Seguridad contra incendios

La importancia de la seguridad física y contra incendios se reconoce desde hace mucho tiempo; éstas son áreas que tradicionalmente han recibido atención. Sin embargo, aunque hay un nivel aparente de efectividad, la protección real es, por lo general, inadecuada.

Tenemos que tener en cuenta los siguientes puntos:

- Ubicación y construcción del centro de computo.
- Aire acondicionado.
- Suministro d energía.
- Riesgo de inundación.
- Acceso.
- Protección, detección y extinción de incendios.
- Mantenimiento.

1.-Ubicación y construcción del centro de cómputo.

1.1- Ubicación

Una tradición pasada dictó que la adquisición de una computadora se debía difundir lo más posible. En consecuencia, muchas instalaciones de cómputo se colocaron dentro de atractivas paredes de vidrio y con un máximo de publicidad. Por lo general, estas instalaciones se ubican en avenidas principales que tenían gran afluencia de peatones y vehículos.

Las serias amenazas que se presentaron contra las instalaciones de cómputo cambiaron rápidamente esta situación. La ubicación de los centros de cómputo se ha vuelto cada vez más clandestina. La selección del local, también se ha vuelto más conservadora, y las computadoras se colocan más lejos de las áreas del tránsito de gran escala, tanto terrestre como aéreo. Aun así, muchas ubicaciones todavía se escogen según el criterio anterior.

1.2- Construcción

A pesar de que ha transcurrido casi una generación de usuarios de computadoras, los administradores han aprendido poca acerca de los requisitos de diseño para las instalaciones de alto nivel de seguridad.

La construcción del interior de la instalación de cómputo también tiene gran importancia. La división tradicional de las áreas casi nunca es la más adecuada para la seguridad. Muchas veces la lose de los terrenos, catalogada como inflamable, es combustible, y las divisiones a prueba de incendios no son las adecuadas para algunas áreas como la biblioteca de computación.

En cuanto al vidrio este debe de ser reforzado, a prueba de balas y de incendios.

1.3 Disposición

El objetivo primordial es, por lo general, el flujo eficiente del trabajo; la seguridad pasa a ser de importancia secundaria. El área de recepción y distribución de datos es de alto riesgo y la más susceptible de sufrir ataques externos; por lo tanto debe estar aislada, hasta donde sea posible, de las áreas componentes de alto riesgo de las instalaciones, como las de captura de datos y procesamiento.

2. Aire Acondicionado

En todas las instalaciones existen grandes problemas con el aire acondicionado; el riesgo que éste implica es doble:

1. El aire acondicionado es indispensable en el lugar donde la computadora trabaje; las fluctuaciones o los desperfectos de consideración pueden ocasionar que la computadora tenga que ser apagada.
2. las instalaciones de aire acondicionado son una fuente de incendios muy frecuentes y también son muy susceptibles al ataque físico, especialmente a través de los ductos.

Para poder afrontar estos riesgos se requiere lo siguiente:

- Se deben instalar equipos de aire acondicionado de respaldo donde ya se hayan establecido las aplicaciones de alto riesgo.
- Se deben instalar redes de protección en todo el sistema de ductos al interior de y exterior.
- Se deben instalar extinguidotes y detectores de incendios en los ductos.
- Se deben instalar monitores y alarmas de sonido efectivas.

3. Suministro de Energía

El suministro de energía para el aire acondicionado, la computadora y el equipo de captura de datos, es importante. En las instalaciones de alto riesgo, especialmente las que cuentan con procesamiento en línea o de tiempo real, el suministro de respaldo es indispensable.

La continuidad del suministro de energía no es el único aspecto. La estabilidad es lo más importante. Es por eso que el centro debe de contar con reguladores de energía para que no se presenten problemas de variación de voltaje.

4. Riesgo de inundación

En lugares donde el riesgo de inundación es grande, las computadoras no se deben de colocar en sótanos o en las áreas de planta baja sino, de preferencia, en las partes altas de una estructura de varios pisos. La mejor opción es no colocar las computadoras en áreas donde el riesgo de inundación sea evidente.

