incendio, inundación, terremotos, etc.
48. ¿Se tienen establecidos procedimientos de actualización a estas copias?
SI ( ) NO ( )
49. Indique el número de copias que se mantienen, de acuerdo con la forma en que se clasifique la información:
0 1 2 3
50. ¿Existe departamento de auditoria interna en la institución?
SI ( ) NO ( )
51. ¿Este departamento de auditoria interna conoce todos los aspectos de los sistemas?
SI ( ) NO ( )
52. ¿Que tipos de controles ha propuesto?
53. ¿Se cumplen?
SI ( ) NO ( )
54. ¿Se auditan los sistemas en operación?
SI ( ) NO ( )
55.¿Con que frecuencia?
a) Cada seis meses ( )
b) Cada año ( )
c) Otra (especifique) ( )
56.¿Cuándo se efectúan modificaciones a los programas, a iniciativa de quién es?
a) Usuario ( )
b) Director de informática ( )
c) Jefe de análisis y programación ( )
d) Programador ( )
e) Otras (especifique) _____
57.¿La solicitud de modificaciones a los programas se hacen en forma?
a) Oral? ( )
b) Escrita? ( )
En caso de ser escrita solicite formatos,
58.Una vez efectuadas las modificaciones, ¿se presentan las pruebas a los interesados?
SI ( ) NO ( )
59.¿Existe control estricto en las modificaciones?
SI ( ) NO ( )
60.¿Se revisa que tengan la fecha de las modificaciones cuando se hayan efectuado?
SI ( ) NO ( )
61.¿Si se tienen terminales conectadas, ¿se ha establecido procedimientos de operación?
SI ( ) NO ( )
62.Se verifica identificación:
a) De la terminal ( )

b) Del Usuario ( )
c) No se pide identificación ( )
63.¿Se ha establecido que información puede ser acezada y por qué persona?
SI ( ) NO ( )
64.¿Se ha establecido un número máximo de violaciones en sucesión para que la computadora cierre esa terminal y se de aviso al responsable de ella?
SI ( ) NO ( )
65.¿Se registra cada violación a los procedimientos con el fin de llevar estadísticas y frenar las tendencias mayores?
SI ( ) NO ( )
66.¿Existen controles y medidas de seguridad sobre las siguientes operaciones?
¿Cuales son?
( )Recepción de documentos_____
( )Información Confidencial_____
( )Captación de documentos_____
( )Cómputo Electrónico_____
( )Programas_____
( )Discotecas y Cintotecas_____
( )Documentos de Salida_____
( )Archivos Magnéticos_____
( )Operación del equipo de computación_____
( )En cuanto al acceso de personal_____
( )Identificación del personal_____
( )Policia_____
( )Seguros contra robo e incendio_____
( )Cajas de seguridad_____
( )Otras (especifique)_____

SEGURIDAD EN LA UTILIZACIÓN DEL EQUIPO

En la actualidad los programas y los equipos son altamente sofisticados y sólo algunas personas dentro del centro de cómputo conocen al detalle el diseño, lo que puede provocar que puedan producir algún deterioro a los sistemas si no se toman las siguientes medidas:

1) Se debe restringir el acceso a los programas y a los archivos.
2) Los operadores deben trabajar con poca supervisión y sin la participación de los programadores, y no deben modificar los programas ni los archivos.
3) Se debe asegurar en todo momento que los datos y archivos usados sean los adecuados, procurando no usar respaldos inadecuados.
4) No debe permitirse la entrada a la red a personas no autorizadas, ni a usar las terminales.
5) Se deben realizar periódicamente una verificación física del uso de terminales y de los reportes obtenidos.
6) Se deben monitorear periódicamente el uso que se le está dando a las terminales.
7) Se deben hacer auditorías periódicas sobre el área de operación y la utilización de las terminales.

8) El usuario es el responsable de los datos, por lo que debe asegurarse que los datos recolectados sean procesados completamente. Esto sólo se logrará por medio de los controles adecuados, los cuales deben ser definidos desde el momento del diseño general del sistema.
9) Deben existir registros que reflejen la transformación entre las diferentes funciones de un sistema.
10) Debe controlarse la distribución de las salidas (reportes, cintas, etc.).
11) Se debe guardar copias de los archivos y programas en lugares ajenos al centro de cómputo y en las instalaciones de alta seguridad; por ejemplo: los bancos.
12) Se debe tener un estricto control sobre el acceso físico a los archivos.
13) En el caso de programas, se debe asignar a cada uno de ellos, una clave que identifique el sistema, subsistema, programa y versión.

