INTRODUCCIÓN

En el ensayo que a continuación presento, hice un estudio concreto de la auditoría informática en seguridad física en el cual muestro las ventajas que se obtienen al efectuarla; lo primordial es que su uso permite reducir riesgos, entre algunos de ellos son: inundación, terremoto, fuego y sabotaje en las áreas de cómputo.

A su vez desarrollé este estudio de ventajas de la auditoría informática en seguridad física para dar a conocer el estado actual y futuro posible de seguridad informática, porque pienso que no es justo que continuamente se ponga en tela de juicio el arduo trabajo de los auditores informáticos, debido a que en muchas ocasiones la gente conoce muy poco de las ventajas que conlleva efectuar la auditoría informática en seguridad física dentro de sus áreas de cómputo y también desconocen la magnitud del problema que enfrentarán al no llevar a cabo dicha auditoría; además intenté brindar algunos planes de estrategia y metodología, que si bien no brindan la solución total como muchos prometen, creo que pueden cubrir parte de lo esencial que hoy se presenta al hablar de auditoría informática en seguridad física.

Por otra parte llevé a cabo este estudio mediante el análisis de algunas metodologías de Auditoría Informática que dependieron de lo que pretendí revisar y analizar, pero como estándar analicé las cuatro fases básicas de un proceso de revisión; las cuales fueron: Estudio preliminar, Revisión y evaluación de control y seguridad, Examen detallado de áreas criticas y Comunicación de resultados.

Además en este estudio que realicé obtuve resultados favorables para mi investigación ya que durante el análisis de las ventajas en la seguridad física en el área de cómputo mediante la utilización de la auditoría informática, pude percatarme que es una función que debería considerarse primordial dentro de cualquier organismo, ya que esta manera se tendrá controlado el ambiente y acceso físico obteniendo como resultado la disminución de siniestros.

INDICE

PLANTEAMIENTO DEL PROBLEMA

En la auditoría informática en seguridad física no existen los trabajos semejantes, ya que está se encarga de dar resguardo específicamente al hardware y al personal que labora dentro del área de cómputo; pero sin olvidar que el software debe tener una buena política de respaldo para que de esta forma sea un resguardo eficiente, ya que al proteger al hardware protegemos los datos que hay dentro de el y como anteriormente lo mencioné el hardware esta asegurado por la seguridad física. Por consiguiente quiero resaltar este punto:

¿La utilización de la auditoría informática en seguridad física permitirá reducir los riesgos de inundación, terremoto, fuego y sabotaje en las áreas de cómputo?

SUBPREGUNTAS DE INVESTIGACIÓN:

- ¿Por qué es tan importante llevar a cabo la auditoría informática en seguridad física en las áreas de cómputo?
- ¿Cuál es la metodología que se debe llevar a cabo para lograr una buena auditoría informática en seguridad física dentro del área de cómputo?
- ¿La auditoría informática establecida permitirá tener pruebas exhaustivas de los bienes informáticos deseados en el área de cómputo?
- ¿Mediante la utilización de la auditoría informática en seguridad física es posible tener ventajas en la supervisión del servicio brindado a los equipo de las áreas de cómputo y también en el lugar donde esta ubicado?
- ¿Con la auditoría informática se puede tener un mejor manejo de medidas de seguridad para el resguardo de los bienes informáticos del área de cómputo?

JUSTIFICACIÓN

Es muy importante estar conscientes de que por más que el área de cómputo de cualquier empresa o institución sea la más segura desde el punto de vista de ataques externos, disturbios, sabotajes, etc.; la seguridad de la misma será nula si no se ha previsto como combatir un incendio.

Por consiguiente la seguridad física es uno de los aspectos más olvidados a la hora del uso de un sistema informático. Si bien, algunos de los aspectos más comunes se prevén, otros no, como la detección de un atacante interno al área de cómputo de la empresa o institución que intentan acceder físicamente a una sala de operaciones de la misma. Se considera que esto puede derivar en que para un atacante sea más fácil lograr tomar y copiar una cinta de la sala, que intentar acceder vía lógica a la misma.

Así, la Seguridad Física consiste en la "aplicación de barreras físicas y procedimientos de control, como medidas de prevención y contramedidas ante amenazas a los recursos e información confidencial". Se refiere a los controles y mecanismos de seguridad dentro y alrededor del Centro de Cómputo así como los medios de acceso remoto al y desde el mismo; implementados para proteger el hardware y medios de almacenamiento de datos.

No obstante, considero que si se lleva a cabo la seguridad física dentro de un área de cómputo hay menos pérdidas económicas con respecto al mecanismo de seguridad; porque si se efectúa una comparación entre dos áreas de cómputo, una con seguridad física y otra sin seguridad física, puedo asegurar que el área que la efectúa esta protegida ante cualquier daño y que suponiendo que esas empresas invierten $100 000°° en mobiliario cada una, después de un desastre total, la que tiene seguridad física perderá $20,000°° y la que no la tiene $90,000°° , ahora después de notar esos resultados, me atrevo a decir que la que tiene seguridad física respaldará el 80% de sus ganancias, mientras que la otra sólo el 10%; por consiguiente sugiero que en las áreas de cómputo siempre deban contar con la seguridad física ya que es un gran beneficio para cualquier empresa.

OBJETIVO PRINCIPAL

Conocer las ventajas que se obtienen al efectuar correctamente la auditoría informática en seguridad física dentro de las áreas de cómputo; para evitar los riesgos de inundación, terremoto, fuego y sabotaje en las áreas de cómputo.

OBJETIVOS ESPECÍFICOS

♦ Determinar los procesos a utilizar mediante la auditoría en informática para verificar el control interno de la función del área de cómputo.

♦ Conocer los distintos tipos de daños que se provocan al no efectuar la auditoría informática en seguridad física.

♦ Identificar las ventajas que se obtienen al llevar a cabo la auditoría en informática en seguridad física.

♦ Determinar las características de los seguros existentes para enfrentar los riesgos relacionados con los equipos de cómputo.

♦ Identificar los elementos que deben considerarse para tener una adecuada auditoría en seguridad física en el uso de los equipos y sistemas, así como en su restauración.

♦ Conocer los procedimientos necesarios para mantener la seguridad física de un centro de cómputo.

1. Auditoría

1.1 Concepto de auditoría

Considero que dentro de una actividad tan reciente y expansiva como la llamada auditoría informática, cabe perfectamente la confusión conceptual tanto entre los diferentes aspectos, áreas o enfoques en sí mismos como por las debidas a la apresurada evolución que experimenta la especialidad.

Por otro lado pienso que si bien la auditoría la consideramos como dice el autor Gabriel Buades que según su libro es un "Examen metódico de una situación relativa a un producto, proceso u organización, en materia de calidad, realizado en cooperación con los interesados para verificar la concordancia de la realidad con lo preestablecido y la adecuación al objetivo buscado"[1]

Creo que estoy de acuerdo con que diga que es un examen metódico; pero más que metódico diría que es una evaluación porque eso es lo que hace evaluar una organización, además pienso que si yo hiciera un concepto de auditoría lo diría así: "Es una evaluación de la eficacia y eficiencia que tiene una organización por personal interno o externo para detectar en las diferentes áreas, errores y proponer las correcciones correspondientes".

Además opino que al desmigajar el contenido de la auditoría y su evolución puedo observar que el concepto permanece inalterable y que son su objeto, es decir la parte a auditar y su finalidad lo que puede variar.

Al referirme a auditoría como tal, es preciso entenderla como una actividad consistente en la presentación de una opinión profesional, sobre si el objeto sometido a análisis presenta adecuadamente la realidad que se pretende reflejar y que en sí deba cumplir con las condiciones que le hayan sido señaladas. En todo caso creo que es una función que entra en la relación con actividades ya realizadas, sobre las cuales hay que presentar una opinión.

[1] Concepto de auditoría. BUADES Gabriel, Ingeniería del Software III, Edición 2002.

