CAPITULO VI

VI. EVALUACIÓN DE LA SEGURIDAD

Introducción

Para muchos la seguridad sigue siendo el área principal a auditar, hasta el punto de que en algunas entidades se creó inicialmente la función de auditoría informática para revisar la seguridad, aunque después se hayan ido ampliando los objetivos.

Ya sabemos que puede haber seguridad sin auditoría, puede existir auditoría de otras áreas, y queda un espacio de encuentro: la auditoría de la seguridad y cuya área puede ser mayor o menor según la entidad y el momento.

Lo cierto es que cada día es mayor la importancia de la información, especialmente relacionada con sistemas basados en el uso de tecnologías de la información y comunicaciones, por lo que el impacto de los fallos, los accesos no autorizados, la revelación de la información, y otras incidencias, tienen un impacto mucho mayor que hace unos años: de ahí la necesidad de protecciones adecuadas que se evaluarán o recomendarán en la auditoría de seguridad.

También es cierto que en muchos casos tan necesario o más que la protección de la información puede ser que las inversiones en sistemas y tecnologías de la información estén alineadas con las estrategias de la entidad, huyendo del enfoque de la tecnología por la tecnología.

La gran importancia del tema sobre seguridad, justifica la extensión de este ultimo capitulo y que en el se presentan los puntos de vista de Mario G. Piattini y Emilio del Peso, David H. Lee, Enrique Hernández y José Antonio Echenique entre otros, autores de gran prestigio y están a la vanguardia de todos los temas relacionados con la auditoría informática.

VI.1 Seguridad lógica y confidencialidad

Fuente: (http://www.monografias.com/trabajos/maudsist.shtml) Toro Oscar.

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 puede 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 1a 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 medidas 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 irrestringido 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.

VI.2 Seguridad lógica

Fuente: (http://www.monografias.com/trabajos11/siste/siste.shtml#eva) D'Sousa Carmen.

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.

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 conectamos 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 la 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.

La seguridad en la informática abarca los conceptos de seguridad física y seguridad lógica:

La seguridad física, se refiere a la protección del Hardware y de los soportes de datos, así como a la de los edificios e instalaciones que los albergan. Contempla las situaciones de Incendios, sabotajes, robos, catástrofes naturales, etc.

La seguridad lógica, se refiere a la seguridad de uso del software, a la protección de los datos, procesos y programas, así como la del ordenado y autorizado acceso de los usuarios a la información.

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 permitir1e 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.

Causas de realización de una Auditoría de Seguridad

Esta constituye la FASE 0 de la auditoría y el orden 0 de actividades de la misma.

El equipo auditor debe conocer las razones por las cuales el cliente desea realizar el Ciclo de Seguridad.

Puede haber muchas causas:

Reglas internas del cliente.
incrementos no previstos de costos.
obligaciones legales.
situación de ineficiencia global notoria. etc.

De esta manera el auditor conocerá el entorno inicial. Así, el equipo auditor elaborará el Plan de Trabajo.

VI.3 Riesgos y controles a auditar

Fuente: (http://www.monografias.com/trabajos 14/riesgosinfor/riesgosinfor2. shtml#do)
Cancelado González Alberto.

La función de la gestión de riesgos es identificar estudiar y e1iminar las fuentes de los eventos perjudiciales antes de que empiecen a amenazar los procesos informáticos.

La gestión de riesgos se divide generalmente en:

Estimación De Riesgos

La estimación de riesgos describe cómo estudiar los riesgos dentro de la planeación general del entorno informático y se divide en los siguientes pasos:

La identificación de riesgos genera una lista de riesgos capaces de afectar el funcionamiento normal del entorno informático.

El análisis de riesgos mide su probabilidad de ocurrencia y su impacto en la organización.

La asignación de prioridades a los riesgos.

Identificación De Riesgos

En este paso se identifican los factores que introducen una amenaza en la planificación del entorno informático. Los principales factores que se ven afectados son:

Creación de la p1anificación que incluye: Planificación excesivamente optimista, planificación con tareas innecesarias, y organización de un entorno informático sin tener en cuenta áreas desconocidas y la envergadura del mismo.

La organización y gestión, que incluye: Presupuestos bajos, El ciclo de revisión/decisión de las directivas es más lento de lo esperado.

El entorno de trabajo, que incluye: Mal funcionamiento de las herramientas de desarrollo, espacios de trabajo inadecuados y la curva de aprendizaje de las nuevas tecnologías es mas larga de lo esperado.

Las decisiones de los usuarios finales, que incluye: Falta de participación de los usuarios finales y la falta de comunicación entre los usuarios y el departamento de informática.

El personal contratado, que incluye: Falta de motivación, falta de trabajo en equipo y trabajos de poca calidad.

Los procesos, que incluye: La burocracia de control de ca1idad y la falta de entusiasmo.

Análisis De Riesgos

Una vez hayan identificado los riesgos en la planificación, el paso siguiente es analizarlos para determinar su impacto, tomando así las posibles alternativas de solución. La explicación de Análisis de riesgos se extenderá posteriormente.

Exposición A Riesgos

Una actividad útil y necesaria en el análisis de riesgos es determinar su nivel de exposición en cada uno de los procesos en que se hayan identificado.

Estimación De La Probabilidad De Perdida

Las principales formas de estimar la probabilidad de pérdida son las siguientes:

Disponer de la persona que está más familiarizada con el entorno informático para que estime la probabilidad de ocurrencia de eventos perjudiciales.

Usar técnicas Delphi o de consenso en grupo. El método Delphi consiste en reunir a un grupo de expertos para solucionar determinados problemas. Dicho grupo realiza la categorización individual de las amenazas y de los objetos del riesgo.

Utilizar la calibración mediante adjetivos, en la cuál las personas involucradas eligen un nivel de riesgo entre (probable, muy probable) y después se convierten a estimaciones cuantitativas.

Priorización De Riesgos

En este paso de la estimación de riesgos, se estiman su prioridad de forma que se tenga forma de centrar el esfuerzo para desarrollar la gestión de riesgos. Cuando se realiza la priorización (elementos de alto riesgo y pequeños riesgos), estos últimos no deben ser de gran preocupación, pues lo verdaderamente crítico se puede dejar en un segundo plano.

Control De Riesgos

Una vez que se hayan identificado los riesgos del entorno informático y analizando su probabilidad de ocurrencia, existen bases para controlados que son:

Planificación
Resolución de riesgos
Monitorización de riesgos

Planificación De Riesgos

Su objetivo, es desarrollar un plan que controle cada uno de los eventos perjudiciales a que se encuentran expuestas las actividades informáticas.

Resolución De Riesgos

La resolución de los riesgos está conformado por los métodos que controlan el problema de un diseño de controles inadecuado, los principales son:

Evitar el Riesgo: No realizar actividades arriesgadas.
Conseguir información acerca del riesgo.
Planificar el entorno informático de forma que si ocurre un riesgo, las actividades informáticas sean cumplidas.
Eliminar el origen del riesgo, si es posible desde su inicio.
Asumir y comunicar el riesgo.

VI.4 Encriptamiento

Fuente: http://www.aceproject.org/main/espanol/et/ete08.htm

El encriptamiento es una forma efectiva de disminuir los riesgos en el uso de tecnología.

Implica la codificación de información que puede ser transmitida vía una red de cómputo o un disco para que solo el emisor y el receptor la puedan leer.

En teoría, cualquier tipo de información computarizada puede ser encriptada. En la práctica, se le utiliza con mayor frecuencia cuando la información se transmite por correo electrónico o internet.

La información es encriptada por el emisor utilizando un programa para "confundir o entremezclar" la información utilizando un código "asegurado". El receptor descifra la información utilizando un código análogo exclusivo. Cualquier persona que intercepte el mensaje verá simplemente información entremezclada que no tendrá ningún sentido sin el código o llave necesaria.

Existen distintos tipos de encriptamiento y distintos niveles de complejidad para hacerlo. Como con cualquier código, los de encriptamiento pueden ser rotos si se cuenta con tiempo y recursos suficientes. Los altamente sofisticados niveles de encriptamiento con que se cuenta hoy en día hacen muy difícil descifrar la información encriptada.

Una forma muy común de encriptamiento son los sistemas criptográficos de llave pública-llave abierta. Este sistema utiliza dos llaves diferentes para cerrar y abrir los archivos y mensajes. Las dos llaves están matemáticamente ligadas. Una persona puede distribuir su llave pública a otros usuarios y uti1izarla para enviarle mensajes encriptados. La persona guarda en secreto la llave privada y la utiliza para decodificar los mensajes que le han enviado con la llave pública.

Otro elemento del encriptamiento es la autentificación el proceso de verificar que un archivo o mensaje no ha sido alterado a lo largo del trayecto entre el emisor y el receptor.

El encriptamiento de la información tiene distintos usos para propósitos electorales. Cuando se envía información sensible a través de una red pública, es recomendable encriptarla: Esto es particularmente importante cuando se envía información personal o sobre la votación a través de una red, en especial por internet o correo electrónico.

La tecnología para el encriptamiento está en constante evolución. Si se está considerando alguna de ella es recomendable consultar a un experto para asegurar que se está utilizando la más reciente.

VI.5 Seguridad del personal.

Fuente: http://apuntes.rincondeIvago.com/auditoria-de-sistemas-informaticos.html

Definición del acceso no autorizado

El acceso a los recursos de la red debe estar permitido a los usuarios autorizados. Esto sé llama acceso autorizado. Una amenaza común que afecta a muchos sitios es el acceso no autorizado a las instalaciones de cómputo. Este acceso puede tomar muchas formas, como el uso de la cuenta de otro usuario para tener acceso a la red y sus recursos. En general, se considera que el uso de cualquier recurso de la red sin permiso previo es un acceso no autorizado. La gravedad del acceso no autorizado depende del sitio y de la naturaleza de la perdida potencial. En algunos sitios, el solo hecho de conceder acceso a un usuario no autorizado puede causar daños irreparables por la cobertura negativa de los medios.

Algunos sitios, debido a su tamaño y visibilidad, pueden ser objetivos más frecuentes que otros. El Equipo de Respuesta de Emergencias de Computo (CERT) ha hecho la observación de que, en general, las universidades de prestigio, los sitios del gobierno y las zonas militares parecen atraer más intrusos. En la sección "Equipo de respuesta de seguridad", puede encontrarse mayor información acerca de CERT, así como sobre otras organizaciones similares.

Riesgo de revelación de información

La revelación de información, ya sea voluntaria o involuntaria, es otro tipo de amenaza. Usted debe determinar el valor y delicadeza de la información guardada en sus computadoras. En el caso de vendedores de hardware y software, el código fuente, los detalles de diseño, los diagramas y la información especifica de un producto representan una ventaja competitiva.

Los hospitales, las compañías de seguros y las instituciones financieras mantienen información confidencial, cuya revelación puede ser perjudicial para los clientes y la reputación de la empresa. Los laboratorios farmacéuticos pueden tener aplicaciones patentadas y no pueden arriesgarse a pérdidas causadas por robos.

A nivel del sistema, la revelación de un archivo de contraseñas de un sistema Unix puede volverlo vulnerable a accesos no autorizados en el futuro. Para muchas organizaciones, un vistazo, a una propuesta o un proyecto de investigación que represente muchos años de trabajo puede darle a su competidor una ventaja injusta.

Muchas veces, la gente supone que los accesos no autorizados de terceros a las redes y computadoras son realizadas por individuos que trabajan por su cuenta. No siempre es así. Los peligros del espionaje industrial gubernamental sistemático son realidades desafortunadas de la vida.

Además, cuando se logra uno de estos accesos no autorizados, por lo general la información fluye por Internet en muy poco tiempo. Hay grupos de noticias y canales de difusión, en Internet (IRC) en los que los usuarios comparten la información que lograron extraer de estas intromisiones.

Identificación de quien esta autorizado para usar los recursos de la red

Debe hacerse una lista de los usuarios que necesitan acceso a los recursos de la red. No es necesario enlistar a cada usuario. La mayoría de estos pueden dividirse en grupos como usuarios de contabilidad, abogados corporativos, ingenieros, etcétera. También debe tomar en cuenta una clase llamada usuarios externos esta se compone de los usuarios que tengan acceso a su red desde otras partes, como estaciones de trabajo autónomas y otras redes; pueden no ser empleados, o bien, pueden ser empleados que tengan acceso a la red desde sus hogares o durante un viaje.

Identificación del uso adecuado de los recursos

Una vez determinados los usuarios autorizados a tener acceso a los recursos de la red, usted debe establecer los lineamientos del uso aceptable de dichos recursos. Los lineamientos dependen de la clase de usuarios, como desarrolladores de software, estudiantes, profesores, usuarios externos, etcétera. Debe tener lineamientos aparte para cada clase. La política debe establecer que tipo de uso es aceptable y cual es inaceptable, así como que tipo de uso esta restringido. La política que usted elabore será la Política de Uso Aceptable (AUP) de esa red. Si el acceso a un recurso de la red esta restringido, debe considerar el nivel de acceso que tendrá cada clase de usuario.

Su AUP debe establecer con claridad que cada usuario es responsable de sus acciones. La responsabilidad de cada usuario existe al margen de los mecanismos de seguridad implantados. No tiene caso construir costosos mecanismos de seguridad con firewalls si un usuario puede revelar la información copiando archivos en disco o cinta y poner los datos a disposición de individuos no autorizados.