No siempre las inundaciones son por causas de ríos ó naturales, sino pro la mala ubicación de las cañerías, las cuales, sino se ubican de manera adecuada pueden causar bloqueos de drenajes o la ruptura de las mismas.

Para poder solucionar este problema se deben de instalar detectores de agua o de inundación, así como también bombas de emergencia para resolver inundaciones inesperadas.

5. Acceso

5.1 Controladores de acceso durante las distintas horas del día o de la noche

Es importante asegurar que los controles durante la noche sean tan estrictos como durante el día. Los controles durante los descansos y cambios de turno son de especial importancia.

5.2 Acceso a terceras personas

Dentro de las terceras personas se incluyen a los ingenieros de aire acondicionado y de computación, los visitantes y el personal de limpieza. Estos y cualquier otro personal ajeno a la instalación debe ser:

- Identificados plenamente.
- Controlados y vigilados en sus actividades durante el acceso.

5.3 Estructura y disposición del área de recepción

En la mayoría de las instalaciones de alta seguridad hay dos o tres niveles de seguridad física para proteger el acceso al área de recepción.

El primer nivel de protección consiste en una barda de seguridad de gran visibilidad alrededor de la instalación, lo cual causa con frecuencia una falsa sensación de seguridad en la empresa, especialmente cuando las personas que trabajan dentro de ella ya fueron exoneradas desde el punto de vista de la seguridad.

5.4 Alarmas contra robos

Las alarmas contra robo, las armaduras y el blindaje se deben usar, hasta donde sea posible, en forma discreta, de manera que no se atraiga la atención sobre el hecho de que existe un dispositivo de alta seguridad.

5.5 Tarjetas de acceso y gafetes

En la actualidad, estos recursos son una forma muy popular de control de acceso. No obstante, los gafetes integrados con sistemas de tarjetas de acceso constituyen un valor adicional.

El acceso físico se debe reforzar y apoyar mediante otros elementos de seguridad.

6. Detección de incendios

Para la detección de incendios se deben de considerar 5 puntos.

1.- Utilizar detectores de fuego y humo se deben colocar cuidadosamente en relación con los aparatos de aire acondicionado, ya que los conductores de éste pueden difundir el calor o el humo y no permitir que se active el detector.

2.- El detector de humo que se elija, debe ser capaz de detectar los distintos tipos de gases que desprendan los cuerpos en combustión.

3.- Los detectores de humo y calor se deben instalar en la sala de computo, junto a las áreas de oficinas y en el perímetro físico de las instalaciones.

4.- Es necesario colocar detectores de humo y calor bajo el piso en los ductos del aire acondicionado.

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

7. Protección contra incendios

Se necesitan lugares especiales de almacenamiento para las cintas y los discos magnéticos que se usan en la instalación o en puntos distantes.

Se debe poner atención para cerciorarse de que los recursos que se ofrecen satisfagan los estándares mínimos de la Asociación de seguros contra incendios y de otros institutos.

Se debe de mantener actualizada toda la documentación y tener copias de seguridad de todos los programas y archivos.

8. Extinción de incendios

En la mayoría de las instalaciones se utiliza algún gas como extintor. El uso del bióxido de carbono se ha generalizado, aunque con reservas, debido al efecto letal que tiene sobre los humanos.

El uso del gas como extintor es de utilidad dudosa en las instalaciones que ocupan varias estructuras. Sin embargo, la efectividad de este tipo de extinguidotes es alta cuando el incendio comienza en la sala de cómputo.

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.

La participación del equipo de bomberos puede ser muy valiosa. Sin embargo, muchas brigadas todavía trabajan de manera tradicional y se necesita instruirlas cuidadosamente respecto a sus acciones.

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. Ya que las cintas magnéticas quemadas despiden humo nocivo.

9. Mantenimiento

La limpieza de la instalación de cómputo es importante desde dos puntos de vista:

1.- Refleja una actitud disciplinada. La seguridad es en gran parte una actitud mental y se refleja en el hecho de que los procedimientos adecuados y efectivos estén en uso.