Por consiguiente es importante saber que la auditoría es indispensable en diversas áreas de auditoría, tales como la financiera, la de gestión, la de cumplimiento y la informática; pero en este caso tomo como referencia la auditoría informática, ya que al efectuarla trae grandes ventajas en cualquier centro computacional, porque la auditoría informática se desempeña mediante la evaluación y revisión específicamente de los sistemas computacionales mediante diversas técnicas eficaces que en su momento permitirán detectar fallas y errores de la información con la que llegué a contar la organización para la correcta toma de decisiones.

Por ello considero que es bueno tomarla como referencia y pensar en todos los beneficios que obtendríamos al hacer uso de la auditoría, de tal modo que se evitarían diversos desastres, ya que su mayor ventaja es que al efectuar la evaluación que se hace en cada auditoría, se consigue en la mayoría de los casos una mejora en el área de cómputo, mediante propuestas alternativas para realizar una corrección del problema en cada situación.

1.2 Concepto de Auditoría Informática

De este modo es bueno tomar la auditoría; pero en este caso la auditoría informática ya que es el tipo de auditoría que elegí para abordar este tema; no obstante pienso que cuando hablo de auditoría tengo una idea de lo que significa, pero si en este caso me refiero a auditoría informática es otro concepto un tanto más diferente, como dice la auditora Gloria Sánchez que según ella " Es el proceso de recoger, agrupar y evaluar evidencias para determinar si un sistema informatizado salvaguarda los activos, mantiene la integridad de los datos, lleva a cabo eficazmente los fines de la organización y utiliza eficientemente los recursos".[2]

Creo que es correcto lo que ella dijo, pero aún así no me convenció mucho su definición, así que a mi parecer opino que se escucharía mejor si digo que la auditoría informática es un examen que se basa del conjunto de las técnicas, actividades y procedimientos para destinarlos a analizar, evaluar, verificar y recomendar en asuntos relativos a la planificación, control eficacia, seguridad y adecuación del servicio informático en la organización, por lo que comprende un

[2] Concepto de Auditoría Informática; editado por la auditora Gloria Sánchez Valriberas en el libro de **PIATTINI** Mario G. y Del Peso Emilio. (2001). **Auditoría Informática. Un enfoque práctico**. (2ª. Ed.). México, Alfaomega, pag. 28.

examen metódico, puntual y discontinuo del servicio informático; de esta forma creo que con este concepto que propongo resalto que el principal objetivo que tiene la auditoría informática es el de mejorar la rentabilidad, la seguridad y la eficacia que se desempeña dentro de una organización.

No obstante es bueno aclarar que la informática que se utiliza en este tipo de auditoría gestiona propiamente la organización, sino que ayuda a la toma de decisiones, desde el momento en que es una herramienta adecuada de colaboración, creo que es por este sentido y debido a su importancia en el funcionamiento de una organización que existe la auditoría informática.

Por otra parte pienso que es importante que la auditoría informática se tenga que llevar a cabo con los sistemas de aplicación, recursos informáticos y en especial con los planes de contingencia; ya que de esta forma la auditoría informática logra su finalidad, la cual considero que es la eficiente operatividad, según normas establecidas de acuerdo a una auditoría interna.

A su vez opino que de acuerdo a los procedimientos o técnicas destacados que se llevan a cabo en una auditoría informática destacan la inspección, observación, averiguación, confirmación, cálculo y análisis; pueden variar ya que cada organización tiene diferentes técnicas; según el auditor Alonso Hernández García, dice que "de estas seis al menos cuatro se ejecutan de forma más eficiente con medios informáticos"[3], los cuales son: inspección, cálculo, análisis y confirmación.

1.3 Auditoría interna

Creo que al hacer referencia de la auditoría interna es un control interno que a mi parecer considero es una ventaja que la auditoría se divida en interna y externa, porque de esta forma me permite especificar claramente el área que se quiere auditar; pero en este caso pienso que más que eso permite tener un control dentro de la organización.

De tal forma que la auditoría realiza el proceso mediante el control interno, ya que es realizado por personal de la organización como una función de asistencia y a su vez de asesoramiento de alto nivel.

[3] Procedimiento de Auditoría. **PIATTINI** Mario G. y Del Peso Emilio. (2001). **Auditoría Informática. Un enfoque práctico**. (2ª. Ed.). México, Alfaomega, pág.12.

De hay que retomo el concepto de Victor Brink el cual dice que la auditoría informática "Es una función independiente de evaluación establecida dentro de una organización para examinar y evaluar sus actividades como un servicio a la misma organización"[4], pienso que este concepto es el ideal ya que maneja los términos idóneos para referirse a la auditoría interna, ya que cuando analice cada palabra me di cuenta que esta definición es cierta porque se lleva a cabo sin restricciones que puedan limitar la examinación.

Además considero que es importante resaltar que es establecida porque de esta forma se confirma el hecho de la realización evidente de la función de auditoría interna por parte de la misma organización.

Por ello señalo que seria malo que cuando una organización establezca una planeación en todos los niveles y proceda a implementarlos en forma de operaciones y no le tenga la vigilancia adecuada, porque daría como resultado simple y sencillamente, unos objetivos establecidos no logrados; ya que estaría fallando principalmente con el trabajo de control, de naturaleza y más que nada con el alcance de los otros controles.

De hay que es importante efectuar una planeación de la auditoría en informática y debe llevarse a cabo alguna metodología para que la auditoría interna o control interno no falle.

2. Planeación de la auditoría en informática

2.1 Metodología para efectuar la auditoría informática.

Según el Diccionario de la Lengua de la Real Academia Española, metodología es "Un conjunto de métodos que se siguen en una investigación científica o en una exposición doctrinal"[5]; pero creo que es más entendible si se define "como una serie de procedimientos que deben ser efectuados en una investigación científica de manera ordenada para alcanzar un resultado homogéneo".

[4] Concepto de auditoría interna.**BRINK** Victor, Witt Herman, **Auditoría Interna Moderna. Evaluación de Operaciones y controles.** Cuarta Edición, ECAFSA, México 1999, Pág. 1.
[5] Concepto de Metodología según el Diccionario de la Lengua de la Real Academia Española.

Considero que es una ventaja muy importante dentro de la auditoría informática en seguridad física ya que si se efectúa una metodología dentro de una organización existe una mayor posibilidad de que los resultados sean óptimos y además se lleven acabo de una manera menos minuciosa porque cada paso que se realice llevara un orden el cual no permitirá la perdida de tiempo en ningún área.

Pienso que la metodología es necesaria para desarrollar cualquier proyecto, pero en este caso en el desarrollo de una buena auditoría informática en seguridad física de manera ordenada y eficaz.

Por otra parte señala el Ing. José María González Zubieta que "Las dos metodologías de evaluación de sistemas por antonomasia son las de Análisis de Riesgos y las de Auditoría Informática"[6]; y creo que es bueno utilizar ambas porque al utilizar la auditoría informática identifica el nivel de exposición por la falta de controles, mientras que la de análisis de riesgos facilita la evaluación de los riesgos y recomienda acciones en base al costo beneficio de las mismas.

No obstante es importante resaltar que las metodologías están dividas en dos grandes familias, las cuales son cuantitativas y las cualitativas; en estas considero que son de gran ventaja utilizarlas, ya que las cuantitativas ayudan a la realización del trabajo mediante un modelo matemático numérico y las cualitativas por su parte se basan en criterio y raciocinio humano las cuales permiten definir adecuadamente el proceso de trabajo que se llegara a necesitar de acuerdo a la experiencia acumulada dentro de la organización; de tal manera que la metodología que se efectúa mediante los siguientes métodos de trabajo para realizar una auditoría informática en seguridad física:

- Conocer el alcance y objetivos de la Auditoría Informática en Seguridad Física.
- Estudiar inicialmente el entorno auditable.
- Determinar los recursos necesarios para realizar la auditoría.
- Elaborar el plan y los programas de trabajo.
- Realizar las actividades propiamente dichas de la auditoría informática en seguridad física.
- Confeccionar y redactar el Informe Final.
- Redactar la Carta de Introducción o Carta de Presentación del Informe Final.