Aunque parezca obvio, la AUP debe establecer claramente que no esta permitido irrumpir en las cuentas o pasar por alto la seguridad. Esto puede ayudar a evitar cuestiones legales planteadas por empleados que pasan por alto la seguridad de la red y después aseguran que no se les informa o capacita adecuadamente acerca de la política de la red. A continuación se muestran los lineamientos que deben escribirse al desarrollar la AUP:

¿Se permite introducirse en las cuentas?
¿Se permite descifrar las contraseñas?
¿Se permite interrumpir servicios?

¿Los usuarios deben suponer que, si un archivo tiene permiso general de lectura, eso los autoriza a leerlo?

¿Debe permitirse que los usuarios modifiquen archivos que no sean suyos, aun cuando dichos usuarios tengan permiso de escritura?

¿Los usuarios deben compartir cuentas?

Determinación de las responsabilidades del usuario

La política de seguridad de la red debe definir los derechos y las responsabilidades de los usuarios que utilizan los recursos y servicios de la red. La siguiente es una lista de los aspectos que usted puede abordar respecto de las responsabilidades de los usuarios:

1. Lineamientos acerca del uso de los recursos de red, tales como que los usuarios estén restringidos

2. Que constituye un abuso en términos de usar recursos de red y afectar el desempeño del sistema y de la red.

3. Esta permitido que los usuarios compartan cuentas o permitan a otros usar la suya.

4. Pueden los usuarios revelar su contraseña en forma temporal, para permitir que otros que trabajen en un proyecto tengan acceso a sus cuentas.

5. Política de contraseña de usuario: con que frecuencia deben cambiar de contraseña los usuarios y que otras restricciones o requerimientos hayal respecto.

6. Los usuarios son responsables de hacer respaldos de sus datos o es esto responsabilidad del administrador del sistema.

7. Consecuencias para los usuarios que divulguen información que pueda estar patentada. Que acciones legales u otros castigos pueden implantarse.

8. Una declaración sobre la privacidad del correo electrónico (Ley de Privacidad en las Comunicaciones Electrónicas)

9. Una política respecto a correo o publicaciones controversiales en las listas de correo o grupos de discusión.

10. Una política sobre comunicaciones electrónicas, tales como falsificación de correo.

La Asociación de Correo Electrónico (EMA, Electrónica Mail Asociación) recomienda que todo sitio debe tener una política acerca de la protección de la privacidad de los empleados.

VI.6 Seguridad en un centro de cómputo

Fuente: (http://www.itver.edu.mx/comunidad/material/serv-computo/ascc/links.html). Casiano Quevedo Julio C, García Vázquez Israel.

Seguridad

Seguridad es el conjunto de metodologías, documentos, programas y dispositivos físicos encaminados a lograr que los recursos de cómputo disponibles en un ambiente dado, sean accedidos única y exclusivamente por quienes tienen la autorización para hacerlo.

La seguridad informática debe vigilar principalmente las siguientes propiedades:

Privacidad.- La información debe ser vista y manipulada únicamente por quienes tienen el derecho o la autoridad de hacerlo. Un ejemplo de ataque a la privacidad es la divulgación de información confidencial.
Integridad.- La información debe ser consistente, fiable y no propensa a alteraciones no deseadas. Un ejemplo de ataque a la integridad es la modificación no autorizada de saldos en un sistema bancario o de calificaciones en un sistema escolar.
Disponibilidad.- La información debe estar en el momento que el usuario requiera de ella.

División de las áreas de administración de la seguridad

Para simplificar, es posible dividir las tareas de administración de seguridad en tres grandes rublos. Estos son:

Autenticación: se refiere a establecer las entidades que puedan tener acceso al universo de recursos de computo que cierto ambiente puede ofrecer.
Autorización: es el hecho de que las entidades autorizadas a tener acceso a los recursos de cómputo, tengan efectivamente acceso únicamente a las áreas de trabajo sobre las cuales ellas deben tener dominio.
Auditoría: se refiere a la continua vigilancia de los servicios en producción. Entra dentro de este rubio el mantener estadísticas de acceso, estadísticas de uso y políticas de acceso físico a los recursos.

Seguridad total en computación

Se requiere un enfoque amplio que abarque cierto número de aspectos relacionados entre sí de manera metódica. Hay dos grandes áreas que se deben incorporar a tal enfoque:

Aspectos administrativos
Aspectos técnicos

Aspectos administrativos

- Políticas de seguridad en un centro de cómputo
- Seguridad física y contra incendios
- Organización y división de las responsabilidades
- Seguros.

Políticas de seguridad en un centro de cómputo

Es necesario que la institución defina políticas de seguridad, en las cuales se deben tener en cuenta que:
La Seguridad debe ser considerada desde la fase de diseño de un Sistema, como parte integral del mismo.

Las políticas de seguridad deben ser definidas por los funcionarios de alto nivel, los cuales deben ser motivados de manera que tengan un rol importante.

Los encargados de soporte, aquellos que son responsables de gestionar la seguridad informática en la organización, han de considerar las siguientes medidas:

- *Distribuir las reglas de seguridad*. Escribir en una lista las reglas básicas de seguridad que los usuarios han de seguir, para mantener la seguridad y ponerlas en un lugar público destacado.
- *Hacer circular regularmente avisos sobre la seguridad*. Utilice ejemplos de daños y problemas procedentes de periódicos, revistas, para ilustrar la necesidad de la vigilancia por mantener la seguridad.
- *Establecer incentivos para la seguridad*. Establezca premios para las ideas que supongan trucos de seguridad y que apoyen las medidas de seguridad oficiales. Haga que los responsables ofrezcan recompensas sustanciosas a los ganadores.
- *Establezca una línea de comunicación sobre seguridad*. El personal debe conocer dónde puede obtener consejos sobre los temas de seguridad.

Seguridad física y contra incendios de los equipos

La seguridad física y contra incendios es un aspecto de suma importancia es de suma importancia en un centro de computo.

Las siguientes recomendaciones, prolongarán la vida de los equipos:

- Ubique el equipo en un área donde no exista mucho movimiento de personal.
- No traslade la computadora sin la autorización y asesoría del Centro de Cómputo.
- Instale la computadora sobre escritorios o muebles estables o especialmente diseñados para ello.
- Ubique el equipo lejos de la luz del sol y de ventanas abiertas.
- La energía eléctrica debe ser regulada a 110 voltios y con polo a tierra. Asesórese debidamente para garantizar una buena toma eléctrica
- No conecte otros aparatos (Radios, maquinas de escribir, calculadoras, etc.) en la misma toma de la computadora. .
- Cada usuario, al momento de terminar las labores diarias, deberá apagar los equipos (Computadora, Impresoras, Escanners).
- Evite colocar encima o cerca de la computadora ganchos, clips, bebidas y comidas que se pueden caer accidentalmente dentro del equipo.
- No fume cerca del equipo, el alquitrán se adhiere a las piezas y circuitos internos del equipo.
- Mantenga libre de polvo las partes externas de la computadora y de las impresoras. Utilice un paño suave y seco. Jamás use agua y jabón.
- Mantenga la pantalla y el teclado cubiertos con fundas cuando no haga uso de ellos por un tiempo considerable o si planea el aseo o reparaciones de las áreas aledañas a la computadora.
- Utilice en la impresora el ancho del papel adecuado. El contacto directo de la cabeza de impresión sobre el rodillo puede estropear ambas partes. (Usuarios con impresoras de matriz de punto)
- Esta prohibido destapar y tratar de arreglar los equipos por su cuenta. En todos los casos asesórese del Centro de Cómputo o del encargado de esta operación.

- No preste los equipos o asegúrese que la persona que lo utilizara conoce su correcta operación

Organización y división de las responsabilidades

La división de responsabilidades permite lograr la revisión y los balances sobre la calidad del trabajo.

Cada persona que labora en la institución debe de tener diferentes actividades dentro de ella, de manera que se puedan organizan para que puedan dividirse las responsabilidades.

Por ejemplo, el personal que prepara los datos y los programadores no deben tener acceso a las actividades de operación.

Es por eso que un centro de cómputo debe de contar con funciones clave, a continuación mencionaremos las más comunes que existen en él:

- Programación
- Preparación de datos
- Redes y comunicaciones
- Control
- Preservación de archivos, etc.

El grado de división entre las diferentes funciones depende del nivel de seguridad que la instalación necesite.

En un centro de cómputo también es de suma importancia que se lleve un control interno de las operaciones que se efectúan. .

Todas estas operaciones efectuadas en el centro de computo son verificadas por auditores tanto internos como externos, los cuales deben de revisar las división de responsabilidades y los procedimientos para verificar que todo este correcto.

Planes y simulacros para la recuperación en casos de desastre

Tipos de desastres

- Destrucción total o parcial de los recursos de procesamiento de datos.
- Destrucción o mal funcionamiento de los recursos ambientales destinados al procesamiento de datos.
- Destrucción total o parcial de los recursos no destinados al procesamiento de datos Destrucción total o parcial de los procedimientos manuales del usuario.
- Pérdida del personal clave
- Huelgas.

Alcance de la planeación contra los desastres

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

Documentación de los sistemas, programación y operaciones.
Recursos de procesamiento que incluyen:
Todo tipo de equipo.
Ambiente para el equipo.

Datos y archivos.
Programas.
Papelería.

Simulación de los desastres

Es necesario llevar a cabo simulaciones de desastres ya que, aunque existen compañías que tienen planes de prevención contra desastres, estos no son puestos en marcha hasta el momento en que ocurre el desastre. Algunas de las siguientes razones son importantes por las cuales realizar un simulacro:

Se prueba la preparación del personal para enfrentar el desastre.
Se identifican las omisiones en los planes contra desastres
El factor sorpresa del simulacro es una buena forma de verificar que existan buenas prácticas de seguridad.

Los simulacros de desastres necesitan de la experiencia y se deben realizar en momentos convenientes. Posteriormente cuando existe mayor experiencia en simulacros dentro del centro de cómputo, estos se deben realizar en un momento no conveniente con el fin de probar la eficiencia de los procedimientos de recuperación.

Cuando se lleva a cabo un simulacro lo que debe pasar es:

El trabajo cesará en forma temporal, para tomar nota del avance del procedimiento
Se completa un inventario de cualquier información que fue destruida por el desastre.

VI.7 Seguridad en contra de virus

Fuente: (http://www.monografias.com/trabajos5/audi/audi.shtml#redes)
Horacio Quinn Eduardo.

Auditoría de la Seguridad Informática:

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.

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 conectamos 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.

La seguridad en la informática abarca los conceptos de seguridad física y seguridad lógica. La seguridad física se refiere a la protección del Hardware y de los soportes de datos, así como a la de los edificios e instalaciones que los albergan. Contempla las situaciones de incendios, sabotajes, robos, catástrofes naturales, etc.

La seguridad lógica se refiere a la seguridad de uso del software, a la protección de los datos, procesos y programas, así como la del ordenado y autorizado acceso de los usuarios a la información.

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.

VI.8 Etapas para implementar un sistema de seguridad

Fuente: (http://www.ilustrados.com/publicaciones/EpyppFyEAyLgAPFJNN.php) Jiménez José Alfredo.

Para dotar de medios necesarios para elaborar su sistema de seguridad se debe considerar los siguientes puntos:

- Sensibilizar a los ejecutivos de la organización en torno al tema de seguridad.
- Se debe realizar un diagnóstico de la situación de riesgo y seguridad de la información en la organización a nivel software, hardware, recursos humanos, y ambientales.
- Elaborar un plan para un programa de seguridad. El plan debe elaborarse contemplando:

Plan de seguridad ideal (o normativo)

Un plan de seguridad para un sistema de seguridad integral debe contemplar:

El plan de seguridad debe asegurar la integridad y exactitud de los datos
Debe permitir identificar la información que es confidencial
Debe contemplar áreas de uso exclusivo
Debe proteger y conservar los activos de desastres provocados por la mano del hombre y los actos abiertamente hostiles
Debe asegurar la capacidad de la organización para sobrevivir accidentes
Debe proteger a los empleados contra tentaciones o sospechas innecesarias
Debe contemplar la administración contra acusaciones por imprudencia

Etapas para implantar un sistema de seguridad en marcha

Para hacer que el plan entre en vigor y los elementos empiecen a funcionar y se observen y acepten las nuevas instituciones, leyes y costumbres del nuevo sistema de seguridad se deben seguir los siguiente 8 pasos:

0. Introducir el tema de seguridad en la visión de la empresa.
0. Definir los procesos de flujo de información y sus riesgos en cuanto a todos los recursos participantes.
0. Capacitar a los gerentes y directivos, contemplando el enfoque global.
0. Designar y capacitar supervisores de área.
0. Definir y trabajar sobre todo las áreas donde se pueden lograr mejoras relativamente rápidas.
0. Mejorar las comunicaciones internas.
0. Identificar claramente las áreas de mayor riesgo corporativo y trabajar con ellas planteando soluciones de alto nivel.
0. Capacitar a todos los trabajadores en los elementos básicos de seguridad y riesgo para el manejo del software, hardware y con respecto a la seguridad física.