También evitará que el programador ponga nombres que nos signifiquen nada y que sean difíciles de identificar, lo que evitará que el programador utilice la computadora para trabajos personales. Otro de los puntos en los que hay que tener seguridad es en el manejo de información. Para controlar este tipo de información se debe:

1) Cuidar que no se obtengan fotocopias de información confidencial sin la debida autorización.
2) Sólo el personal autorizado debe tener acceso a la información confidencial.
3) Controlar los listados tanto de los procesos correctos como aquellos procesos con terminación incorrecta.
4) Controlar el número de copias y la destrucción de la información y del papel carbón de los reportes muy confidenciales.
El factor más importante de la eliminación de riesgos en la programación es que todos los programas y archivos estén debidamente documentados.

El siguiente factor en importancia es contar con los respaldos, y duplicados de los sistemas, programas, archivos y documentación necesarios para que pueda funcionar el plan de emergencia.

- Equipo, programas y archivos
- Control de aplicaciones por terminal
- Definir una estrategia de seguridad de la red y de respaldos
- Requerimientos físicos.
- Estándar de archivos.
- Auditoría interna en el momento del diseño del sistema, su implantación y puntos de verificación y control.

SEGURIDAD AL RESTAURAR EL EQUIPO

En un mundo que depende cada día mas de los servicios proporcionados por las computadoras, es vital definir procedimientos en caso de una posible falta o siniestro. Cuando ocurra una contingencia, es esencial que se conozca al detalle el motivo que la

originó y el daño causado, lo que permitirá recuperar en el menor tiempo posible el proceso perdido. También se debe analizar el impacto futuro en el funcionamiento de la organización y prevenir cualquier implicación negativa.

En todas las actividades relacionadas con las ciencias de la computación, existe un riesgo aceptable, y es necesario analizar y entender estos factores para establecer los procedimientos que permitan analizarlos al máximo y en caso que ocurran, poder reparar el daño y reanudar la operación lo mas rápidamente posible.
En una situación ideal, se deberían elaborar planes para manejar cualquier contingencia que se presente.
Analizando cada aplicación se deben definir planes de recuperación y reanudación, para asegurarse que los usuarios se vean afectados lo menos posible en caso de falla o siniestro.

Las acciones de recuperación disponibles a nivel operativo pueden ser algunas de las siguientes:

- En algunos casos es conveniente no realizar ninguna acción y reanudar el proceso.
- Mediante copias periódicas de los archivos se puede reanudar un proceso a partir de una fecha determinada.
- El procesamiento anterior complementado con un registro de las transacciones que afectaron a los archivos permitirá retroceder en los movimientos realizados a un archivo al punto de tener la seguridad del contenido del mismo a partir de él reanudar el proceso.
- Analizar el flujo de datos y procedimientos y cambiar el proceso normal por un proceso alterno de emergencia.
- Reconfigurar los recursos disponibles, tanto de equipo y sistemas como de comunicaciones.

Cualquier procedimiento que se determine que es el adecuado para un caso de emergencia deberá ser planeado y probado previamente.
Este grupo de emergencia deberá tener un conocimiento de los posibles procedimientos que puede utilizar, además de un conocimiento de las características de las aplicaciones, tanto desde el punto técnico como de su prioridad, el nivel de servicio planeado y su influjo en la operación de la organización.
Además de los procedimientos de recuperación y reinicio de la información, se deben contemplar los procedimientos operativos de los recursos físicos como hardware y comunicaciones, planeando la utilización de equipos que permitan seguir operando en caso de falta de la corriente eléctrica, caminos alternos de comunicación y utilización de instalaciones de cómputo similares. Estas y otras medidas de recuperación y reinicio deberán ser planeadas y probadas previamente como en el caso de la información.
El objetivo del siguiente cuestionario es evaluar los procedimientos de restauración y repetición de procesos en el sistema de cómputo.
1) ¿Existen procedimientos relativos a la restauración y repetición de procesos en el sistema de cómputo?
SI ( ) NO ( )
2) ¿Enuncie los procedimientos mencionados en el inciso anterior?

3) ¿Cuentan los operadores con alguna documentación en donde se guarden las instrucciones actualizadas para el manejo de restauraciones?
SI ( ) NO ( )
En el momento que se hacen cambios o correcciones a los programas y/o archivos se deben tener las siguientes precauciones:
1) Las correcciones de programas deben ser debidamente autorizadas y probadas. Con esto se busca evitar que se cambien por nueva versión que antes no ha sido perfectamente probada y actualizada.
2) Los nuevos sistemas deben estar adecuadamente documentos y probados.
3) Los errores corregidos deben estar adecuadamente documentados y las correcciones autorizadas y verificadas.
Los archivos de nuevos registros o correcciones ya existentes deben estar documentados y verificados antes de obtener reportes.