[6] Tipos de metodología de evaluación de sistemas, PIATTINI Mario G. y Del Peso Emilio. (2001). Auditoría Informática. Un enfoque práctico. (2ª. Ed.). México, Alfaomega, pág.44

Creo que esta metodología siempre será el fruto del nivel profesional de cada uno y que con su utilización tendremos una visión clara y precisa de cómo conseguir un mejor resultado en el nivel de control de cada organización, aunque el nivel de control resultante debe ser similar.

2.2 Revisión preliminar y detallada

Considero que es benéfico llevar a cabo una revisión preliminar y detallada dentro de las áreas de cómputo al efectuar una auditoría informática, ya que esta permite tener un control interno y a su vez a optimizar la eficiencia de las contramedidas. De esta forma pienso que es correcto efectuar la revisión preliminar ya que como primer punto a definir sería los objetivos y el alcance de la auditoría, además que con esta revisión previa ayudaría a conocer e identificar a los usuarios afectados por la auditoría.

A mi parecer creo que si la realizamos de una forma ordenada será mejor, para empezar creo que es necesario tener siempre un objetivo ya que este permite determinar que la auditoría produce información exacta y completa en el momento oportuno; de esta forma es importante saber y definir de una manera clara el objetivo ya que este punto es tal vez la más importante en el trabajo de auditorías informativas.

Posteriormente es de gran importancia resaltar que debe de llevar un programa concreto de revisión; pero para empezar es una ventaja identificar el área a revisar, por ejemplo podría decir a partir del calendario de revisiones, ya que de esta manera se permitiría notificar al responsable del área de cómputo y prepararse utilizando papeles de trabajo de auditorías anteriores. Después de esto pienso que debe identificarse las informaciones necesarias para la auditoría y para las pruebas, para obtener informaciones generales; de hay que sería más factible definir los objetivos y el alcance de la auditoría.

Creo que después de conseguir esa información será mucho más fácil obtener un conocimiento detallado de la aplicación de la auditoría informática en seguridad física dentro de áreas de computación ya que se de esta forma se examinaría la documentación de usuarios, de desarrollo y de operación mediante entrevistas con los usuarios y el personal implicado en el área de cómputo a revisar.

No obstante pienso que es otra ventaja tener los resultados de dichas entrevista efectuadas al personal implicado; ya que con ellos sería posible obtener de una forma eficiente la identificación de los puntos de control crítico en el área de cómputo, además que con esos resultados será más fácil ya que se realizaría algún organigrama de flujos de información el cual nos permitirá identificar sin ningún problema los peligros y los riesgos que podrían surgir en cada punto, de tal forma que señale de manera clara que la necesidad de un control es más importante. De hay que creo que sería factible la elaboración del diseño y elaboración de los procedimientos de la auditoría.

Considero que una vez teniendo el diseño, la ejecución de pruebas en los puntos críticos de control se realizará de manera concisa la observación detenida del cumplimiento de los estándares y los procedimientos formales, así como los procedimientos descritos por el organigrama; de esta forma se estaría tomando en cuenta que se verifiquen los controles internos para que cumplan con los estándares, del trabajo de la organización, de los requerimientos legales, de los principios generales y de las prácticas generales de informática.

Pero además pienso que este tipo de ejecución de pruebas se hacen de acuerdo a revisiones subjetivas y pruebas, como resultado de la revisión del cumplimiento de procedimientos.

3. Evaluación de la seguridad

3.1 Seguridad física

De acuerdo a lo que dice el autor Echenique acerca de la seguridad física, dice que "El objetivo es establecer políticas, procedimientos y prácticas para evitar las interrupciones prolongadas del servicio de procedimientos de información, debido a contingencias como incendio, inundación, huelgas, disturbios, sabotaje, terremotos, huracanes, etc., y continuar en un medio de emergencia hasta que sea restaurado el servicio completo"[7]

Estoy de acuerdo con Echenique ya que el objetivo que el plantea creo que bien definido ya que de esa forma se evaluarán las protecciones físicas de instalaciones, equipos y por supuesto habrá que considerar a las personas.

[7] Objetivo establecido para Seguridad Física en el libro de Echenique, García, José Antonio, Auditoría Informática, Segunda Edición, McGrawHill, México, 2001, Pág. 219.

De esta forma la auditoría informática en seguridad física se distingue la preocupación especial por quienes están en el área o de los daños que puedan afectar a los usuarios dentro del área de cómputo.

Pienso que si no se tiene conocimiento de lo antes mencionado entonces podrían surgir algunas amenazas para la seguridad como incendios, inundaciones, disturbios, sabotajes, entre otros, los cuales podrían provocar pérdidas de dinero en las organizaciones.

[8]

Figura 1. Amenazas para la seguridad

3.2 Ubicación y construcción del centro de cómputo

Opinó que la mejor manera de llevar a cabo la seguridad física es iniciando por la ubicación y construcción de la organización ya que se tiene que tener precaución con los materiales altamente inflamables y también con las paredes que no quedan perfectamente selladas y despiden polvo, debido a que de esta forma se podría evitar la pérdida de bienes a causa de incendios ó en todo caso que los equipos se dañen a causa del polvo.

Agrego que es bueno que dentro de un centro de cómputo se verifique la utilización de los pisos tomando en cuenta las políticas de la auditoría informática en seguridad física, ya que una de las ventajas que tiene el buen uso de los "pisos falsos"[9] es que ayudaría a tener un mejor tendido y protección del cableado del sistema; y además nos ayudaría a prever un excelente método para llevar el aire acondicionado cerca de los equipos.

[8] Figura 1. http://www.cfbsoft.com

[9] Se recomienda que el piso sea hecho con plástico antiestático, que tenga una superficie de 45cm de alto y que sean removibles fácilmente.

Pienso que si se emplea esta auditoría en el aire acondicionado manejando los procedimientos indicados por la misma ayudaría a mejorar el control de "la temperatura y la humedad"[10] del centro de cómputo sin afectar a las unidades del sistema.

Es importante también saber que debemos tener bastante cuidado con la instalación eléctrica, porque si no le tomamos importancia puede provocar fallas de energía que puede producir pérdidas de información y a su vez también es una de los principales provocadores de incendios.

Creo que es bueno tener conexiones independientes para los equipos de cómputo, en especial en las oficinas donde hay conectadas terminales, y además pienso que debe contar con tierra física, porque digo que de esta forma se protegerá a los equipos contra un cortocircuito en caso de una descarga.

Además pienso que también es bueno tener una protección contra roedores en los cables de sistema eléctrico y de comunicaciones; porque en la mayoría de ocasiones los roedores se comen el plástico de los cables, por lo que a esto considero que se debe tener cuidado de combatir con esta tipo de fauna nociva, y tener a su vez precaución de que el veneno o fumigante que se use para combatirla no provoque problemas al personal.

3.3 Seguridad contra desastres naturales

Considero que toda área de cómputo siempre está expuesta a múltiples peligros cuya ocurrencia está fuera del control del hombre, como es el caso del frío, el calor, las lluvias, los sismos y el peligro del terreno (como el hundimiento del piso). Por consiguiente pienso que para prevenir los desastres de tipo natural se necesita una buena elección del lugar en el que se va a situar el centro, y una planificación cuidadosa de la distribución y materiales, además de realizar un plan de recuperación. Además creo que es importante consultar a una persona capacitada que asegure que el edificio soportará el peso de las máquinas.

[10] La temperatura ideal recomendada es de 22°C. Echenique García, José Antonio, Auditoría Informática, Segunda edición, Mc Graw Hill, México, 2001, pág. 228

Por otro lado pienso que cuando nos referimos a desastres naturales normalmente creemos que basta con recibir por anticipado los avisos de tormentas, tempestades, tifones y catástrofes sísmicas similares; ya que las condiciones atmosféricas severas se asocian a ciertas partes del mundo y la probabilidad de que ocurran está documentada y eso nos hace creer que nunca sucederán, pero lo cierto es que nadie esta exento de este tipo de desastres.

 [11]

Figura 2. Inundación

No obstante considero que la frecuencia y severidad de su ocurrencia deben ser tomadas en cuenta al decidir la construcción de un edificio. También por otra parte creo que es importante llevar a cabo la comprobación de los informes climatológicos o la existencia de un servicio que notifique la proximidad de una tormenta severa, a su vez tomar precauciones adicionales, tales como la retirada de objetos móviles, la provisión de calor, iluminación o combustible para la emergencia; ya que si lo efectuamos de esta forma obtendremos como ventaja permitirnos estar en un lugar más seguro.