2.- El mal mantenimiento crea las puertas y las ventanas no cierran correctamente; o bien, propicia incendios, por ejemplo, al dejar papeleras o cajas en los rincones de la salas.

PLANES Y SIMULACROS PARA LA RECUPERACIÓN EN CASO DE DESASTRES

Es notorio que la mayoría de las compañías piensen que cuentan con planes adecuados de recuperación en casos de desastres, y que cubren todas las categorías de desastre. La realidad es que la mayor parte de esos planes son superficiales, no estructurados e inadecuados para afrontar las complicaciones que surgen de un desastre real.

Muchas empresas llevan a cabo lo que describen como simulacros de desastre; estos tienen en principio la forma de procesar el trabajo en una máquina de respaldo.

Una institución financiera, dotada de grandes sistemas en línea, solía cuestionar con frecuencia la viabilidad de cualquier simulacro de recuperación en caso de desastre. La base de este argumento consistía en que no era posible contemplar la indisponibilidad de los sistemas por una hora, mucho menos uno o dos días.

Después de un análisis detallado se encontró que se podía realizar un simulacro de desastre significativo mediante el establecimiento de una corriente de procesamiento paralela, operada sobre la base de que ocurriera un desastre. Este simulacro incluía una verificación total de las redes, los interruptores del equipo auxiliar, etc.; fue un ejercicio muy complejo pero logró imitar el posible impacto de un desastre real.

Una de las grandes objeciones a los simulacros de desastres es el costo. Este varía, según la frecuencia con que se realicen estas pruebas. Si se trabaja sobre un promedio de dos a tres veces al año para las instalaciones grandes, el costo no resulta elevado.

1.- TIPOS DE DESASTRE

Al considerar los planes y los simulacros de desastre, se necesita delinear los distintos tipos de desastre que pueden ocurrir:

1. Destrucción completa de los recursos centralizados de procesamiento de datos.
2. Destrucción parcial de los recursos centralizados de procesamiento de datos
3. Destrucción o mal funcionamiento de los recursos ambientales Destinados al procesamiento centralizado de datos; por ejemplo, aire acondicionado, energía, etc.
4. Destrucción total o parcial de los recursos descentralizados de Procesamiento de datos.
5. Destrucción total o parcial de los procedimientos manuales del usuario, utilizados para la captura de *la información de entrada* para los sistemas de cómputo.
6. Pérdida del personal de cómputo clave
7. Interrupción por huelga

2.- ALCANCE DE LA PLANEACIÓN CONTRA DESASTRES

La planeación contra desastres debe abarcar tanto las aplicaciones en proceso de desarrollo como las operativas. En el caso de las ultimas, existen ciertas áreas que necesitan protección en caso de desastre o ciertos recursos que deben estar disponibles para la recuperación:

1. Documentación de los sistemas, la programación y las operaciones.
2. Recursos de procesamiento que incluyen:
   -Todo tipo de equipo
   -Ambiente para el equipo
   -Datos y archivos
   -Programas
   -Papelería

Los procedimientos de planificación contra desastres tendrán que definir en forma detallada los arreglos que se hagan para cada caso, la organización y las responsabilidades para aplicarlos y un marco de trabajo para la iniciación y aplicación paso por paso de los procedimientos de recuperación.

3.- APLICACIONES EN EL PROCESO DE DESARROLLO

En el análisis de los proyectos de cómputo indica un crecimiento de tamaño en ellos, aunque en la actualidad estén quizá mejor estructurados.

En términos teóricos, un desastre se puede presentar en cualquier etapa del desarrollo de una aplicación. No obstante, el desastre tiende a suceder cuando la aplicación está casi terminada pero la documentación no está completa.

En cada punto de verificación o pausa del proyecto, es importante que se lleve a cabo una revisión cuidadosa a fin de asegurar que existe una adecuada protección contra desastres.

4.- APLICACIONES TERMINADAS

4.1. *Sistemas y programación*

Esta es un área deficiente. Las aplicaciones se encuentran en cambio constante todo el tiempo y, en muchos casos, la documentación no se modifica para reflejar lo que sucede en la práctica.