Beneficios de un sistema de seguridad

Los beneficios de un sistema de seguridad bien elaborados son inmediatos, ya que él la organización trabajará sobre una plataforma confiable, que se refleja en los siguientes puntos:

- Aumento de la productividad.
- Aumento de la motivación del personal.
- Compromiso con la misión de la compañía.
- Mejora de las relaciones laborales.
- Ayuda a formar equipos competentes.
- Mejora de los climas laborales para los RR.HH.

VI.9 Seguro sobre equipo electrónico

SECCION 1. DAÑOS MATERIALES AL EQUIPO ELECTRONICO

CLAUSULA 1a. COBERTURA BASICA. RIESGOS CUBIERTOS.

Los bienes que se amparan en esta cobertura y se mencionan en la especificación que se agrega y forma parte de la presente Sección, quedan amparados contra daños o pérdidas materiales que sufran en forma súbita e imprevista, que hagan necesaria su reparación o reemplazo a fin de dejarlos en condiciones similares a las existentes inmediatamente antes de ocurrir el siniestro, a consecuencia de los riesgos que en seguida se citan y únicamente dentro del predio consignado en la carátula de la póliza, una vez terminadas las pruebas de operación iniciales, ya sea que estén en operación, revisión, mantenimiento o inactivos:

Incendio, impacto directo de rayo, implosión, explosión, extinción de incendios.
Humo, hollín, gases, líquidos o polvos corrosivos, acción del agua o humedad que no provengan de las condiciones atmosféricas comunes en la región.
Corto-circuito, arco voltaico, perturbaciones por campos magnéticos, sobretensiones causadas por rayo, tostadura de aislamientos.
Defectos de fabricación, de material, de diseño o de instalación.
Errores de manejo, descuido, negligencia, impericia o mala intención del personal del Asegurado.
Actos mal intencionados y dolo de terceros.
Pérdida o daños materiales causados por robo con violencia, tentativa de tal robo y/o asalto. Se entenderá por robo con violencia, el perpetrado por cualquier persona o

personas que haciendo uso de violencia, del exterior al interior del local en que se encuentren los bienes asegurados, deje señales visibles de la violencia en el lugar por donde se penetró. Se entenderá por asalto aquel perpetrado mediante el uso de fuerza o violencia (sea moral o física) sobre las personas.

Hundimiento del terreno, deslizamiento de tierra, caída de rocas, aludes que no sean causados por terremoto o erupción volcánica, granizo y helada.

Cuerpos extraños que se introduzcan en los bienes asegurados.

Otros Daños no excluidos en esta póliza.

CLAUSULA 2a. RIESGOS, GASTOS Y BIENES EXCLUIDOS QUE PUEDEN CUBRIRSE MEDIANTE CONVENIO EXPRESO.

Por convenio expreso entre el Asegurado y la Compañía, esta póliza puede extenderse a cubrir:

Terremoto y/o erupción volcánica.

Granizo, ciclón, huracán o vientos tempestuosos.

Inundación.

Huelgas, alborotos populares, conmoción civil, vandalismo y daños por actos de personas mal intencionadas.

Robo sin violencia.

Gastos adicionales por concepto de flete express no aéreo, trabajos en días festivos y horas extras; siempre que tales gastos sean erogados con motivo de la reparación de un daño cubierto.

Gastos por flete aéreo erogados con motivo de la reparación de un daño cubierto.

Daños que sobrevengan en el equipo electrónico asegurado a consecuencia de daño material en el equipo de climatización.

Equipos móviles y portátiles dentro o fuera de los predios señalados en la carátula de la póliza.

Gastos por albañilería, andamios y escaleras.

CLAUSULA 3a. EXCLUSIONES.

La Compañía no será responsable por pérdidas o daños que sobrevengan por las siguientes causas:

a) Fallas o defectos de los bienes asegurados, existentes al inicio de vigencia de este seguro.
b) Pérdidas o daños que sean consecuencia directa del funcionamiento prolongado o deterioro gradual debido a condiciones atmosféricas o ambientales imperantes en el predio, tales como: desgaste, erosión, corrosión, incrustación, agrietamiento, cavitación.
c) Cualquier gasto efectuado con objeto de corregir deficiencias de capacidad u operación del equipo asegurado.
d) Cualquier gasto erogado con respecto al mantenimiento que efectúen terceros, mediante un contrato. Entendiéndose como mantenimiento aquel que obligue a un tercero a revisar periódicamente y reemplazar partes desgastadas o defectuosas.
e) Pérdidas o daños de los que sean legal o contractualmente responsables el fabricante o el proveedor de los bienes asegurados.

f) Pérdidas o daños a equipos tomados en arrendamiento o alquiler, cuando la responsabilidad recaiga en el arrendador ya sea legalmente o según convenio de arrendamiento y/o mantenimiento.
g) Daños y responsabilidad por reducción de ingresos y/o cualquier otra pérdida consecuencial.
) Pérdidas o daños que sufran por uso de las partes desgastables, tales como bulbos, válvulas, tubos, bandas, fusibles, sellos, cintas, muelles, resortes, cadenas, herramientas recambiables, rodillos grabados, objetos de vidrio, porcelana o cerámica; sin embargo, sí quedan cubiertos, cuando los daños sufridos sean a consecuencia de un riesgo cubierto.
) Pérdidas o daños que sufra cualquier elemento o medio de operación, tales como: lubricantes, combustibles, agentes químicos, a excepción del mercurio utilizado en rectificadores de corriente y los aisladores de cerámica que sí quedan cubiertos en la presente póliza, a menos que los daños sufridos sean consecuencia de un riesgo cubierto.
) Defectos estéticos, tales como raspaduras de superficies pintadas, pulidas o barnizadas. Sin embargo, la Compañía conviene en cubrir las pérdidas o daños mencionados en este inciso cuando dichas partes hayan sido afectadas por una pérdida o daño indemnizable ocurridos a los bienes asegurados.
) Pérdidas o daños ocurridos a equipos que operen bajo tierra, en el agua, en el aire, naves aéreas o espaciales.

QUE HACER EN CASO DE SINIESTRO

RECOMENDACIONES GENERALES

0. Se deberá reportar el siniestro de inmediato ya sea a su Agente o bien directamente a la Compañía con el objeto de que se certifiquen los daños o pérdidas. A este efecto la Compañía designará un Ajustador Profesional al que se le deberán brindar las facilidades necesarias para que pueda cumplir con el objetivo. Al momento de dar el aviso, es necesario que proporcione el número de la póliza, el nombre del Asegurado, la ubicación del siniestro y que se describan los hechos acontecidos.
0. Es importante que se tomen las medidas necesarias para evitar que el daño sufrido se agrave.
0. En caso necesario, dar parte a las Autoridades competentes y solicitar copias certificadas de las actas que se levanten.
0. Cualquier reparación deberá ser previamente autorizada por la Compañía.
0. La documentación que se describe más adelante es la que usualmente se requiere considerando una reclamación que no reviste características especiales; en los casos en que si las tenga, posiblemente el Ajustador le solicitará documentación adicional. En cualquier caso tanto su Agente como el Ajustador le orientarán sobre documentación específica la cuál deberá ser entregada lo más rápidamente posible para estar en condiciones de brindarle un servicio oportuno.
0. Las copias de Actas, Oficios y Partes deberán ser en todos los casos copias certificadas.
0. Tenga presente que cualquier acción o documentación que le sea solicitada tiene por objeto indemnizar sus pérdidas de una manera justa y con la oportunidad debida.

DOCUMENTACION NECESARIA

Es conveniente tener a la mano su póliza de seguro y su último recibo de pago para que el Ajustador pueda conocer los alcances de la misma y acelerar los trámites, especialmente cuando los hechos ocurran en días no hábiles.

Carta de formal reclamación del Asegurado a la Compañía, detallando el monto de la pérdida y las causas que la originaron.

Acta denuncia de los hechos antes de las Autoridades competentes.

Copia del poder notarial del Asegurado o de sus representantes legales tratándose de personas morales.

Inventario de pérdidas que deberá contener descripción, cantidad y valor de los objetos que se reclaman.

Contratos de mantenimiento y/o servicio de los equipos afectados.

Copias de los documentos que sirven de base para fundamentar la reclamación, tales como copias de balances, facturas, avalúos, etc.

En su caso, copia de la reclamación a los causantes del siniestro.

VI.10 Seguridad en la utilización del equipo

Fuente: (http://www.monografias.com/trabajos/maudisistlmaudisist.shtml) Toro Oscar.

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:

Se debe restringir el acceso a los programas y a los archivos.

Los operadores deben trabajar con poca supervisión y sin la participación de los programadores, y no deben modificar los programas ni los archivos.

Se debe asegurar en todo momento que los datos y archivos usados sean los adecuados, procurando no usar respaldos inadecuados.

No debe permitirse la entrada a la red a personas no autorizadas, ni a usar las terminales.

Se deben realizar periódicamente una verificación física del uso de terminales y de los reportes obtenidos.

Se deben monitorear periódicamente el uso que se le está dando a las terminales.

Se deben hacer auditorías periódicas sobre el área de operación y la utilización de las terminales.

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. .

Deben existir registros que reflejen la transformación entre las diferentes funciones de un sistema.

Debe controlarse la distribución de las salidas (reportes, cintas, ate.).

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.

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 qué 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.
0. Sólo el personal autorizado debe tener acceso a la información confidencial.
0. Controlar los listados tanto de los procesos correctos como aquellos procesos con terminación Incorrecta.
0. Controlar el número de coplas 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.

VI.11 Seguridad al restaurar el equipo

Fuente: (http://www.itapizaco.edu.mx/paginas/maudisist.html) Toro Oscar.

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 más 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.

¿Existen procedimientos relativos a la restauración y repetición de procesos en el sistema de cómputo?
SI ( ) NO ( )

¿Enuncie los procedimientos mencionados en el inciso anterior?

¿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:

0) 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.

0) Los nuevos sistemas deben estar adecuadamente documentos y probados.

0) 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.

VI.12 Plan de contingencias

Fuente: (http://www.inei.gob.pe/web/metodologias/attach/lib611/0300.htm) INEI.

Esquema general

El Plan de Contingencias implica un análisis de los posibles riesgos a los cuales pueden estar expuestos nuestros equipos de cómputo y la información contenida en los diversos medios de almacenamiento, por lo que en este Manual haremos un análisis de los riesgos, cómo reducir su posibilidad de ocurrencia y los procedimientos a seguir en caso que se presentara el problema.

Pese a todas nuestras medidas de seguridad puede ocurrir un desastre, por tanto es necesario que el Plan de Contingencias incluya un Plan de Recuperación de Desastres, el cual tendrá como objetivo, restaurar el Servicio de Cómputo en forma rápida, eficiente y con el menor costo y pérdidas posibles.

Si bien es cierto que se pueden presentar diferentes niveles de daños, también se hace necesario presuponer que el daño ha sido total, con la finalidad de tener un Plan de Contingencias lo más completo posible. .

Vamos a trabajar en base a un ejemplo que presupone un incendio en nuestro local, el cual nos ha dejado sin equipos de cómputo y sin los archivos magnéticos (programas y datos) contenidos en dichos equipos y en las oficinas del local.

Hay dos ámbitos que vamos a analizar. El primero abarca las actividades que se deben realizar y los grupos de trabajo o responsables de operarias. El segundo, el control, esto es, las pruebas y verificaciones periódicas de que el Plan de Contingencias está operativo y actualizado.

Haciendo un esquema, el Plan de Contingencias abarcará los siguientes aspectos:

- Plan de Reducción de Riesgos (Plan de Seguridad).
- Plan de Recuperación de Desastres.
  Actividades Previas al Desastre.
  Establecimiento del Plan de Acción.
  Formación de Equipos Operativos.
  Formación de Equipos de Evaluación (auditoría de cumplimiento de procedimientos de Seguridad).
  - Actividades durante el Desastre.
  - Plan de Emergencias.
  - Formación de Equipos.
  - Entrenamiento.
  - Actividades después del Desastre.

  Evaluación de Daños.
  Priorización de Actividades del Plan de Acción señaladas en 2.1.1
  Ejecución de Actividades
  Evaluación de Resultados.
  Retroalimentación del Plan de Acción.

Plan de riesgos (plan de seguridad)

Para asegurar que se consideran todas las posibles eventualidades, se ha de elaborar una lista de todos los riesgos conocidos, para lo cual se deberá realizar un análisis de riesgos.

Análisis de riesgos

El análisis de riesgos supone más que el hecho de calcular la posibilidad de que ocurran cosas negativas. Se ha de poder obtener una evaluación económica del impacto de estos sucesos negativos. Este valor se podrá utilizar para contrastar el costo de la protección de la Información en análisis, versus el costo de volverla a producir (reproducir).

La evaluación de riesgos y presentación de respuestas debe prepararse de forma personalizada para cada organización.

La evaluación de riesgos supone imaginarse lo que puede ir mal y a continuación estimar el coste que supondría. Se ha de tener en cuenta la probabilidad de que sucedan cada uno de los problemas posibles. De esta forma se pueden priorizar los problemas y su coste potencial desarrollando un plan de acción adecuado.

El análisis de riesgos supone responder a preguntas del tipo:

¿Qué puede ir mal?
¿Con qué frecuencia puede ocurrir?
¿Cuáles serían sus consecuencias?
¿Qué fiabilidad tienen las respuestas a las tres primeras preguntas?