Por otra parte también existe la posibilidad de terremotos; en los cuales creo que estos fenómenos sísmicos pueden ser tan poco intensos que solamente instrumentos muy sensibles los detectan o tan intensos que causan la destrucción de edificios y hasta la pérdida de vidas humanas. Es por tal motivo que pienso que el problema actualmente con respecto a estos fenómenos está ocurriendo en lugares donde no se los asociaba. Por fortuna los daños en las zonas improbables suelen ser ligeros.

[11] Figura 2. http://www.segu.inf.com

Sin embargo opino es por eso que no debemos olvidar que la zona a seleccionar debe contar con los servicios básicos, así como los que se requieren para el funcionamiento del lugar, que se encuentren disponibles y operen eficientemente; algunos factores a considerar tenemos las líneas telefónicas, la energía eléctrica, el drenaje, las facilidades de comunicación y antenas de comunicación. De esta forma se puede lograr de manera eficiente una buena seguridad física.

3.4 Seguridad de autorización de acceso

Considero que el principal elemento de control de acceso físico debe involucrar la identificación positiva del personal que entra o sale del área bajo un estricto control; porque pienso que si una persona no autorizada no tiene acceso, el riesgo se reduce.

Aunque los controles de acceso físico lleguen a variar según las distintas horas del día, opino que es benéfico asegurar que durante la noche sean tan estrictos como durante el día. Por eso opino que los controles durante los descansos y cambios de turno son de especial importancia; por tal motivo creo que es una ventaja que se efectué la evolución de los siguientes elementos es necesaria para diseñar los procedimientos de acceso en una instalación de cómputo: *Estructura y disposición del área de recepción, Acceso de terceras personas e Identificación del personal.*

Estructura y disposición del área de recepción

En esta creo que las áreas de alta seguridad donde se necesita considerar también la posibilidad de ataque físico se debe identificar y admitir tanto a los empleados como a los visitantes de uno en uno. También se pueden utilizar dispositivos magnéticos automáticos y otros recursos en el área de recepción.

Acceso de terceras personas

Dentro de las terceras personas incluyo a los de mantenimiento del aire acondicionado y de computación, los visitantes y el personal de limpieza. Porque pienso que estos y cualquier otro personal ajeno a la instalación deben ser:

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

Ya que considero que el riesgo puede provenir de este personal debido a que en ocasiones su instancia se puede confundir con cualquier otro visitante.

[12]

Figura 3. Intruso

Identificación del personal

Algunos parámetros que a mi parecer se deben asociar a la identificación del personal son:

Algo que se porta:

Este debe consistir en la identificación mediante algún objeto que porta tal como, tarjetas magnéticas, llaves o bolsas. Por ejemplo, las tarjetas pueden incluir un código magnético, estar codificadas de acuerdo al color (por así decirlo, rojo para los programadores, azul para los analistas, etc.), e inclusive llevar la foto del propietario. Sin embargo creo que el problema con esta técnica, sería la posibilidad de que el objeto que se porta sea reproducido por individuos no autorizados. Debido a que en ocasiones uno puede creer que es difícil e imposible, pero lo que es cierto es que para algunos no es imposible reproducir una tarjeta con código magnético. Es por esta razón que esta técnica debe llevarse a cabo en conjunción con otros identificadores para proporcionar una identificación positiva.

[12] Figura 3. http://www.seguridadcorporativa.org

Algo que se sabe:

La autorización considero que puede manejarse individualmente ya de esta forma se obtendrán optimas ventajas de seguridad; ya que se pueden efectuar individualmente para cada puerta, y controlar aspectos como la hora y el día de las funciones. De esta manera, la actividad puede monitorearse, y cualquier intento de entrar que no sea autorizado será detectado de inmediato. Debido a que este tipo de identificación implica el conocimiento de algún dato específico, como el número de empleado, algún número confidencial, contraseña o combinación, etc.

3.5 Detección de humo y fuego, extintores

La protección contra fuego pienso que es lograda de una mejor manera a través de una correcta construcción del edificio (el cual debe procurarse que sea resistente al fuego); sin embargo creo que siempre habrá materiales combustibles y equipo dentro del edificio, así que considero que debe ser necesario asegurar que el equipo contra incendio esté disponible de forma inmediata, para que de esta manera se pueda controlar el fuego con relativa facilidad. No obstante opino que los elementos necesarios que se deben consideran sobresalientes son:

- Las paredes del área del equipo de cómputo deben de ser de material incombustible. Ya que si el área del equipo de cómputo tiene en una o más paredes exteriores adyacentes a un edificio que sea susceptible de incendio, la instalación de ventanas irrompibles tendrá como ventaja una mejor seguridad.
- El techo falso debe de ser de material incombustible o resistente al fuego.
- Todas las canalizaciones y materiales aislantes deben ser de materiales incombustibles y que no desprendan polvo.
- El piso falso instalado sobre el piso real debe ser incombustible.
- Los detectores de fuego y humo se deben colocar cuidadosamente en relación con los aparatos de aire acondicionado, ya que pienso que los conductores de éste pueden difundir el calor o el humo y no permitir que se active el detector.
- Las alarmas contra incendios deben estar conectadas con la alarma central del lugar, o bien directamente al departamento de bomberos.

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

Es por eso que considero que se necesita ubicar los extintores apropiados en lugares de acceso inmediato y es conveniente señalizarlos. De la misma forma, todo aviso o recomendación relativa a la seguridad pienso que debe ser claramente visible; en este caso debe de existir indicadores de prohibición de fumar.

Tipo de material	Tipo de extintor			
	H_2O	CO_2	Espuma	Polvo seco
Seco	E	Luego agua	E	Luego agua
Líquidos	E	E	E	E
Eléctrico	NU	E	NU	E

NU = No usar
E = Excelente

[13]

Figura 4. Tipo de extintores

No obstante creo que también es benéfico definir y documentar los procedimientos que deben seguirse en caso de incendio; además, se debe entrenar al personal acerca de su uso. Debido a que se ha descubierto que ésta es un área débil, sobre todo en instalaciones cuyos índices de cambio de personal son altos y con frecuencia muchos empleados no saben exactamente qué deben hacer en caso de incendio.

[13] Figura 4. http://www.segu.inf.com

3.6 Instalación eléctrica

Considero que la instalación eléctrica en un centro de cómputo es muy importante, ya que todo el funcionamiento del mismo depende de ella, por lo tanto creo que una falla en la instalación puede llegar a provocar serios daños al equipo así como detener completamente la operación del mismo.

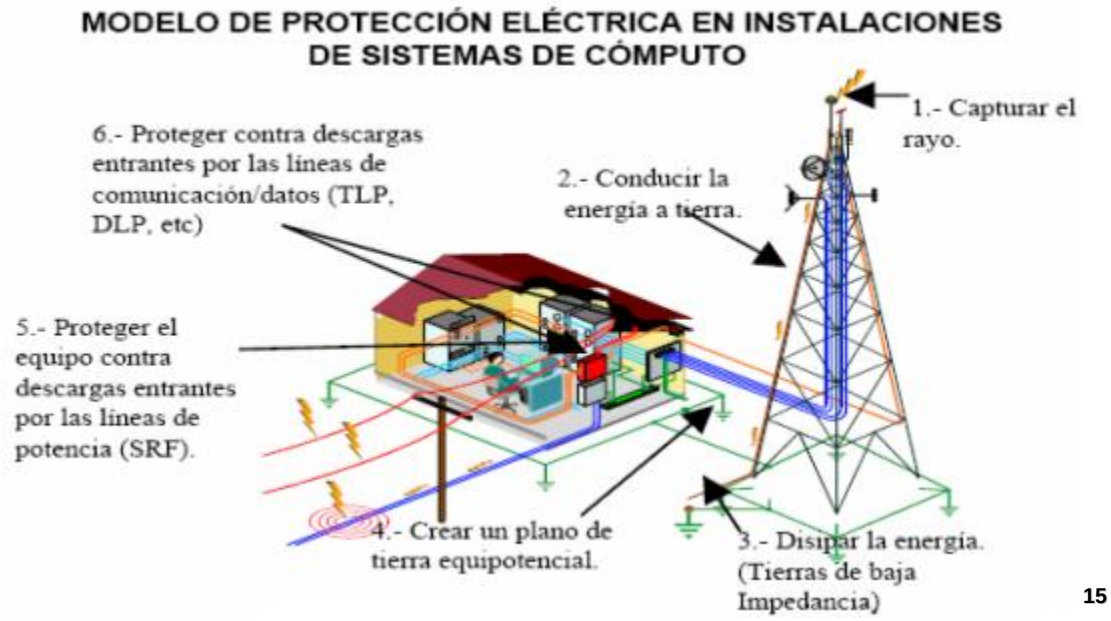
No obstante pienso que es de gran importancia conocer y tener presentes los voltajes de trabajo especificados por los proveedores del equipo de cómputo, del equipo de aire acondicionado y del equipo adicional; ya que de esta forma se reducen los riesgos de tener un accidente. Además para el equipo de cómputo y aire acondicionado se requiere corriente regulada e ininterrumpida.