Por la tanto, los planes contra desastres no solo deben considerar la existencia de tal documentación sino también las consecuencias que puede traer el que esta documentación se pierda.

4.2 *Operaciones de procesamiento*

Comprenden el sistema completo desde el momento que se presta el servicio solicitado o se produce el informe. En consecuencia, la planeación contra desastres debe incluir las actividades y los procedimientos del usuario, los recursos de transmisión y redes, el procesamiento centralizado y la redistribución de los resultados a los puntos de usuarios.

4.2.1. *Equipo*

La planeación contra desastres debe cubrir el equipo que se utiliza en cada etapa del proceso del sistema:

-Equipo de terminales o de entrada de datos
-Equipo de procesamiento
-Equipo ambiental, es decir, aire acondicionado, energía, etc.
-Recursos de distribución y arreglos incluyendo red y terminales
-Guillotinas, desintercaladoras y cortadoras

4.2.2. *Datos y archivos*

Cada aplicación se debe revisar con mucho cuidado y también se deben realizar los arreglos necesarios para datos y archivos. Un aspecto que con frecuencia se descuida consiste en que existe una cantidad considerable de datos para transacciones. Debido a que la recaptura de estos datos puede requerir mucho tiempo, es importante guardarlos en forma legible por el computador.

4.2.3. *Papelería*

El surtido continuo de papelería requiere un lapso considerable entre el pedido y la entrega. Se necesita contar con existencias de papelería de emergencia, las cuales de deberán guardar en otro lugar para evitar las dificultades que traería la destrucción del depósito central de papelería que incluye;

-Datos fuente
-Documentación de informes y resultados, por ejemplo, facturas y balances.

5.- SIMULACROS DE DESASTRES

Los simulacros contra desastres son importantes por:

1. Se prueban la conciencia y preparación del personal para afrontar el desastre
2. Se identifican las omisiones en los planes contra desastres
3. El elemento sorpresa de los simulacros de desastres constituye una buena verificación moral para garantizar que se encuentren vigentes.

5.1. *Frecuencia de los simulacros de desastre*

Los simulacros se deben realizar de manera esporádica. Los simulacros no se deben anunciar. La planeación de estos requiere que una o dos personas sepan de su realización y guarden el secreto, de otra forma el elemento sorpresa se pierde.
Los simulacros de desastre necesitan de la experiencia y se sugiere que se realicen en un momento relativamente conveniente. Pero los desastres reales rara vez ocurren en momentos convenientes, por lo que después de una o dos pruebas, se debe realizar el simulacro en un momento muy inconveniente, por ejemplo, cuando haya exceso de trabajo.

5.2. *Forma del simulacro de desastre*

La prueba de desastre adquiere la forma de un desastre simulado. Se anuncia que un desastre de cierto tipo, por ejemplo, incendio o accidente, ha ocurrido y se instruye a los empleados para que sigan los procedimientos contra desastres. Lo siguiente debe ocurrir:

1) Todo el trabajo debe cesar en forma temporal, de tal manera que se tome nota del estado del procesamiento
2) Se debe completar un inventario de cualquier información que haya s sido destruida a causa del desastre.
3) Ya que se hizo esto, el trabajo puede recompensar aunque de vez en Cuando es preferible continuar el simulacro durante el uso del equipo de respaldo.

5.3. *Análisis del impacto*

Se reúne el siguiente inventario:

1. Las aplicaciones en desarrollo
2. Las aplicaciones operativas, en proceso o no.
3. La información perdida
4. El informe de la respuesta del personal y los detalles sobre el conocimiento inapropiado
5. La cuantificación de la pérdida por la destrucción de información o la interrupción del proceso
6. La efectividad de los procedimientos de recuperación y respaldo, basados en el uso real de información y equipo de respaldo

Una vez reunido esto, se debe realizar un análisis cuidadoso de las debilidades detectadas durante el simulacro. Se debe formular un plan de acción detallado para la aplicación de los cambios que garanticen mayor protección en caso de un desastre real