En lo fundamental la evaluación de riesgos que se ha de llevar a cabo ha de contestar, con la mayor fiabilidad posible, a las siguientes preguntas:

¿Qué se intenta proteger?
¿Cuál es su valor para uno o para la organización?
¿Frente a qué se intenta proteger?

¿Cuál es la probabilidad de un ataque?

A continuación se muestra un ejemplo de cómo se realiza una evaluación de riesgos.

El o los responsables de la oficina de informática se sentarán con los responsables de las áreas usuarias y realizarán el siguiente conjunto de puntualizaciones:

¿A qué riesgos en la seguridad informática se enfrenta la Institución?

Al fuego, que puede destruir los equipos y archivos.
Al robo común, llevándose los equipos y archivos.
Al vandalismo, que dañen los equipos y archivos.
A fallas en los equipos, que dañen los archivos.
A equivocaciones, que dañen los archivos.
A la acción de virus, que dañen los equipos y archivos.
A terremotos, que destruyen el equipo y los archivos.
A accesos no autorizados, filtrándose datos no autorizados.

Al robo de datos, difundiéndose los datos sin cobrarlos.
Al fraude, desviando fondos merced a la computadora.

Esta lista de riesgos que se puede enfrentar en la seguridad, es bastante corta. La institución deberá profundizar en el tema para poder tomar todas las medidas del caso.

Luego de elaborar esta lista, el personal de la Institución estará listo para responder a los efectos que estos riesgos tendrán para su Institución.

¿Qué probabilidad hay de que tenga efecto alguno de los riesgos mencionados?

Al fuego, que puede destruir los equipos y los archivos

¿La Institución cuenta con protección contra incendios?
¿Se cuenta con sistemas de aspersión automática?
¿Diversos extintores?
¿Detectores de humo?
¿Los empleados están preparados para enfrentar un posible incendio?

A un robo común, llevándose los equipos y archivos

¿En que tipo de vecindario se encuentra la Institución?
¿Hay venta de drogas?
¿Las computadoras se ven desde la calle?
¿Hay personal de seguridad en la Institución?
¿Cuántos vigilantes hay?
¿Los vigilantes, están ubicados en zonas estratégicas?

Al vandalismo, que dañen los equipos y archivos

¿Existe la posibilidad que un ladrón desilusionado o frustrado cause daños?
¿Hay la probabilidad de que causen algún otro tipo de daño intencionado?

A fallas en los equipos, que dañen los archivos

¿Los equipos tienen un mantenimiento continuo por parte de personal calificado?
¿Cuáles son las condiciones actuales del hardware?
¿Es posible predecir las fallas a que están expuestos los equipos?

A equivocaciones que dañen los archivos

¿Cuánto saben los empleados de computadoras o redes?

Los que no conocen del manejo de la computadora, ¿saben a quién pedir ayuda?

Durante el tiempo de vacaciones de los empleados, ¿qué tipo de personal los sustituye y qué tanto saben del manejo de computadoras?

A la acción de virus, que dañen los archivos

¿Se prueba software en la oficina sin hacerle un examen previo?

¿Está permitido el uso de disquetes en la oficina?
¿Todas las máquinas tienen unidades de disquetes?
¿Se cuentan con procedimientos contra los virus?

A terremotos, que destruyen los equipos y archivos

¿La Institución se encuentra en una zona sísmica?
¿El edificio cumple con las normas antisísmicas?
Un terremoto, ¿cuánto daño podría causar?

A accesos no autorizados, filtrándose datos importantes

¿Cuánta competencia hay para la Institución?
¿Qué probabilidad hay que un competidor intente hacer un acceso no autorizado?
¿El modem se usa para llamar fuera y también se puede utilizar para comunicarse hacia dentro?
¿Contamos con Sistemas de Seguridad en el Correo Electrónico o Internet?

Al robo de datos; difundiéndose los datos.

¿Cuánto valor tienen actualmente las Bases de Datos?
¿Cuánta pérdida podría causar en caso de que se hicieran públicas?
¿Se ha elaborado una lista de los posibles sospechosos que pudieran efectuar el robo?
La lista de sospechosos, ¿es amplia o corta?

Al fraude, desviando fondos merced a la computadora.

¿Cuántas personas se ocupan de la contabilidad de la Institución?
¿El sistema de contabilidad es confiable?

Las personas que trabajan en el departamento de contabilidad, ¿qué tipo de antecedentes laborales tienen?

¿Existe acceso al Sistema Contable desde otros Sistemas o Personas?

Para cada riesgo, se debe determinar la probabilidad del factor de riesgo. Como ejemplo se mencionan algunos factores de riesgo:

Factor de riesgo bajo
Factor de riesgo muy bajo
Factor de riesgo alto
Factor de riesgo muy alto
Factor de riesgo medio

Luego se efectuará un resumen de los riesgos ordenados por el factor de riesgo de cada uno.

Ejemplo:

TIPO DE RIESGO	FACTOR DE RIESGO
Robo	Alto

Vandalismo	Medio
Fallas en los equipos	Medio
Acción de virus	Medio
Equivocaciones	Bajo
Terremotos	Bajo
Accesos no autorizados	Bajo
Robo de datos	Bajo
Fuego	Bajo
Fraude	Muy bajo

Análisis de fallas en la seguridad

Esto supone estudiar las computadoras, su software, localización y utilización con el objeto de identificar los resquicios en la seguridad que pudieran suponer un peligro. Por ejemplo, si se instala una computadora personal nueva, para recibir informes de inventario desde otras PC's vía modem situados en lugares remotos, y debido a que el modem se ha de configurar para que pueda recibir datos, se ha abierto una vía de acceso al sistema informático. Habrá que tomar medidas de seguridad para protegerlo, como puede ser la validación de la clave de acceso.

Protecciones actuales

Generales, se hace una copia casi diaria de los archivos que son vitales para la Institución.
Robo común, se cierran las puertas de entrada y ventanas.
Vandalismo, se cierra la puerta de entrada.

Falla de los equipos, se tratan con cuidado, se realiza el mantenimiento de forma regular, no se permite fumar, está previsto el préstamo de otros equipos.

Daño por virus, todo el software que llega se analiza en un sistema utilizando software antivirus. Los programas de dominio público y de uso compartido (Shareware), sólo se usan si proceden de una fuente fiable.

Equivocaciones, los empleados tienen buena formación. Cuando son necesarios, se intenta conseguir buenos trabajadores temporales.

Terremoto, nada. Aparte de la protección contra incendios, la cual es buena.

Acceso no autorizado, se cierra la puerta de entrada. Varias computadoras disponen de llave de bloqueo del teclado.

Robo de datos, se cierra la puerta principal. Varias computadoras disponen de llave de bloqueo del teclado

Fuego, en la actualidad se encuentra instalado Sistemas contra incendios, extinguidores, en sitios estratégicos y se brinda entrenamiento en el manejo de los sistemas o extinguidores al personal, en forma periódica.

En los Capítulos siguientes se brinda información completa y detallada de la Seguridad de Equipos y de la Información.

VI.13 Plan de recuperación de desastres

Es importante definir los procedimientos y planes de acción para el caso de una posible falla, siniestro o desastre en el área Informática, considerando como tal todas las áreas de los usuarios que procesan información por medio de la computadora.

Cuando ocurra una contingencia, es esencial que se conozca al detalle el motivo que la originó y el daño producido, lo que permitirá recuperar en el menor tiempo posible el proceso perdido.

La elaboración de los procedimientos que se determinen como adecuados para un caso de emergencia, deben ser planeados y probados fehacientemente.

Los procedimientos deberán ser de ejecución obligatoria y bajo la responsabilidad de los encargados de la realización de los mismos, debiendo haber procesos de verificación de su cumplimiento. En estos procedimientos estará involucrado todo el personal de la Institución.

Los procedimientos de planes de recuperación de desastres deben de emanar de la máxima autoridad Institucional, para garantizar su difusión y estricto cumplimiento.

Las actividades a realizar en un Plan de Recuperación de Desastres se pueden clasificar en tres etapas:

Actividades Previas al Desastre.
Actividades Durante el Desastre.
Actividades Después del Desastre.

Actividades previas al desastre

Son todas las actividades de planeamiento, preparación, entrenamiento y ejecución de las actividades de resguardo de la información, que nos aseguren un proceso de Recuperación con el menor costo posible a nuestra Institución.

Podemos detallar las siguientes Actividades Generales:

Establecimiento del Plan de Acción.
Formación de Equipos Operativos.
Formación de Equipos de Evaluación (auditoria de cumplimiento de los procedimientos sobre Seguridad).

Establecimiento de plan de acción

En esta fase de Planeamiento se debe de establecer los procedimientos relativos a:

a) Sistemas e Información.
b) Equipos de Cómputo.
c) Obtención y almacenamiento de los Respaldos de Información (BACKUPS).
d) Políticas (Normas y Procedimientos de Backups).

a) Sistemas e Información. La Institución deberá tener una relación de los Sistemas de Información con los que cuenta, tanto los realizados por el centro de cómputo como los hechos

por las áreas usuarias. Debiendo identificar toda información sistematizada o no, que sea necesaria para la buena marcha Institucional.

La relación de Sistemas de Información deberá detallar los siguientes datos:

Nombre del Sistema.

Lenguaje o Paquete con el que fue creado el Sistema. Programas que lo conforman (tanto programas fuentes como programas objetos, rutinas, macros, etc.).

La Dirección (Gerencia, Departamento, etc.) que genera la información base (el «dueño» del Sistema).

Las unidades o departamentos (internos/externos) que usan la información del Sistema.
El volumen de los archivos que trabaja el Sistema.
El volumen de transacciones diarias, semanales y mensuales que maneja el sistema.
El equipamiento necesario para un manejo óptimo del Sistema.
La(s) fecha(s) en las que la información es necesitada con carácter de urgencia.

El nivel de importancia estratégica que tiene la información de este Sistema para la Institución (medido en horas o días que la Institución puede funcionar adecuadamente, sin disponer de la información del Sistema). Equipamiento mínimo necesario para que el Sistema pueda seguir funcionando (considerar su utilización en tres turnos de trabajo, para que el equipamiento sea el mínimo posible).

Actividades a realizar para volver a contar con el Sistema de Información (actividades de Restore).

Con toda esta información se deberá de realizar una lista priorizada (un ranking) de los Sistemas de Información necesarios para que la Institución pueda recuperar su operatividad perdida en el desastre (contingencia).

b) Equipos de Cómputo. Aparte de las Normas de Seguridad que se verán en los capítulos siguientes, hay que tener en cuenta:

Inventario actualizado de los equipos de manejo de información (computadoras, lectoras de microfichas, impresoras, etc.), especificando su contenido (software que usa, principales archivos que contiene), su ubicación y nivel de uso Institucional.

Pólizas de Seguros Comerciales. Como parte de la protección de los Activos Institucionales, pero haciendo la salvedad en el contrato, que en casos de siniestros, la restitución del Computador siniestrado se podrá hacer por otro de mayor potencia (por actualización tecnológica), siempre y cuando esté dentro de los montos asegurados.

Señalización o etiquetado de los Computadores de acuerdo a la importancia de su contenido, para ser priorizados en caso de evacuación. Por ejemplo etiquetar (colocar un sticker) de color rojo a los Servidores, color amarillo a las PC’s con Información importante o estratégica y color verde a las PC’s de contenidos normales.

Tener siempre actualizada una relación de PC’s requeridas como mínimo para cada Sistema permanente de la Institución (que por sus funciones constituyen el eje central de los

Servicios Informáticos de la Institución), las funciones que realizaría y su posible uso en dos o tres turnos de trabajo, para cubrir las funciones básicas y prioritarias de cada uno de estos Sistemas.

c) Obtención y almacenamiento de los respaldos de información (BACKUPS).

Se deberá establecer los procedimientos para la obtención de copias de Seguridad de todos los elementos de software necesarios para asegurar la correcta ejecución de los Sistemas o aplicativos de la Institución. Para lo cual se debe contar con:

1) Backups del Sistema Operativo (en caso de tener varios Sistemas Operativos o versiones, se contará con una copia de cada uno de ellos).

2) Backups del Software Base (Paquetes y/o Lenguajes de Programación con los cuales han sido desarrollados o interactúan nuestros Aplicativos Institucionales).

3) Backups del Software Aplicativo (Considerando tanto los programas fuentes, como los programas objetos correspondientes, y cualquier otro software o procedimiento que también trabaje con la data, para producir los resultados con los cuales trabaja el usuario final). Se debe considerar también las copias de los listados fuentes de los programas definitivos, para casos de problemas.

4) Backups de los Datos (Bases de Datos, Índices, tablas de validación, passwords, y todo archivo necesario para la correcta ejecución del Software Aplicativo de nuestra Institución).

5) Backups del Hardware. Se puede implementar bajo dos modalidades:

Modalidad Externa. Mediante convenio con otra Institución que tenga equipos similares o mayores y que brinden la seguridad de poder procesar nuestra Información, y ser puestos a nuestra disposición, al ocurrir una contingencia y mientras se busca una solución definitiva al siniestro producido. Este tipo de convenios debe tener tanto las consideraciones de equipamiento como de ambientes y facilidades de trabajo que cada institución se compromete a brindar, y debe de ser actualizado cada vez que se efectúen cambios importantes de sistemas que afecten a cualquiera de las instituciones.