Por otra parte Echenique dice que "Los reguladores son dispositivos eléctricos que reducen el riesgo de tener un accidente por los cambios de corriente debido a que están construidos dentro de un sistema de corriente ininterrumpido UPS (Uninterruptible Power Supply System)"[14]

Más sin embargo no estoy de acuerdo, porque creo que no todos los reguladores son buenos, porque en algunas ocasiones provocan dos problemas específicamente, tales como: que el regulador no proteja a todos lo equipos, ya que el requerimiento eléctrico sobrepasa sus capacidades, y el otro es que se puede provocar una sobrecarga en los contactos y por consiguiente cabe la posibilidad de un incendio o de una descarga, la cual puede afectar en las instalaciones del área de cómputo.

Digo que también es benéfico tener cuidado al adquirir reguladores que tengan un nivel máximo y un nivel mínimo, porque si no checamos los niveles debido a que en caso de que hubiera una sobrecarga dentro de ciertos límites indicados por el fabricante del equipo, la disminuiría hasta el nivel aceptable con la cual se obtendría un nivel de energía eléctrica adecuada para usar, pero si fuera el caso de que existiera una baja de corriente no la pueden elevar a niveles mínimos aceptable.

[14] Echenique García, José Antonio, Auditoría Informática, Segunda edición, Mc Graw Hill, México, 2001, pág. 222.



[15]

Figura 5. Modelo de protección eléctrica en instalaciones de sistemas de cómputo

Creo que es bueno no pasar por alto este tipo de observaciones, ya que si no se cuenta con un regulador perjudicaría a los equipo el hecho de que hubiera una baja de energía prolongada, que no es detectada y esta provocaría que el equipo continué prendido en un nivel bajo, que una sobrecarga, que hace que automáticamente el equipo se apague.

Por ello señalo que es benéfico saber que una forma de asegurarse de que un regulador actuará en una sobrecarga o en bajos niveles, es contar con un regulador que tenga un sistema no interrumpido "(no-break)"[16], ya que en caso de que exista una variación que los niveles mínimos y máximos, automáticamente entrará el sistema no interrumpido.

[15] Figura 5. http://www.riuady.uady.mx
[16] Sistema que evita que la energía sea interrumpida al momento de ser usada por algún usuario. Echenique García, José Antonio, Auditoría Informática, Segunda edición, Mc Graw Hill, México 2001, pág. 223.

Pienso que un "sistema de energía no interrumpido (UPS)"[17] es una buena opción en este tipo de situaciones, porque este sistema proporciona energía eléctrica a la computadora por un cierto periodo, dependiendo de lo afectado que este llegara a ser, ya que la corriente puede ser de horas o de algunos minutos, de tal forma que se pueda respaldar la información.

No obstante creo que es bueno evaluar las posibilidades de que no se tenga corriente en la zona en que se trabaja, porque de esta forma se puede determinar el tiempo que necesita el sistema no interrumpido. Además considero que también es recomendable evaluar los problemas que puede provocar el no contar con electricidad y las prioridades y necesidades que se tienen; ya en la mayoría de los casos se necesita un determinado periodo para respaldar los archivos de computadoras personales.

Por otra parte considero que es importante saber que tipo de riesgo trae consigo este tipo de problemas de energía; uno de los riesgos que ocasionaría el problema de energía es la posibilidad de incendio, en el cual creo que para evitarlo seria una ventaja tener los cables en compartimientos y canales resistentes al fuego, de manera que los cables estén adecuadamente aislados, fuera de los lugares de paso del personal y que no se encuentren por toda la oficina.

Pienso que el fuego es una de las principales amenazas contra la seguridad, especialmente en las computadoras, ya que considero que puede destruir fácilmente los archivos de información y programas.

Creo que para evitar los incendios se deben considerar diversos factores para reducir los riesgos a los que se encuentra sometido un centro de cómputos como son; que el área en la que se encuentran las computadoras estén en un local que no sea combustible o inflamable; además no debe situarse encima, debajo o adyacente a áreas donde se procesen, fabriquen o almacenen materiales inflamables, explosivos, gases tóxicos o sustancias radioactivas.

Considero que también las paredes deben hacerse de materiales incombustibles y extenderse desde el suelo al techo; pero sin olvidar que debe construirse un piso falso instalado sobre el piso real, con materiales incombustibles y resistentes al fuego.

[17] Generador de batería o de gas, que hace interfase entre la energía eléctrica y el dispositivo de entrada eléctrica a la computadora. Echenique García, José Antonio, Auditoría Informática, Segunda edición, Mc Graw Hill, México 2001, pág. 223.

Por consiguiente pienso que seria una gran ventaja emplear muebles incombustibles, y cestos metálicos para papeles, porque estos evitarían que si en algún momento hubiese un incendio se haga más grande.


[18]

Figura 6. Centro de cómputo

Por otro lado considero que sería benéfico instalar los equipos de cómputo en áreas en las cuales el acceso sea solo para personal autorizado, ya que de esta forma se evitaría algún tipo de terrorismo dentro del área.

Por lo tanto digo que es importante saber que los incendios son causados generalmente por el uso inadecuado de combustibles, fallas de instalación eléctrica defectuosa y también por el inadecuado almacenamiento y traslado de sustancias peligrosas.

Por otra parte existe la invasión de agua por exceso de escurrimiento superficiales o por acumulación en terrenos planos, ocasionada por falta de drenaje ya sea natural o artificial.

Además de las causas naturales de inundaciones, puede existir la posibilidad de una inundación provocada por la necesidad de apagar un incendio en un piso superior.

Pienso que para evitar este inconveniente se pueden tomar algunas medidas como: construir un techo impermeable para evitar el paso de agua desde un nivel superior y acondicionar las puertas para contener el agua que bajase por las escaleras.

[18] Figura 6. http://www.delitosinformaticos.com

Por consiguiente digo que sería benéfica la presencia de un especialista, porque este puede ayudar a evaluar riesgos particulares dentro del área de cómputo debido a que los sistemas se vuelven más complicados y a que se necesita de alguien que tenga el conocimiento necesario para la aplicación de soluciones que estén de acuerdo con las normas de seguridad física.

Sin embargo he analizado que en algunas ocasiones es tan difícil el trabajo de los especialistas, debido a que; tienen que ser cuidadosos con diversos detallitos dentro de las áreas de cómputo y por mencionar algunos, están los picos y ruidos electromagnéticos, ya que las subidas (picos) y caídas de tensión no son el único problema eléctrico al que se han de enfrentar los usuarios.

Por esto digo que es una ventaja que algunos edificios de oficina ya se construyan con los cables instalados, porque de esta forma se evita el tiempo y el gasto posterior, y de esta forma que se minimiza el riesgo de un corte, rozadura u otro daño accidental.

No obstante considero que en la mayoría de las organizaciones, estos problemas entran dentro de la categoría de daños naturales; sin embargo también se pueden ver como un medio para atacar la red si el objetivo es únicamente interferir en su funcionamiento.