PROCEDIMIENTOS DE RESPALDO EN CASO DE DESASTRE

Se debe establecer en cada dirección de informática un plan de emergencia el cual ha de ser aprobado por la dirección de informática y contener tanto procedimiento como información para ayudar a la recuperación de interrupciones en la operación del sistema de cómputo.
El sistema debe ser probado y utilizado en condiciones anormales, para que en casó de usarse en situaciones de emergencia, se tenga la seguridad que funcionará.
La prueba del plan de emergencia debe hacerse sobre la base de que la emergencia existe y se ha de utilizar respaldos.
Se deben evitar suposiciones que, en un momento de emergencia, hagan inoperante el respaldo, en efecto, aunque el equipo de cómputo sea aparentemente el mismo, puede haber diferencias en la configuración, el sistema operativo, en disco etc.

El plan de emergencia una vez aprobado, se distribuye entre personal responsable de su operación, por precaución es conveniente tener una copia fuera de la dirección de informática.
En virtud de la información que contiene el plan de emergencia, se considerará como confidencial o de acceso restringido.
La elaboración del plan y de los componentes puede hacerse en forma independiente de acuerdo con los requerimientos de emergencia, La estructura del plan debe ser tal que facilite su actualización.
Para la preparación del plan se seleccionará el personal que realice las actividades claves del plan. El grupo de recuperación en caso de emergencia debe estar integrado por personal de administración de la dirección de informática, debe tener tareas específicas como la operación del equipo de respaldo, la interfaz administrativa.
Los desastres que pueden suceder podemos clasificar así:
a) Completa destrucción del centro de cómputo,
b) Destrucción parcial del centro de cómputo,
c) Destrucción o mal funcionamiento de los equipos auxiliares del centro de cómputo (electricidad, aire, acondicionado, etc.)

d) Destrucción parcial o total de los equipos descentralizados
e) Pérdida total o parcial de información, manuales o documentación
f) Pérdida del personal clave
g) Huelga o problemas laborales.

El plan en caso de desastre debe incluir:

- La documentación de programación y de operación.
- Los equipos:
    - El equipo completo
    - El ambiente de los equipos
    - Datos y archivos
    - Papelería y equipo accesorio
    - Sistemas (sistemas operativos, bases de datos, programas).

El plan en caso de desastre debe considerar todos los puntos por separado y en forma integral como sistema. La documentación estará en todo momento tan actualizada como sea posible, ya que en muchas ocasiones no se tienen actualizadas las últimas modificaciones y eso provoca que el plan de emergencia no pueda ser utilizado.

Cuando el plan sea requerido debido a una emergencia, el grupo deberá:

- Asegurarse de que todos los miembros sean notificados,
- Informar al director de informática,
- Cuantificar el daño o pérdida del equipo, archivos y documentos para definir que parte del plan debe ser activada.
- Determinar el estado de todos los sistemas en proceso,
- Notificar a los proveedores del equipo cual fue el daño,
- Establecer la estrategia para llevar a cabo las operaciones de emergencias tomando en cuenta:
    - Elaboración de una lista con los métodos disponibles para realizar la recuperación
    - Señalamiento de la posibilidad de alternar los procedimientos de operación (por ejemplo, cambios en los dispositivos, sustituciones de procesos en línea por procesos en lote).
    - Señalamiento de las necesidades para armar y transportar al lugar de respaldo todos los archivos, programas, etc., que se requieren.
    - Estimación de las necesidades de tiempo de las computadoras para un periodo largo.

Cuando ocurra la emergencia, se deberá reducir la carga de procesos, analizando alternativas como:

- Posponer las aplicaciones de prioridad más baja,
- Cambiar la frecuencia del proceso de trabajos.
- Suspender las aplicaciones en desarrollo.

Por otro lado, se debe establecer una coordinación estrecha con el personal de seguridad a fin de proteger la información.
Respecto a la configuración del equipo hay que tener toda la información correspondiente al hardware y software del equipo propio y del respaldo.
Deberán tenerse todas las especificaciones de los servicios auxiliares tales como energía eléctrica, aire acondicionado, etc. a fin de contar con servicios de respaldo adecuados y reducir al mínimo las restricciones de procesos, se deberán tomar en cuenta las siguientes consideraciones:

- Mínimo de memoria principal requerida y el equipo periférico que permita procesar las aplicaciones esenciales.
- Se debe tener documentados los cambios de software.
- En caso de respaldo en otras instituciones, previamente se deberá conocer el tiempo de computadora disponible.

Es conveniente incluir en el acuerdo de soporte recíproco los siguientes puntos:

- Configuración de equipos.
- Configuración de equipos de captación de datos.
- Sistemas operativos.
- Configuración de equipos periféricos.

- Ver anexos al final del documento.