Modalidad Interna. Si tenemos más de un local, en ambos debemos tener señalados los equipos, que por sus características técnicas y capacidades, son susceptibles de ser usados como equipos de emergencia del otro local, debiéndose poner por escrito (igual que en el caso externo), todas las actividades a realizar y los compromisos asumidos.

En ambos casos se deberá probar y asegurar que los procesos de restauración de Información posibiliten el funcionamiento adecuado de los Sistemas. En algunos casos puede ser necesario volver a recompilar nuestro software aplicativo bajo plataformas diferentes a la original, por lo que es imprescindible contar con los programas fuentes, al mismo grado de actualización que los programas objeto.

d) Políticas (Normas y Procedimientos de Backups)

Se debe establecer los procedimientos, normas, y determinación de responsabilidades en la obtención de los Backups mencionados anteriormente en el punto «C», debiéndose incluir:

Periodicidad de cada Tipo de Backup.

Respaldo de Información de movimiento entre los periodos que no se sacan Backups (backups incrementales).

Uso obligatorio de un formulario estándar para el registro y control de los Backups (se incluye un formato tipo en el anexo «IV».)

Correspondencia entre la relación de Sistemas e Informaciones necesarias para la buena marcha de la empresa (mencionado en el punto «a»), y los backups efectuados.

Almacenamiento de los Backups en condiciones ambientales óptimas, dependiendo del medio magnético empleado.

Reemplazo de los Backups, en forma periódica, antes que el medio magnético de soporte se pueda deteriorar (reciclaje o refresco).

Almacenamiento de los Backups en locales diferentes donde reside la información primaria (evitando la pérdida si el desastre alcanzo todo el edificio o local estudiado).

Pruebas periódicas de los Backups (Restore), verificando su funcionalidad, a través de los sistemas, comparando contra resultados anteriores confiables.

Formación de equipos operativos

En cada unidad operativa de la Institución, que almacene información y sirva para la operatividad Institucional, se deberá designar un responsable de la seguridad de la Información de su unidad.

Pudiendo ser el jefe de dicha Área Operativa.

Sus labores serán:

Ponerse en contacto con los propietarios de las aplicaciones y trabajar con ellos.
Proporcionar soporte técnico para las copias de respaldo de las aplicaciones.
Planificar y establecer los requerimientos de los sistemas operativos en cuanto a archivos, bibliotecas, utilitarios, etc., para los principales sistemas y subsistemas.
Supervisar procedimientos de respaldo y restauración.
Supervisar la carga de archivos de datos de las aplicaciones, y la creación de los respaldos incrementales.
Coordinar líneas, terminales, modem, otros aditamentos para comunicaciones.
Establecer procedimientos de seguridad en los sitios de recuperación.
Organizar la prueba de hardware y software.
Ejecutar trabajos de recuperación.
Cargar y probar archivos del sistema operativo y otros sistemas almacenados en el local alternante.
Realizar procedimientos de control de inventario y seguridad del almacenamiento en el local alternante.
Establecer y llevar a cabo procedimientos para restaurar el lugar de recuperación.
Participar en las pruebas y simulacros de desastres.

Formación de equipos de evaluación (auditoría de cumplimiento de los procedimientos sobre seguridad)

Esta función debe ser realizada de preferencia por personal de Inspectoría, de no ser posible, la realizará el personal del área de Informática, debiendo establecerse claramente sus funciones, responsabilidades y objetivos:

Revisar que las Normas y procedimientos con respecto a Backups y seguridad de equipos y data se cumpla.

Supervisar la realización periódica de los backups, por parte de los equipos operativos, comprobando físicamente su realización, adecuado registro y almacenamiento.

Revisar la correlación entre la relación de Sistemas e Informaciones necesarios para la buena marcha de la Institución (detallados en «a»), y los backups realizados.

Informar de los cumplimientos e incumplimientos de las Normas, para las acciones de corrección respectivas.

Actividades durante el desastre

Una vez presentada la Contingencia o Siniestro, se deberá ejecutar las siguientes actividades, planificadas previamente:

- Plan de Emergencias.
- Formación de Equipos.
- Entrenamiento.
- Plan de Emergencias

En este plan se establecen las acciones se deben realizar cuando se presente un Siniestro, así como la difusión de las mismas.

Es conveniente prever los posibles escenarios de ocurrencia del Siniestro:

Durante el día.
Durante la Noche o madrugada.

Este plan deberá incluir la participación y actividades a realizar por todas y cada una de las personas que se pueden encontrar presentes en el área donde ocurre el siniestro, debiendo detallar:

Vías de salida o escape.
Plan de Evacuación del Personal.
Plan de puesta a buen recaudo de los activos (incluyendo los activos de Información) de la Institución (si las circunstancias del siniestro lo posibilitan)
Ubicación y señalización de los elementos contra el siniestro (extinguidores, cobertores contra agua, etc.)
Secuencia de llamadas en caso de siniestro, tener a la mano: elementos de iluminación (linternas), lista de teléfonos de Bomberos I Ambulancia, Jefatura de Seguridad y de su personal (equipos de seguridad) nombrados para estos casos.

Formación de equipos

Establecer claramente cada equipo (nombres, puestos, ubicación, etc.) con funciones claramente definidas a ejecutar durante el siniestro.

Si bien la premisa básica es la protección de la Integridad del personal, en caso de que el siniestro lo permita (por estar en un inicio o estar en una área cercana, etc.), deberá de existir dos equipos de personas que actúen directamente durante el siniestro, un equipo para combatir el siniestro y otro para el salvamento de los recursos Informáticos, de acuerdo a los lineamientos o clasificación de prioridades.

Entrenamiento

Establecer un programa de prácticas periódicas de todo el personal en la lucha contra los diferentes tipos de siniestros, de acuerdo a los roles que se le hayan asignado en los planes de evacuación del personal o equipos, para minimizar costos se puede aprovechar fechas de recarga de extinguidores, charlas de los proveedores, etc.

Un aspecto importante es que el personal tome conciencia de que los siniestros (incendios, inundaciones, terremotos, apagones, etc.) pueden realmente ocurrir, y tomen con seriedad y responsabilidad estos entrenamientos, para estos efectos es conveniente que participen los elementos directivos, dando el ejemplo de la importancia que la alta dirección otorga a la Seguridad Institucional.

Actividad después del desastre

Después de ocurrido el Siniestro o Desastre es necesario realizar las actividades que se detallan, las cuales deben estar especificadas en el Plan de Acción.

- Evaluación de Daños.
- Priorización de Actividades del Plan de Acción.
- Ejecución de Actividades.
- Evaluación de Resultados.
- Retroalimentación del Plan de Acción.

Evaluación de daños.

Inmediatamente después que el siniestro ha concluido, se deberá evaluar la magnitud del daño que se ha producido, que sistemas se están afectando, que equipos han quedado no operativos, cuales se pueden recuperar, y en cuanto tiempo, etc.

Adicionalmente se deberá lanzar un pre-aviso a la Institución con la cual tenemos el convenio de respaldo, para ir avanzando en las labores de preparación de entrega de los equipos por dicha Institución.

Priorización de actividades del plan de acción.

Toda vez que el Plan de acción es general y contempla una pérdida total, la evaluación de daños reales y su comparación contra el Plan, nos dará la lista de las actividades que debemos realizar, siempre priorizándola en vista a las actividades estratégicas y urgentes de nuestra Institución.

Es importante evaluar la dedicación del personal a actividades que puedan no haberse afectado, para ver su asignamiento temporal a las actividades afectadas, en apoyo al personal de los sistemas afectados y soporte técnico.

Ejecución de actividades.

La ejecución de actividades implica la creación de equipos de trabajo para realizar las actividades previamente planificadas en el Plan de acción. Cada uno de estos equipos deberá contar con un coordinador que deberá reportar diariamente el avance de los trabajos de recuperación y, en caso de producirse algún problema, reportarlo de inmediato a la jefatura a cargo del Plan de Contingencias.

Los trabajos de recuperación tendrán dos etapas, la primera la restauración del servicio usando los recursos de la Institución o local de respaldo, y la segunda etapa es volver a contar con los recursos en las cantidades y lugares propios del Sistema de Información, debiendo ser esta última etapa lo suficientemente rápida y eficiente para no perjudicar el buen servicio de nuestro Sistema e imagen Institucional, como para no perjudicar la operatividad de la Institución o local de respaldo.

Evaluación de resultados.

Una vez concluidas las labores de Recuperación del (los) Sistema(s) que fueron afectados por el siniestro, debemos de evaluar objetivamente, todas las actividades realizadas, que tan bien se hicieron, que tiempo tomaron, que circunstancias modificaron (aceleraron o entorpecieron) las actividades del plan de acción, como se comportaron los equipos de trabajo, etc.

De la Evaluación de resultados y del siniestro en si, deberían de salir dos tipos de recomendaciones, una la retroalimentación del plan de Contingencias y otra una lista de recomendaciones para minimizar los riesgos y pérdida que ocasionaron el siniestro.

Retroalimentación del plan de acción.

Con la evaluación de resultados, debemos de optimizar el plan de acción original, mejorando las actividades que tuvieron algún tipo de dificultad y reforzando los elementos que funcionaron adecuadamente.

El otro elemento es evaluar cual hubiera sido el costo de no haber tenido nuestra Institución el plan de contingencias llevado a cabo.

VI.14 Amenazas más comunes contra la seguridad

Desastres Naturales
El fuego

El fuego es un elemento comprendido dentro de las principales amenazas contra la seguridad, este a su vez es un problema critico en un centro de cómputo por varias razones: primero, porque el centro está lleno de material combustible como papel, cajas, etc. El hardware y el cableado del suelo falso pueden ser también fuente de serios incendios. Desgraciadamente los sistemas antifuego dejan mucho que desear, causando casi igual daño que el propio fuego,

sobre todo a los elementos electrónicos. El dióxido de carbono, actual alternativa del agua, resulta peligroso para los propios empleados si quedan atrapados en la sala de cómputo.

El fuego es considerado el principal enemigo del computador ya que puede destruir fácilmente los ficheros de información y programas.

Además de la pérdida de ficheros o del equipo, el fuego puede causar otras pérdidas no cubiertas por el seguro. La más importante es la pérdida del "momento del negocio". Un contratiempo de semanas o meses causa irreparables daños a cualquier organización, aunque lograra situarse en las condiciones originales.

A continuación presentaremos algunos elementos en la lucha contra este tipo de amenaza.

Sistemas automáticos antifuego

a) Sprinklers. Es un sistema "Tipo Ducha». La instalación de este sistema se efectúa en la parte superior del ambiente, como el techo.

Cuando se activa el sprinklers se abren las válvulas y como si fuera una ducha, cae el agua al lugar donde los detectores de humo y/o calor detectan la señal de incendio.

Este sistema es bastante eficaz para combatir un posible incendio, pero no es recomendable en los departamentos con equipos de cómputo, ya que este sistema puede dañar los equipos, además de ser el agua un excelente conductor de la electricidad.

b) Inundación del área con gas. Otro de los métodos muy eficaces para combatir el fuego es la inundación del área con gas antifuego. En una emergencia por fuego, el área se inunda con un determinado gas como:

Dióxido de Carbono,
Halón.

Extinguidores manuales

Cuando no se cuenta con sistemas automáticos antifuego y se vea o perciba señales de fuego, entonces se debe actuar con rapidez para poder sofocar el incendio. Para ello, se debe tener en cuenta el material que está siendo consumido por el fuego. Para cada tipo de situación hay un agente antifuego ideal, así tenemos:

	GAS CARBONICO (CO2)	**ESPUMA**	**AGUA**
PAPEL, MADERA **este tipo de material que deja brasa o ceniza requiere un en la superficie**	apaga solamente en la superficie	sofoca	excelente enfría y empapa apaga totalmente
EQUIPAMIENTO	Excelente No deja residuos,	Conduce la electricidad	Conductora de la electricidad

ELECTRICO	no daña el equipamiento y no es conductor de la electricidad	y además daña el equipo	
LIQUIDOS INFLAMABLES **(Aceites, gasolina, grasa, etc.), requieren** **Acción rápida de sofocar y enfriar**	Bueno; no deja residuos y es inofensivo	Excelente; produce una sábana de espuma que sofoca y enfría	

CO2	1.- Retirar la traba de seguridad 2.- Asegure firmemente el mango difusor 3.- Apretar el gatillo 4.- Oriente el chorro hacia la base del fuego haciendo un barrido **Alcance**: 1 a 2 metros **Sustancia**: Bióxido de carbono **Momento del Recargo**: Pérdida del 10% o mas de peso
POLVO QUIMICO	1.- Abra la ampolla de gas 2.- Asegure firmemente el mango del difusor 3.- Apretar el gatillo 4.- Oriente el chorro de manera de crear una cortina de polvo sobre le fuego **Alcance:** 2 a 4 metros **Sustancia:** Polvo Químico seco y CO2 producido por el contacto del polvo con el fuego **Momento de Recargo:** Pérdida de peso de la ampolla superior al 10%
ESPUMA	1.- Inversión del aparato para abajo 2.- Oriente el chorro para la base del fuego **Alcance:** 9 a 18 metros **Sustancia:** Espuma formada por burbujas consistentes llenas de CO2 **Momento del Recargo:** Anualmente
AGUA-GAS	Simplemente maniobra de apertura de la ampolla de CO2 que sirve de propagador. **Alcance:** 9 a 20 metros **Sustancia:** Agua **Momento del Recargo:** Anualmente

Recomendaciones

El personal designado para usar extinguidores de fuego debe ser entrenado en su uso. Ellos deben recibir algunas lecciones de instrucciones en el mecanismo de lucha contra el fuego y luego, estar enseñados de cómo operar el extinguidor de mano.