Y para esto es benéfico que el cableado de la red que se recomienda para instalar tenga un determinado grado de seguridad militar, ya que esto impedirá la posibilidad de infiltraciones y monitoreos de la información que circula por el cable debido a que este cableado de alto nivel de seguridad consta de un sistema de tubos herméticamente cerrados por cuyo interior circula aire a presión y el cable a lo largo de la tubería hay sensores conectados a una computadora, ya que de esta forma permitirán detectar si hay algún tipo de variación de presión, ya que si la hay, se disparará un sistema de alarma.

3.7 Temperatura y humedad

Para ello considero que la temperatura adecuada debe de ser de 18° C y que el límite de humedad no debe superar el 65%, debido a que algunos equipos grandes de cómputo, o bien las computadoras personales que son usadas en zonas muy cálidas o desérticas, necesitan de un sistema de aire acondicionado para estar en operación constante, con base en los siguientes parámetros:

- Disipación térmica. Esta es mostrada en unidades térmicas británicas por hora.
- Movimiento de aire. Este se muestra en pies cúbicos por minuto.
- Pérdidas por transferencia de calor. En esta creo que se ocasionan por medio de:
  a) pisos, paredes y techos o iluminación.
  b) diferencias en temperatura entre la sala de cómputo y áreas adyacentes.
  c) por medio de aquellas ventanas expuestas a los rayos del sol.

Por consiguiente pienso que sería benéfico que el personal designado para usar extinguidores de fuego deba ser entrenado en su uso, para así evitar algún riesgo para el área de cómputo y del mismo personal; además que se evitaría que el personal interfiriera con este proceso automático.

No obstante creo que es una ventaja el hecho de suministrar información del centro de cómputo, al departamento local de bomberos, antes de que ellos sean llamados en una emergencia, ya que de esta manera se evitaría la pérdida de tiempo y además ellos pueden ofrecernos excelentes consejos como precauciones para prevenir incendios.

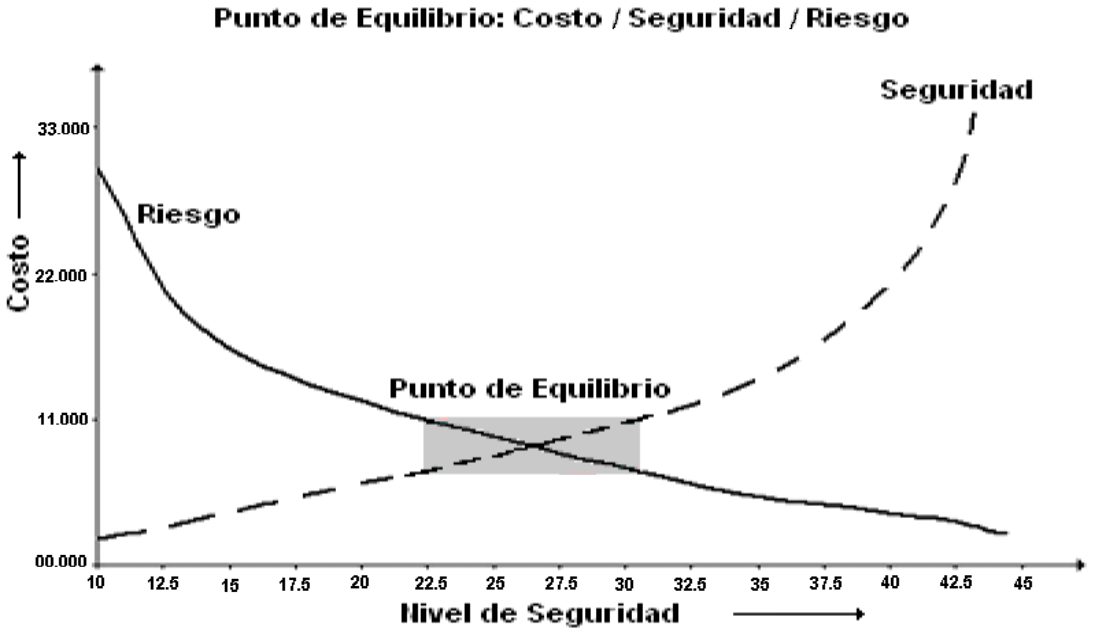
3.8 Costo-Beneficio en seguridad física

Creo que desde un punto de vista oficial, es un desafío responder la pregunta del valor de la información, ya que siempre ha sido difícil, y más difícil aún hacer estos costos justificables; pues a mi parecer es importante saber que si deseo justificarlo, debo darle un valor; en este caso establecer el valor de los bienes y recursos protegidos, el costo de los medios necesarios para romper las medidas de seguridad establecidas y también el costo de las medidas de seguridad dentro del mecanismo de seguridad con que se cuenta en el área de cómputo.

No obstante pienso que si se protegen los bienes serán más caros de lo que valen (el lápiz dentro de la caja fuerte), entonces será una ventaja ya que resultará más conveniente obtenerlos de nuevo en caso de perderlos.

De esta forma creo que se debe tratar de valorar los costos en que se puede incurrir en el peor de los casos contrastando con el costo de la medida de seguridad adoptada.

De tal modo que una vez evaluados los riesgos y los costos en los que se está dispuesto a incurrir decidido el nivel de seguridad a adoptar, podrá obtenerse un punto de equilibrio en tres dimensiones. Las cuales las represento con la siguiente gráfica:



[19]

Figura 7. Punto de Equilibrio

Como puede apreciarse al aumentar la seguridad y los costos en los que incurre tienen como beneficio la disminución de los riesgos, pero como ya se sabe los costos tenderán al infinito teniendo como meta lograr el 100% de seguridad ya que nunca se logrará no correr algún tipo de riesgo. Pero considero que lo importante siempre será lograr conocer cuan seguro se estará conociendo los costos y los riesgos que se corren (punto de equilibrio).

[19] Figura 7. http://www.arcet.gov.ar

4. Plan de contingencia y procedimientos de respaldo para casos de desastre

4.1 Plan de contingencia

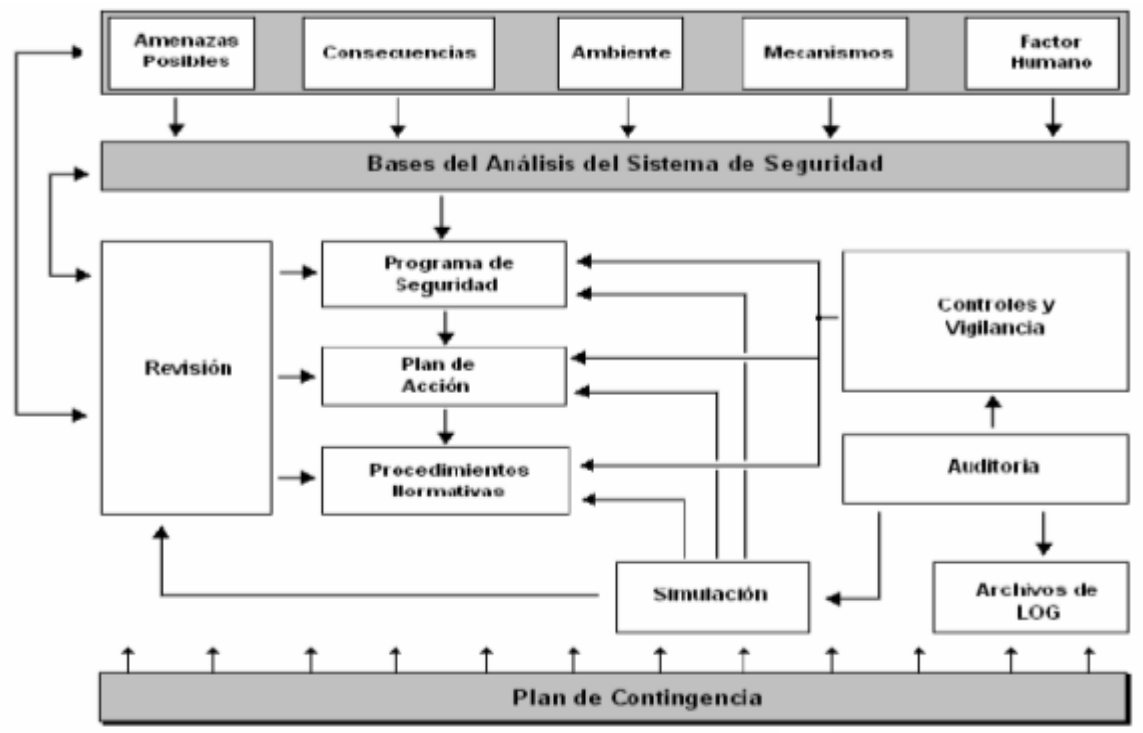
Pienso que es importante hacer uso de un plan de contingencia ya que implica diseñar un futuro deseado e identificar las formas precisas para lograrlo. Creo que su esencia consiste en la identificación sistemática de las oportunidades y peligros que puedan surgir en el futuro, los cuales creo que combinados con otros datos importantes tienen la ventaja de proporcionan la base para lograr que en las áreas de computación se tomen las mejores decisiones en el presente para explorar esas mismas oportunidades y evitar los peligros que posteriormente pueden ocasionar desastres.

Considero que un plan de contingencia es una "presentación para tomar acciones específicas cuando surja un evento o condición que no esté considerado en el proceso de planeación formal". Es decir, se trata de un conjunto de procedimientos de recuperación para casos de desastre ó viéndolo desde otro punto de vista pienso que es plan formal que describe pasos apropiados que se deben seguir en caso de un desastre o emergencia.

Opino que siempre es benéfico tener en cuenta que para efectuar un plan de contingencia dentro de un área de cómputo conocer un amplio estado de acciones consistentes para ser tomadas como son: *antes,* un plan de respaldo; *durante,* un plan de emergencia y *después,* como un plan de recuperación tras un desastre.

De esta forma pienso que es una gran ventaja efectuar un plan de contingencia adecuado porque ayuda a la instalación de cómputo y a la organización en general a minimizar sus pérdidas en caso de desastre, y reanudar las operaciones normales de una manera rápida, eficiente y oportuna.

Una proposición de una forma de realizar un plan de contingencia adecuada puede apreciarse en el siguiente diagrama:



[20]

Figura 8. Manual de seguridad

Con este diagrama trato de explicar que se debe de comenzar realizando una evaluación del factor humano, el medio en donde se desempeña, los mecanismos con los cuales se cuenta para llevar a cabo la tarea encomendada, las amenazas posibles y sus posibles consecuencias.

Luego de evaluar estos elementos y establecida la base del análisis, pienso que se origina un programa de seguridad, el plan de acción y las normas y procedimientos a llevar a cabo.

No obstante creo que para que tolo lo anterior llegue a buen fin debe realizarse un control periódico de estas políticas, que asegure el fiel cumplimiento de todos los procedimientos enumerados. Para asegurar un marco efectivo se realiza una auditoría a los Archivos de Logs (archivos de registro de actividades) de estos controles.

[20] Figura 8. http://www.arcert.gov.ar

Además pienso que todo esto se debe realizar con el objeto de confirmar que todo lo creado funciona en un marco real, se realiza una simulación de eventos y acontecimientos que atenten contra la seguridad del sistema. De esta forma opino que esta simulación y los casos reales registrados generan una realimentación y revisión que permiten adecuar las políticas generadas en primera instancia.

Por consiguiente considero que el plan de contingencia es el encargado de suministrar el respaldo necesario en caso de que la política falle.

Por otro lado creo que para realizar un plan de contingencia es importante tener una noción de lo que es un desastre; pienso que el término desastre significa la interrupción en la capacidad de acceso a la información y el procesamiento de la misma a través de las computadoras, necesarias para la operación normal de cualquier organización.

Según el auditor Gabriel Desmonts Basilio dice que "el plan de contingencia debe iniciar con un acuerdo de empresa para el plan de contingencia, después continuar con un acuerdo de un proceso alternativo y efectuar el manual del plan de contingencia".[21]

De acuerdo a lo que señaló el auditor Gabriel, estoy de acuerdo con el ya que el plan de contingencia constituye en cierta forma un control netamente preventivo, ya que se configura como un instrumento que permite prevenir la eventualidad de un desastre, así como mantener el nivel de operación del ambiente informático; esto forma un control correctivo en la cual se materializa un riesgo, debido a que se pretende reducir el impacto de éste.

Es por eso que creo que sería recomendable establecer un modelo a seguir, tomando como sugerencia aquellas organizaciones que se han preocupado por su desarrollo y crecimiento, porque pienso que han establecido dentro de la estructura orgánica de algunas organizaciones una función definida para la administración de riesgos y que han obteniendo estupendos resultados, como una disminución considerable del impacto físico y económico de los riesgos dentro de la misma organización.

[21] Adquisición de información según el auditor Gabriel Desmonsts Basilio en el libro de **PIATTINI** Mario G. y Del Peso Emilio. (2001). **Auditoría Informática. Un enfoque práctico**. (2ª. Ed.). México, Alfaomega, pp.192-195.

Sin embargo a pesar de que este tipo de plan implica invertir tiempo, dinero y esfuerzo, y su verdadero valor sólo se podrá medir en el caso en que se presente alguna contingencia; pienso que tiene como principal ventaja la protección de la seguridad física ante cualquier amenaza de desastre.

4.2 Selección de la estrategia

De acuerdo a las necesidades de la organización, pienso que es bueno que se recomiende manejarlo conforme a los procedimientos siguientes, ya que de esta forma se seleccionará la estrategia adecuada:

- Objetivo
- Características
- Consideraciones
- Aspectos Base
- Elementos del plan de contingencia

Dentro de lo que seria el objetivo considero que al definirlo su propósito principal de un plan de contingencia sería "mantener a la compañía y sus actividades operando aún en una situación de desastre", es decir, habilitar a la organización para responder y sobrevivir a problemas críticos o catastróficos, de forma que permita una pronta recuperación de la operación normal del centro de cómputo.

Este plan creo que dependerá de la naturaleza de la organización, ya que inevitablemente incurrirá en costos altos. Sin embargo pienso que es importante tener en mente que su importancia no depende de la probabilidad de un desastre, sino del efecto que éste pueda tener; ya que se debe considerar que la pérdida parcial o total de las facilidades del procesamiento de datos puede causar entre otras cosas: Pérdidas financieras directas, pérdidas de la producción, pérdidas financieras indirectas, pérdidas de clientes, costos extras para apoyo, costos de compensación, pérdidas de control, información errónea o incompleta e incluso bases pobres para la toma de decisiones.

Por otra parte es importante tomar como características; que en una organización, el plan de contingencia debe contemplar dos aspectos: operacional y administrativo.

Porque en el nivel operacional, cada usuario debe saber qué hacer cuando aparezca el problema; asimismo debe saber la respuesta a la pregunta ¿a quién hay que llamar?, porque pienso que es elemental que el plan de contingencia determine quién debe tomar las decisiones durante la recuperación del desastre y establezca la disponibilidad y entrenamiento del personal debidamente experimentado.

No obstante agrego que en el nivel administrativo, el plan deba contemplar aspectos como: Definición de riesgos y porcentajes de factibilidad a que está expuesta la organización, identificación de las aplicaciones críticas para las áreas de computación, procedimiento de recuperación para la reproducción de información, la configuración del equipo de cómputo similar y su localización, localización del software de reemplazo, localización de equipos de apoyo como generadores y aire acondicionado, la ayuda que se puede esperar del proveedor del equipo y por último la acción a ser tomada en cada daño parcial inesperado.

Por otro lado creo que las consideraciones que se deben tomar en el plan de contingencia que se efectúa en la auditoría de seguridad física, son: designar al grupo encargado de elaborar el plan de contingencia; tomar en cuenta los factores externos que puedan afectar la operación de la organización al elaborar el plan de contingencia.

Además creo que los aspectos base de un plan de contingencia pueden dirigirse sobre algunas de las siguientes áreas:

Facilidad de destrucción, en este el equipo de planeación debe considerar incluir revisiones que podrían ser necesarias en caso de que las instalaciones primarias fueran sólo parcialmente destruidas.