Si hay sistemas de detección de fuego que activaron el Sistema de Extinción, todo el personal de esa área debe estar entrenado en la forma cómo usarlos. Es muy importante que todo el personal reciba la instrucción de no interferir con este proceso automático y evitar su actuación en el sistema de extinción, a menos que estén seguros que no hay fuego.

Muchas veces la sensibilidad de comienzo de fuego en los aparatos de detección es muy alta. Esto genera falsas alarmas y el personal de operación se acostumbra a detener el sistema automático de extinción de fuego, sin observar realmente si hay incendio.

Cuidado al seleccionar e implementar detector de fuego y sistema de extinción y su conexión es efectuada con fuerza eléctrica

El detector de fuego y el sistema de extinción deben ser seleccionados e instalados, con la mejor información de la tasación del riesgo, el costo y los posibles orígenes de fuego.

También, considerar cómo estos sistemas de detección y extinción pueden ser integrados a su fuerza eléctrica. Esto ahorraría el costo de la instalación inicial y con algunos sistemas de extinción, daños por agua en el caso de fuego.

Una consideración más contra el incendio estaría dada por el uso de paredes protectoras de fuego alrededor de las áreas que se desea proteger del incendio, que podría originarse en las áreas adyacentes.

Proteja su sistema contra daños de humo

El humo, en particular la clase que es principalmente espeso, negro y de materiales especiales, puede ser muy dañino y requiere una lenta y costosa operación de limpieza.

La mayoría de humos que llegan y dañan el Sistema de Procesamiento de Datos, son originados por fuegos externos al Centro de Procesamiento de Datos. Es frecuente introducirlos en el Centro, a través del sistema de aire acondicionado.

Se debe examinar el potencial del problema y tomar las medidas apropiadas para operar reguladores e impedir la entrada de humo. Colocando adecuadas cubiertas plásticas para todo el equipo, escritorios y cabinas, puede ayudar a reducir el daño ocasionado por el humo y/o agua.

Se consigue sacar el humo del área de sistemas, tan rápido como sea posible, con el uso de diferentes ventiladores. Estos son provechosos luego de que la generación o ingreso del humo ha sido eliminado.

Mantener buenas relaciones con el departamento local de bomberos

Conseguir información con el Departamento local de Bomberos, antes de que ellos sean llamados en una emergencia. Hacer que el Departamento esté consciente de las particularidades y vulnerabilidades del sistema por excesivas cantidades de agua que provienen de arriba y la conveniencia de una salida para el humo, tanto que minimice la cantidad de penetración al área de Procesamiento de Datos.

No es razonable anticipar que el Departamento de Bomberos puede estar completamente enterado de la situación peculiar presentada por su particular instalación. Ellos no podrían proporcionar intereses apropiados para la protección del sistema de Procesamiento de Datos, si no se les ha dado la oportunidad de revisarlo. Además, ellos pueden, usualmente, ofrecer excelentes consejos como precauciones, los cuales deben ser tomados para prevenir incendios.

Mantener procedimientos planeados para recibir y almacenar abastecimientos de papel

La plataforma de recepción, a menudo provee un fácil acceso a todos los servicios de oportunidades para hacer entrega de materiales incendiarios, que puedan destruir los servicios.

Debe proveerse mucho cuidado para limitar el uso de plataformas de recepción como un medio de acceso al edificio. Por consiguiente, el abastecimiento de papel en demasía, de aquel que se necesita para satisfacer los requerimientos inmediatos del Centro de Procesamiento de Datos, debe ser almacenado en un lugar apropiado para proveer detección de fuego y servicios de extinción.

El agua

Otro de los peligros relevantes es el agua. El agua puede entrar en una sala de computadores por varios conductos.

Computadores en sótanos o a nivel de calle son vulnerables a inundaciones, los centros de cómputo también pueden quedar inundados por cañerías reventadas en el suelo, falso techo o paredes.

Aunque realmente el agua es una amenaza para los componentes del computador y cables, no constituye un verdadero peligro para las Cintas magnéticas. Se ha demostrado en pruebas, que cintas sumergidas en agua durante varias horas han podido ser leídas de nuevo (libres de errores), después de secarlas durante dos días. Si el agua, por si sola, no constituye un serio peligro y el calor por debajo de 120 grados no es perjudicial, ambos elementos juntos pueden causar serios problemas.

Las cintas magnéticas pueden ser destruidas por temperaturas de sólo 54 grados cuando la humedad relativa es del 85 por 100. Estas condiciones pueden producirse fácilmente dentro de un coche cerrado en un día caluroso.

Proteja su sistema contra daños causados por el agua

Daños por agua pueden ocurrir como resultado de goteas de la tapa del techo de la torre de enfriamiento, goteo del techo, goteas de tuberías de techo y de operaciones de sistemas de regadío en pisos sobre el Centro de Procesamiento de Datos. Proteger el equipo, así como los muebles y cabinas contra agua y trazar un plan para la rápida eliminación de algo de agua que podría entrar en el área.

Poner particular atención en la instalación de desagües bajo el piso construido donde están instalados los sistemas de cables. La conveniencia de cubiertas plásticas son inapreciables en la protección del equipo contra el agua, procedente de filtraciones a través del techo.

Fallas en infraestructura: servicios

Instalaciones eléctricas

Para que funcionen adecuadamente, las computadoras personales necesitan de una fuente de alimentación eléctrica fiable, es decir, una que se mantenga dentro de parámetros específicos. Si se interrumpe inesperadamente la alimentación eléctrica o varia en forma significativa, fuera de los valores normales, las consecuencias pueden ser serias. Pueden perderse o dañarse los datos que hay en memoria, se puede dañar el hardware, interrumpirse las operaciones activas y la información podría quedar temporal o definitivamente inaccesible.

Por lo general las computadoras personales toman la electricidad de los circuitos eléctricos domésticos normales, a los que se llama tomas de corriente. Esta corriente es bastante fuerte, siendo una **corriente alterna** (ac), ya que alterna el positivo con el negativo. La mayor parte de las computadoras personales incluyen un elemento denominado fuente de alimentación, la cual recibe corriente alterna de las tomas de corriente y la convierte o transforma en la corriente continua de baja potencia que utilizan los componentes de la computadora.

La fuente de alimentación es un componente vital de cualquier computadora personal, y es la que ha de soportar la mayor parte de las anomalías del suministro eléctrico. Actualmente existe el concepto de fuente de alimentación redundante, la cual entrará en operación si de detecta una falla en la fuente de alimentación principal.

En nuestro medio se han podido identificar siete problemas de energía más frecuente:

1. Fallas de energía.
2. Transistores y pulsos.
3. Bajo voltaje.
4. Ruido electromagnético.
5. Distorsión.
6. Alto voltaje.
7. Variación de frecuencia.

Existen dispositivos que protegen de estas consecuencias negativas, los cuales tienen nombres como:

Supresores de picos.
Estabilizadores, y
Sistemas de alimentación interrumpida (SAI o UPS: UNINTERRRUPTIBLE POWER SISTEM).

Como prever las fallas que generan altas temperaturas

Para entender algunas de las cosas que pueden dar problemas en los circuitos eléctricos, puede servir de ayuda imaginarse que la electricidad llega desde la central eléctrica hasta los enchufes de la oficina, sale por el hilo activo y a continuación vuelve a la central a través del neutro, tras haber realizado su trabajo. Los materiales a través de los cuales la electricidad fluye libremente, como es el cobre de los cables de la oficina, se denominan conductores. La electricidad es esencialmente perezosa, intentando volver a la central eléctrica lo más rápidamente posible a través de cualquier conductor disponible.

Lo que impide que la electricidad vuelva demasiado pronto es el aislamiento, el cual impide el paso de la electricidad. La goma, el plástico y una gran cantidad de materiales no metálicos son buenos aislantes. Por ejemplo la carcaza de algunas computadoras está hecha de metal conductor, pero si se toca ésta nos da una descarga eléctrica, porque los aislantes mantienen la corriente dentro de los componentes internos del sistema.

Sin embargo bajo ciertas condiciones extremas, como puede ser un voltaje muy alto, incluso los mejores aislantes dejan de actuar, permitiendo que la corriente fluya por donde no debería.

Las fallas en los circuitos eléctricos se producen a menudo por un aislante o un conductor que no trabaja adecuadamente, generando inconvenientes, por lo general, altas temperaturas. Existen formas de prever estas fallas y tecnologías para minimizar el impacto de éstas; como por ejemplo:

a) Tomas de tierra.

Se denomina así a la comunicación entre un circuito eléctrico y el suelo natural para dar seguridad a las personas protegiéndolas de los peligros procedentes de una ruptura del aislamiento eléctrico.

También se le llama puesta a tierra. La comunicación con tierra se logra mediante la conexión de un circuito dado (toma corriente) a un conductor en contacto con el suelo. Estas conexiones a tierra se hacen frecuentemente por medio de placas, varillas o tubos de cobre enterrados profundamente en la tierra húmeda, con o sin agregados de ciertos componentes como

carbón vegetal, salo elementos químicos ("laborgel", etc.), según especificaciones técnicas indicadas para las instalaciones eléctricas.

Objetivo. El objetivo de una toma a tierra puede ser de distintos tipos. En la práctica sirve para proteger de contactos accidentales las partes de una instalación no destinada a estar bajo tensión y, para disipar sobre tensiones de origen atmosférico o de origen industrial, ya sea por maniobra o por pérdida de aislamiento.

La toma a tierra limita la tensión que, con respecto a tierra, puede aparecer en cualquier elemento conductor de una instalación y asegura con ello la correcta actuación de los dispositivos de protección de la instalación eléctrica.

Funciones. La toma a tierra cumplirá las siguientes funciones:

Proteger a las personas, limitando la tensión que respecto a la tierra, puedan alcanzar las masas metálicas.

Proteger a personas, equipos y materiales, asegurando la actuación de los dispositivos de protección como: pararrayos, descargadores eléctricos de líneas de energía o señal, así como interruptores diferenciales.

Facilitar el paso a tierra de las corrientes de defecto y de las descargas de origen atmosférico u otro.

Partes. Todo sistema de Toma a tierra constará de las siguientes partes:

Toma de Tierra o Puesta a Tierra.
Línea principal de tierra.
Derivaciones de las líneas principales de tierra.
Conductores de protección.

Mantenimiento. Las inspecciones deben realizarse anualmente, con el fin de comprobar la resistencia y las conexiones. Es recomendable que esta labor se efectúe en los meses de verano o en tiempo de sequía, con el fin de evaluarlas en el momento más crítico del año por falta de humedad.

Es recomendable un mantenimiento preventivo de 3 a 4 años dependiendo de las propiedades electroquímicas estables.

b) Fusibles

Al cablear la computadora, la carcaza normalmente se conecta a la tercera patilla del cable de alimentación. En algunos casos, puede que la tierra se conecte también al neutro. Si la electricidad pasara a través del aislante y llegase a la carcaza, entonces pasaría directa desde el conductor de tierra hasta ésta. Simultáneamente, esta derivación de electricidad aumentaría la intensidad de corriente que va por el circuito. Este incremento puede ser detectado por un fusible o un diferencial. Estos dos dispositivos están diseñados para interrumpir un circuito si se sobrecargan (Un fusible debe ser sustituido tras fundirse, mientras que un diferencial se debe restaurar tras saltar) Si una parte de una computadora funde un fusible o hace saltar un

diferencial, primero se debe desconectar el equipo. A continuación debe desconectarse el cable de alimentación que lleva al equipo y buscar la falla que ha hecho saltar el fusible. Arreglado el problema, se puede volver a conectar el equipo. Vuelva a encender el equipo, pero esté preparado para tener que apagarlo de nuevo, y rápidamente, si el problema no se hubiera arreglado adecuadamente.

Entre las causas menos problemáticas para que se fundan los fusibles o salten los diferenciales se encuentra la sobrecarga de un circuito eléctrico. Para corregir esto se necesita reorganizar la distribución de enchufes sobre las placas, distribuyendo la carga de forma más uniforme.

Entre las fallas más serias, se incluyen los cables dañados de forma que el aislante entre los conductores se ha roto. En los aparatos, los aislantes pueden decaer o fundirse, dando lugar a cortocircuitos. Al sustituir los fusibles de una computadora, se ha de tener cuidado que todos los equipos deben estar apagados y desconectados antes de cambiar el fusible. No se debe olvidar que algunos elementos del equipo, como es el caso de los monitores, pueden mantener una carga de alto voltaje incluso, después de haberse apagado.

Debe asegurarse que el fusible de recambio es de la misma capacidad que el fundido. Por ejemplo, si el fusible fundido viene marcado como de 2 amperios, no se debe sustituir por uno de 3 amperios. Un fusible de 3 amperios dejará pasar 1 amperio más de intensidad de lo que fijó el diseñador del equipo. Si se siguen fundiendo fusibles en el equipo, entonces hay algo que funciona mal.

No se apruebe las reparaciones de los fusibles, usando hilos de cobre o similares.

c) Extensiones Eléctricas y capacidades

Las computadoras personales a veces ocupan rápidamente todas las tomas de corriente. Pocas oficinas se encuentran equipadas con las suficientes placas de pared. Dado que es necesario conectar además algún equipo que no es informático, es fácil ver que son muy necesarias las extensiones eléctricas múltiples. El uso de estas extensiones eléctricas debe ser controlado con cuidado por los responsables de las oficinas. No sólo para que no queden a la vista, sino también porque suponen un peligro considerable para aquellos que tengan que pasar por encima. Aparte del daño físico que puede provocar engancharse repentinamente con el cable, se trata de una forma rápida y poco agradable de desconectar un sistema completo.

Por razones de seguridad física y de trabajo se recomienda tener en cuenta las siguientes reglas:

Las extensiones eléctricas deben estar fuera de las zonas de paso, siempre que sea posible.
Se debe utilizar canaletas de goma adecuadas para cubrir los cables, si van a cruzar una zona de paso.
No se debe encadenar sucesivos múltiples, ya que esto puede hacer que pase más corriente de la que los cables están diseñados para soportar. Utilice los enchufes de pared siempre que sea posible.
Si es posible, utilizar extensiones eléctricas que incluyan fusibles o diferenciales. Esto puede ayudar a limitar el daño ante fallas eléctricas.
Se debe comprobar siempre la carga frente a las extensiones eléctricas. La mayor parte de ellas llevan los amperios que admite cada extensión, no debiendo superar esta cifra el amperaje total de todos los aparatos conectados a ellas.

Adquiera toma corrientes de pared y/o extensiones eléctricas mixtas, capaces de trabajar tanto con enchufes de patas planas, como cilíndricas.
Tanto los toma corrientes de pared como las extensiones eléctricas deben tener toma a tierra.

Caídas y subidas de tensión

Las caídas y subidas de tensión y los picos tienen un impacto negativo en todo tipo de aparato electrónico, entre los que se incluyen las computadoras personales, los monitores, las impresoras y los demás periféricos.

Lo que causa problemas en las computadoras personales son las grandes oscilaciones en el voltaje. Por ejemplo, una caída por debajo de los 200V y una subida por encima de los 240V. Si una caída dura más de una fracción de segundo, puede generar una falta de alimentación a la memoria de acceso aleatorio, con lo que los datos que allí se encuentren, pueden perderse o, como mínimo, resultar desordenados. Es más, el efecto de la vuelta de la corriente a su valor normal puede tener también efectos perniciosos.

Los efectos de una subida son difíciles de predecir, dependiendo hasta cierto punto de la fuente de alimentación de la computadora. Esta tiene un efecto moderador sobre subidas de la corriente, pero puede que no sea suficiente para evitar cortes temporales en los circuitos que lleven a que se desordenen los datos o incluso se dañen los circuitos impresos. Un comportamiento errático es el primer síntoma de una subida de tensión.

Si se es cuidadoso, es bastante aconsejable medir el voltaje. Un típico multímetro digital, dará una medición del voltaje si introduce sus terminales en el enchufe.

Si la lectura del voltaje continúa fluctuando, anote la medida más alta y la más baja. Si se encuentran dentro de un margen del 5 por 100, alrededor del voltaje esperado, probablemente no causará ningún problema. Si las oscilaciones se encuentran fuera de este margen, puede ser recomendable pedir que un electricista revise el cableado e invertir en algún equipo de acondicionamiento de corriente (Estabilizadores de Voltaje).

a) Supresores de subidas de tensión

Una protección relativamente barata ante las subidas de tensión es un supresor de subidas. Este es un dispositivo eléctrico situado entre la computadora personal y la fuente de corriente. Incluye una circuitería electrónica que recorta el voltaje cuando éste comienza a subir por encima de un nivel aceptable. El supresor de subidas evita que las "Subidas de la corriente de alimentación peligrosas lleguen al equipo.

La circuitería del supresor de subidas es bastante compacta, por lo que estas unidades pueden encontrarse con distintas formas y tamaños. Cualquier buen supresor de subidas de tensión debe contar con las siguientes características:

Ructor de circuito. Cualquier supresor de sobre tensiones debe incluir un ruptor del circuito, un conmutador rearmable que corta la alimentación si se sobrecargan los circuitos (normalmente un switch). Este es el mínimo nivel de protección para cualquier dispositivo, debiendo incluso la extensión eléctrica múltiple más sencilla, de incluir uno. También cabe señalar el hecho de que una extensión eléctrica múltiple tenga un ruptor, no lo convierte en un

supresor de sobretensiones. Se ha de señalar que si un ruptor ha saltado, no se debe rearmar (apretar el switch) hasta que no se haya determinado primero la causa que lo hizo saltar.

Protección separada. Muchos supresores de subidas de tensión ofrecen varios puntos de conexión para conectar el sistema. El diseño de la unidad debe proteger cada punto de conexión de forma separada. Con este diseño es fácil que pueda hacer frente a subidas más grandes que con otro en que simplemente se protege la línea que va al múltiple. La protección separada también puede contribuir a reducir la interferencia de ruido entre los distintos elementos conectados al mismo circuito de alimentación.

Medidas. Se puede encontrar distintas medidas relativas a los supresores de subidas de tensión en la documentación que traen. Una medida básica es la capacidad, en términos de la corriente total que el dispositivo está diseñado para proteger. Esta medida tiene aquí el mismo significado que para una extensión eléctrica múltiple. Si éste o el supresor presentan un valor de 10 amperios, en ese caso el total de intensidad de todos los equipos conectados al elemento no debe superar esa cantidad. El voltaje de cierre inicial es la tensión a la que se produce el efecto de cierre de la circuitería del elemento.

b) Picos

Una variación en la corriente más peligrosa y difícil de medir son los picos. Estos consisten en una súbita subida de tensión a niveles muy altos. Muchos de estos picos son causados por la conexión y desconexión de grandes aparatos eléctricos. Los picos son de dos tipos distintos:

Modo Normal y

Modo Común. .

Los sucesos de modo normal se pueden medir entre los hilos activo y neutro del circuito eléctrico del edificio. Los de modo común se miden entre el neutro y la tierra.

Un pico en modo normal de gran magnitud puede dañar la fuente de alimentación de la microcomputadora. Sin embargo, un pico en modo común de sólo unas pocas docenas de voltios puede dañar los circuitos lógicos o producir errores entre las computadoras.

Protección frente a Picos. Los circuitos supresores de sobretensiones ofrecen buena protección frente a picos en modo normal, pero podría causar algunos de modo común. Por ello, muchos supresores de sobre tensión también poseen una circuitería para bloqueo de picos separada, y se comercializan como protectores para sobretensiones y picos.

Los criterios de adquisición de un protector ante picos son en gran parte los mismos que los de los protectores ante sobretensiones, siendo normal y deseable que una misma unidad ofrezca protección ante ambos, aunque se debe comprobar sus especificaciones para asegurarse. La capacidad de impedir que los picos alcancen el equipo a veces se miden en julios.

Un julio es una medida de energía, la energía consumida durante cierto periodo de tiempo, así por ejemplo, un producto puede venir con la especificación de que suprime picos de 140 julios.

También puede venir con una especificación en amperios, como seria "picos de 140 julios a 6.500 amperios". Por lo general, cuando mayor sea el voltaje - julios - amperios que el protector puede tratar, se considera mejor.

Ruido electrónico

Las subidas y caldas de tensión y los picos no son el único problema eléctrico al que se han de enfrentar los usuarios de computadoras. También está el tema del Ruido, no se trata del que se puede oír, sino del ruido eléctrico que interfiere en el funcionamiento de los componentes electrónicos.

Para describir el ruido se utilizan dos términos:

Interferencia de radiofrecuencia (RFI)

Interferencia electromagnética (EMI)

Este ruido se puede ver literalmente cuando se utiliza un taladro eléctrico cerca de un televisor. El motor eléctrico del taladro hará que aparezcan líneas, nieve u otras alteraciones en la pantalla. Una interferencia similar puede ser causada por las bujías de un automóvil. También puede generarse interferencia de radio con teléfonos inalámbricos que utilizan ondas de radio para comunicar entre la unidad móvil y la base. No sólo la recepción de la TV, sino también la integridad de los datos dentro de una computadora están en peligro ante éstas u otras fuentes de interferencia.

Las computadoras personales corren el riesgo de sufrir tanto interferencias externas como emisiones electromagnéticas y de radio creadas por las propias computadoras. Muchos de los circuitos de una computadora generan EMI y RFI.

El ruido eléctrico también afecta a las transmisiones telefónicas. Se pueden conseguir filtros para las líneas telefónicas que realizan transmisión de datos y fax. En algunos casos, éstos vienen combinados con supresores de subidas de tensión y picos. La línea de teléfono de la pared se acopla a la unidad supresora, y a continuación se conecta el teléfono - modem - fax a la unidad, quedando la línea telefónica filtrada y protegida.

El otro aspecto de los problemas de ruido con el teléfono es la interferencia de los teléfonos con las computadoras personales.

Esto ocurría a menudo con los primeros teléfonos inalámbricos, pudiendo ser necesario tener la unidad de base del teléfono inalámbrico lejos de la computadora.

Protección ante el Ruido. Para proteger las computadoras de las interferencias electromagnéticas y de radio frecuencia es necesario considerar lo siguiente:

Ruido en la línea de alimentación

Algunos supresores de subidas de tensión y picos están diseñados con una circuitería que filtra el ruido de la fuente de alimentación. La supresión del ruido se mide en decibeles.

Situación de los aparatos

Como regla general se puede decir que las computadoras personales y los aparatos eléctricos de gran consumo no congenian. Cuando se instalan puestos de trabajo con computadoras se debe intentar tenerlos lejos de estos equipos. Es difícil suprimir la interferencia generada por las potentes corrientes que circulan por estas máquinas, como son las grúas, ascensores, prensas de imprenta y los soldadores eléctricos. En la mayor parte de las oficinas esto no es un problema, otros aparatos de oficina, como son las fotocopiadoras, están normalmente apantalladas. Sin embargo, los ascensores pueden ser un problema en los edificios de oficinas, y el uso industrial de las computadoras crece rápidamente. Por ello, en algunos casos será necesario encerrar la computadora personal en una caja metálica, para protegerla de las interferencias del ruido eléctrico.

Otros equipos informáticos

Un buen supresor de subidas de tensión y ruido, filtrará la interferencia por ruido en la red entre los distintos componentes conectados a él. Sin embargo la carcaza exterior de algunos componentes puede que no esté adecuadamente apantallada, dando lugar a interferencias entre los dispositivos.

Es útil no olvidar que los problemas de incompatibilidad por ruido electromagnético aparecen de cuando en cuando, incluso con productos del mismo fabricante.

Conmutación

Cuando se abren o cierran los conmutadores, algo de electricidad se escapa en forma de chispa, corto, sobre tensión o pico. Si se conecta y desconecta un secador de pelo en una habitación oscura probablemente verá este fenómeno. Si desenchufa el secador mientras está funcionando probablemente verá una chispa en el enchufe.

Estas chispas pueden tener dos aspectos negativos sobre los sensibles equipos de las computadoras. En primer lugar el pico, la subida brusca de voltaje frente a la que nos protegen los protectores de picos.

El segundo efecto negativo de la conmutación es el tema mucho más complejo de los armónicos, frecuencias eléctricas sustancialmente más altas que la corriente que las ha producido.

La acción rápida del conmutador tiene el mismo efecto que el golpe con el dedo que produce armónicos en la cuerda de una guitarra. La generación de estas frecuencias no deseadas por un elemento del equipo, puede interferir con el funcionamiento de un elemento próximo.

Los buenos protectores ante sobretensiones y picos que suministran tensión a más de un elemento, ofrecerán algún tipo de aislamiento para cada elemento con el objetivo de evitar este problema, algunas veces descrito como ruido.

Reglas para evitar problemas de conmutación. Se puede ayudar a evitar estos problemas siguiendo las siguientes reglas:

No enchufar ni desenchufar aparatos eléctricos que estén encendidos

No enchufar ni desenchufar especialmente las computadoras, impresoras y monitores. A menudo estos aparatos poseen alguna forma de protección en sus circuitos de conexión que no pueden actuar, si estando encendido el aparato, lo desenchufamos o lo enchufamos. Debido a que conectar por separado cada elemento del equipo puede ser una rutina desagradable, puede ser

recomendable utilizar un centro de conexión, una unidad con protección ante sobretensiones y picos con diseño en forma de consola que alimenta a todos los elementos del sistema

Garantizar el suministro electrónico

Las caídas, subidas de tensión y los picos tienen un impacto negativo en todo tipo de aparato electrónico, entre los que se incluyen las computadoras, monitores, las impresoras y los demás periféricos.

Un corte de la alimentación de la unidad principal puede:

Hacer que desaparezca la información que hay en la RAM. Los datos recién introducidos o recién editados que no se hayan grabado, se pierden.

Se interrumpe el proceso de escritura en el disco. Se puede perder información de importancia que necesita el sistema operativo, como puede ser la localización de un archivo, dando como resultado que pierdan o desorganicen archivos.

Puede "aterrizar" un disco fijo. La cabeza de lectura -escritura de la mayor parte de los discos fijos se separa automáticamente del disco cuando se desconecta la unidad, pero puede ocurrir en algunos sistemas que la cabeza "aterrice" sobre la superficie del disco y la dañe, dando lugar a que se pierdan datos e incluso, resulte dañado físicamente el disco.

Interrumpir impresión. Cuando vuelva la tensión se han de continuar los procesos de impresión.
En algunos casos se ha de volver a comenzar el proceso de impresión.

Se interrumpen las comunicaciones. Cuando vuelve la corriente, los datos que se estaban transfiriendo entre las computadoras deben de ser comprobados para tener exactitud, y los archivos que se estaban transmitiendo puede que haya que volver a transmitirlos.

Detiene el trabajo.

El sistema queda expuesto a picos y subidas de tensión cuando vuelve la tensión. Normalmente se desconectan los equipos cuando se va la corriente, pero esto no siempre es posible. Cuando la empresa de electricidad restaura el servicio, a menudo viene con picos que pueden dañar los aparatos que no se hubieran desconectado.

a) U.P.S o S.AJ. (sistema de energía ininte-rrumpible)

Energía de seguridad para un sistema de computación, cuando la energía eléctrica de la línea se interrumpe o baja a un nivel de tensión inaceptable. El UPS suministra electricidad a una PC (estación o servidor) cuando falla el fluido eléctrico. Esta unidad hace transparente a las interrupciones de fracciones de segundo que inevitablemente detiene a los sistemas y le permite seguir trabajando durante varios minutos. Los pequeños sistemas UPS proveen energía de baterías por sólo unos pocos minutos. Los sistemas más sofisticados están conectados a generadores eléctricos y pueden proveer energía durante días enteros. Los sistemas UPS proveen generalmente protección contra sobrecarga y pueden proveer asimismo regulación de tensión.

Selección de un UPS. Al seleccionar un UPS se debe tener en cuenta los siguientes factores principales:

Requerimientos de Potencia (actuales y futuros)
Requerimiento de frecuencia
Tiempo de respaldo requerido
Futuras Expansiones
Picos por corriente de arranque
Servicio de Mantenimiento
Soporte Técnico (antes, durante y después de la instalación)

Tecnologías de UPS. Mencionaremos las siguientes:

OFF-UNE, STAND BY (FUERA DE LINEA)
LINEA INTERACTIVA
TRUE ON-LINE (EN VERDADERA LINEA)

UPS OFF LINE ¡FUERA DE LINEA. El flujo normal de energía que abastece la carga en un UPS-off-Line, es a través de un by-pass. Esta configuración utiliza un cargador tipo stand by para cargar las baterías después de una descarga, debido a que el inversor tipo stand by suministra energía a la carga después de una condición de pérdida o bajo voltaje. Este tipo de sistema abastece la carga con energía eléctrica muy poco filtrada.

Durante una caída de tensión en la línea, el inversor actúa en tiempos de 3 y 4 ms. y la carga es ahora abastecida por el inversor. La proximidad a una onda sinusoidal de la energía que proporciona el inversor, dependerá totalmente del diseño y tipo de éste, lo que redundará directamente en el costo del UPS. La señal de salida del inversor en el UPS-off-line es generalmente onda cuadrada.

Ventajas:

Bajo costo debido, entre otras cosas, a la utilización de un pequeño cargador, inversor mucho menos sofisticado y a la eliminación de la circuitería para el by-pass.

La eficiencia normal de operación es alta (95-98%).
La mayoría de sus componentes tendrán bajo número de horas de operación.
La poca utilización de los componentes de los sistemas off-line, da como resultado que éstos puedan ser contenidos en configuraciones físicas pequeñas.
Los transientes eléctricos que producen este tipo de UPS son aceptados por la mayoría de cargas eléctricas poco sofisticadas, tales como las que contienen fuentes de switcheo.

Desventajas:

Durante la operación normal, no hay acondicionamiento de energía.

Durante la caída o pérdida total de energía en la línea, la carga crítica es transferida al inversor en un tiempo típico de 4ms., pudiendo existir en este intervalo transientes que puedan afectar a cargas electrónicas sensitivas.

Tiempos mayores de recarga de sus baterías.

Los problemas en el inversor no pueden ser detectados hasta que el inversor esté operando para dar soporte a la carga.

Línea interactiva. La tecnología de línea interactiva es básicamente la misma que la tecnología OFF-UNE, con la diferencia que cuenta adicional mente con un regulador automático de voltaje (AVR). Durante la condición de bajo voltaje, el AVR lo incrementa a un voltaje aceptable para la carga, disminuyendo así el número de veces que el inversor actúa sobre las baterías.

Ventajas:

Menor precio que los equipos On-Une, debido a la utilización de un pequeño cargador de baterías, un inversor menos sofisticado debido a la eliminación de la circuitería para el by-pass.

Eficiencia normal de operación alta (95-98%).

El bajo uso de sus baterías extiende la vida útil de las mismas.

La mayoría de los componentes, igual que en los sistemas Off-Une, tendrán bajo número de horas de operación.

Los transientes eléctricos que producen este tipo de UPS, son aceptados por la mayoría de cargas eléctricas poco sofisticadas, tales como las que contienen fuentes de switcheo.

Mejor filtrado de la línea debido a la utilización del A VR.

Onda sinusoidal tanto al trabajar con el A VR o el inversor.

Desventajas:

Durante la caída o pérdida total de energía en la línea, la carga crítica es transferida al inversor en un tiempo típico de 4ms., pudiendo existir en este intervalo transientes que puedan afectar a cargas electrónicas sensitivas.

Tiempos mayores de recarga de sus baterías.

Los problemas en el inversor no pueden ser detectados hasta que el inversor esté operando para dar soporte a la carga.

True on line/en verdadera línea. El flujo normal de energía en un UPS True On Line, es a través del rectificador/cargador y del inversor, para así soportar la carga crítica. Esta utiliza circuitería especial de by-pass para los casos en que el inversor sea sobrecargado, ya sea dentro de la operación normal o debido al exceso de corriente que utilizan algunas cargas durante su arranque, y también para los casos en que se requiera dar mantenimiento al UPS sin que sea necesario apagar la carga.

Este tipo de sistema abastece la carga crítica con energía continua regulada y acondicionada sin ninguna variación de voltaje o de frecuencia.

Durante la pérdida de tensión en la línea o al estar fuera del rango de tolerancia, el inversor utilizará las baterías para abastecer de energía a la carga sin tiempo de transferencia, debido a que el rectificador-cargador y las baterías operan continuamente en paralelo y también, a

que no hay switcheo involucrado para hacer cambio de modo de operación normal al modo de descarga de baterías o emergencia.

Ventajas:

Provee energía continua regulada y acondicionada a la carga crítica, dándole a ésta la tensión sin variaciones en voltaje ni en frecuencia.

En esta tecnología no existe el requerimiento de intercambiar corriente alterna a corriente directa y viceversa, durante una pérdida de energía en la línea o durante el ciclo de descarga de baterías, por lo que elimina así la posibilidad de transientes de conmutación que pueden afectar la carga.

La alta capacidad del rectificador-cargador produce entre otras cosas una carga mucho más rápida de las baterías.

Proveen una salida de energía de excelente calidad para una operación adecuada de la carga crítica conectada.

Las funciones independientes del rectificador-cargador, el inversor y el switch estático en esta tecnología, producen una operación sumamente confiable del UPS.

Mantenimiento:

Antes de instalar la unidad, se recomienda hacer una inspección ocular del estado del equipo recepcionado, si no está en perfectas condiciones, deberá notificarse al proveedor respectivo.

Escoger una localización que esté limpia y seca, donde la temperatura ambiental no exceda de 35°C. No colocar el UPS en un espacio cerrado donde el flujo de aire esté restringido. Como el flujo de aire es de interés primordial, asegurarse de que el área en que el UPS debe ser localizado no esté sujeto a la contaminación de polvo, gases corrosivos, exceso de humedad, vapor de aceite u otras sustancias combustibles.

Al limpiar el equipo, no usar líquidos o agentes de limpieza a base de aerosol. Se puede mantener el UPS limpio y fresco, aspirando periódicamente los depósitos de polvo alrededor de las rejillas de ventilación y limpiando la unidad con un paño seco.

b) Grupo electrogeno

Máquinas que generan energía eléctrica, aprovechando la energía máxima producida por máquinas de combustión interna.

Una planta generadora ideal, deberá tener el rendimiento y capacidad adecuada para alcanzar los requerimientos de carga que va a soportar. .Esta hará que no tenga capacidad excesiva o funciones innecesarias que incrementarían el costo inicial y el costo de operación.

Para obtener el rendimiento y la confiabilidad adecuada, se recomienda que se declare las especificaciones en términos de rendimiento deseado, en vez de intentar especificar un determinado tamaño, tipo o marca de equipo.

Es necesario mencionar que el circuito de generación eléctrica produce extraños voltajes y corrientes en el circuito de comunicación telefónica. Esto puede ser peligroso para las personas o puede dañar los aparatos o interferir las comunicaciones. Por eso, se debe evitar la proximidad de un grupo electrógeno con los circuitos telefónicos y proteger éstos con dispositivos que eviten los peligros y la interferencia.

Tablero de Control. El tablero de control debe ser diseñado de acuerdo al voltaje y corriente que se propone soportar, y debe ser equipado con los dispositivos necesarios de protección contra fallas para proteger al generador de daños, cuando hay fallas o sobrecargas en el sistema.

Mantenimiento.

La limpieza con paño seco puede ser satisfactoria cuando los componentes son pequeños. Generalmente se recomienda soplar la suciedad con aire comprimido, especialmente en los lugares donde se ha juntado tierra y no se puede llegar con el paño.

El polvo y la tierra pueden quitarse con una escobilla de cerdas y luego aspirar. No usar escobilla de alambre.

Los componentes eléctricos, después de la limpieza, almacenamiento o embarque deben secarse antes de hacerlos funcionar.

Comprobar la zona alrededor de las aberturas de admisión y escape del aire estén limpias y sin obstrucciones.

Inspeccionar que no haya conexiones sueltas o contaminadas. Si durante la inspección se muestra que los revestimientos de barniz de los devanados se han deteriorado, se les debe volver a cubrir con barniz de aislamiento.

Como regla general, los cojinetes deben relubricarse anualmente. Condiciones de operación muy severas, tales como ambientes muy calurosos y polvorientos, requerirán una lubricación más frecuente. .

En caso que los grupos electrógenos sean usados sólo en emergencias, se debe establecer una política de puesta en funcionamiento los fines de semana durante 1 ó 2 horas, para mantener operativo los equipos.

Bibliografía Capitulo VI

Echenique, José Antonio. 1994. "Auditoría en Informática". McGraw-Hill

H., David. 2001. "Auditoría en Centros de Cómputo: Objetivos, Lineamientos y Procedimientos. Trillas. México.

Hernández, Hernández Enrique. 2002. "Auditoría Informática: Un Enfoque Practico Metodológico". CECSA. México.

Piattini, Mario G. 1998. "Auditoría Informática". Alfaomega

Piattini, Mario G. Y Del peso, Emilio. 2001. "Auditoría Informática: Un Enfoque Practico". Alfaomega. México.

Administración de Centros de Cómputo
http://members.es.d/ofal/Tutor/OrgCentroComputo.htmll

Administración de Centros de Cómputo
http://www.educar/educadores/iguerrero/AdmoCC/acc.html

Administración de Centros de Cómputo
http://galeon.hispavista.com/zaboot/analisiscc.htmll

Toro Oscar. 26/12/1999. "Manual de auditoría de sistemas".
http://www.monografias.com/trabajos/maudsist.shtml

D'Sousa Carmen. 27/11/2002. "Auditoria de Sistemas"
http://www.monografias.com/trabajos11/siste/siste.shtml#eva

Cancelado González Alberto. 16/11/2004. "Sistema de administración de riesgos en tecnología informática".
http://www.monografias.com/trabajos14/riesgosinfor/riesgosinfor2.shtml#do

http://www.aceproject.org/main/espanol/et/ete08.htm

http://apuntes.rincondeIvago.com/auditoria-de-sistemas-informaticos.html

Casiano Quevedo Julio C., García Vázquez Israel. 12/12/2000. "Administración de servicios de centro de computo".
http://www.itver.edu.mx/comunidad/material/serv-computo/ascc/links.html

Horacio Quinn Eduardo. 08/11/2000. "La Auditoria informática dentro de las etapas de análisis de sistemas administrativos".
http://www.monografias.com/trabajos5/audi/audi.shtml#redes

Jiménez José Alfredo. 04/08/2003. "Evaluación seguridad de un sistema de información".
http://www.ilustrados.com/publicaciones/EpyppFyEAyLgAPFJNN.php

Toro Oscar. 04/08/2003. "Manual de auditoría de sistemas".
http://www.itapizaco.edu.mx/paginas/maudisist.html

Instituto Nacional de Estadística e Informática “Plan de Contingencias y Seguridad de la Información
http://www.inei.gob.pe/web/metodologias/attach/lib611/0300.htm
José Alfredo Jiménez. 04/08/2003. “Evaluación seguridad de un sistema de información”.
http://www.ilustrados.com/publicaciones/EpyppFyEAyLgAPFJNN.php

Oscar Toro. 04/08/2003. “Manual de auditoría de sistemas”. http://www.itapizaco.edu.mx/paginas/maudisist.html

Instituto Nacional de Estadística e Informática “Plan de Contingencias y Seguridad de la Información
http://www.inei.gob.pe/web/metodologias/attach/lib611/0300.htm