Disponibilidad de personal, en este creo que es bueno tomar como base un organigrama para el plan de contingencia en caso de desastre, porque debe ser un subgrupo que incluya personal de toda la organización, con las posiciones clave identificadas como necesarias para ejecutar el plan.

Determinar los tiempos del desastre; pienso que deben ser fijados para los diversos momentos en que un desastre puede ocurrir, porque si se toma en cuenta esta determinación de tiempos se pude llegar a identificar los tiempos en que podrá haber los más devastadores efectos sobre la organización; ya que algunas organizaciones dependen totalmente del procesamiento nocturno, mientras que otras pueden creer que la falta de disponibilidad de sistemas en la línea durante las horas pico de utilización, pueden ser el más devastador periodo de tiempo.

Instalaciones de almacenamiento fuera del Centro de Cómputo, en este pienso que en muchas organizaciones suponen que estas instalaciones sobrevivirán al desastre; esto puede ser un falso supuesto si la instalación esta cerca al desastre.

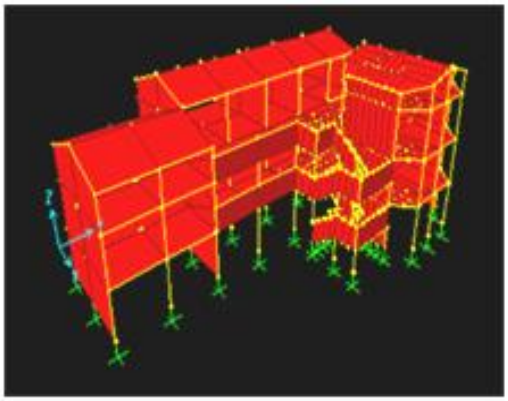
 [22]

Figura 9. Análisis de la vulnerabilidad estructural de un centro de cómputo

Ciertamente, los medios magnéticos protegidos, el aprovisionamiento crítico y otros registros proveerán los medios para recuperar la normalidad de operación; otros aspectos que el equipo de planeación que a mi criterio se deben de considerar incluyen: Desastres que afecten únicamente a departamentos usuarios específicos y Trabajos sin procesar y trabajos en proceso; ya que me atrevo a agregar que para realizar una buena selección de estrategia para el plan de contingencia debe considerar como un documento con vida, es decir, debe ser dinámico, por lo que también creo que se deberá estar modificando cada vez que cambien algunos de los siguientes factores: Cambio de personal, cambio de equipo de instalación, cambio de sistemas, cambio de contratos de mantenimientos, cambio en las pólizas de seguros, ruptura de privacía en el plan de contingencia y recuperación.

[22] Figura 9. http://segu.inf.com

Por otra parte creo los principales Elementos del Plan de Contingencia son tres y según mi criterio son: *Acciones de emergencia*; en el cual considero que se debe contener el daño en el momento, así como limitarlo tanto como sea posible, contemplando todos los desastres naturales y eventos no considerados. *Acciones de recuperación*, en este elemento considero que se deben abarcar el mantenimiento de partes críticas entre la pérdida del servicio y los recursos, así como su recuperación o restauración. *Acciones de respaldo*, en este pienso que son el conjunto de acciones a realizar una vez que se ha presentado cualquier contingencia que afecte la continuidad operativa, ya sea en forma parcial o total, a las instalaciones auxiliares, recursos, con la finalidad de estar preparados para hacer frente a cualquier contingencia. Ya que si se realiza así se reducirá su impacto, permitiendo restablecer a la brevedad posible los diferentes servicios interrumpidos.

5. Ventajas de la Auditoría Informática en Seguridad Física

a) Permite reducir riesgos, entre algunos de ellos son: inundación, terremoto, fuego y sabotaje en las áreas de cómputo.

b) Da a conocer el estado actual y futuro posible de seguridad informática.

c) Se tendrá controlado el ambiente y acceso físico obteniendo como resultado la disminución de siniestros.

d) Da resguardo específicamente al hardware y al personal que labora dentro del área de cómputo.

e) Evalúa la eficacia y eficiencia que tiene una organización por personal interno o externo para detectar de las diferentes áreas errores y proponer las correcciones correspondientes.

f) Permite detectar fallas y errores de la información con la que llegué a contar la organización para la correcta toma de decisiones.

g) Consigue en la mayoría de los casos una mejora en el área de cómputo, mediante propuestas alternativas.

h) Accede a la especificación clara del área que se quiere auditar.

i) Se consigue tener un mejor control dentro del área de cómputo.

j) Al efectuarla tomando una metodología dentro de una organización existe una mayor posibilidad de que los resultados sean óptimos y además se lleven acabo de una manera menos minuciosa porque cada paso que se realice llevara un orden el cual no permitirá la perdida de tiempo en ningún área.

k) Al llevarla a cabo mediante la utilización de su metodología que está divida en dos grandes familias, las cuales son cuantitativas y las cualitativas; nos permitirá conocer el alcance y los objetivos de la Auditoría Informática en Seguridad Física.

l) Al utilizarla se identifica fácilmente el área a revisar, por ejemplo podría decir a partir del calendario de revisiones, ya que de esta manera se permitiría notificar al responsable del área de cómputo y prepararse utilizando papeles de trabajo de auditorías anteriores.

m) Al efectuar entrevistas al personal implicado mediante la auditoría en seguridad física se hace posible obtener de una forma eficiente la identificación de los puntos de control crítico en el área de cómputo.

n) A través de una buena utilización de los procedimientos de seguridad física que se aplican en con la auditoría informática, se consigue una mejor protección del hardware, además de el acceso al área de cómputo.

o) Permite estar en un lugar más seguro, ya que se estudia desde su nivel climático, el lugar, las personas que trabajan dentro y los riesgos que ocurren frecuentemente dentro de un área de computo, como son: que los pisos sean seguros, la electricidad este bien colocada e incluso el drenaje que no afecte esta área.

p) Al ejecutar la auditoría informática en seguridad física se le indica hacer uso de muebles incombustibles, y cestos metálicos para papeles, debido a que estos ayudarían en algún momento si hubiese un incendio a que no se haga más grande.

q) Suministra información del centro de cómputo, al departamento local de bomberos, antes de que ellos sean llamados en una emergencia, ya que de esta manera se evitaría la pérdida de tiempo y además ellos pueden ofrecernos excelentes consejos como precauciones para prevenir incendios.

r) Si se protegen los bienes serán más caros de lo que valen (el lápiz dentro de la caja fuerte), entonces resultará más conveniente obtenerlos de nuevo en caso de perderlos, ya que estarán asegurados.

s) Proporciona la base para lograr que en las áreas de cómputo se tomen las mejores decisiones en el presente para explorar esas mismas oportunidades y evitar los peligros que posteriormente pueden ocasionar desastres.

t) Al desarrollar un plan de contingencia adecuado ayuda a la instalación de cómputo y a la organización en general a minimizar sus pérdidas en caso de desastre, y reanudar las operaciones normales de una manera rápida, eficiente y oportuna.

CONCLUSIONES

Considero que siempre será indispensable evaluar y controlar permanentemente la seguridad física de las áreas de cómputo mediante la utilización de la auditoría informática, ya que permanentemente la seguridad física de las áreas de cómputo es la base para comenzar a integrar la seguridad como una función primordial dentro de cualquier organismo.

No obstante pienso que a su vez es importante controlar el ambiente y acceso físico debido a que de esta forma se logra disminuir siniestros, trabajar mejor manteniendo la sensación de seguridad, descartar falsas hipótesis si se produjeran incidentes e incluso tener los medios para luchar contra accidentes.

Por otra parte creo que las distintas alternativas estudiadas son suficientes para conocer en todo momento el estado del medio en el que nos desempeñamos; y así tomar decisiones sobre la base de la información brindada por los medios de control adecuados, en este caso la realización de la auditoría informática.

Por consiguiente digo que aunque estas decisiones puedan variar desde el conocimiento de las áreas que recorren ciertas personas hasta la extremo de evacuar el edificio en caso de accidentes; siempre tomaran un punto de partida, el cual a mi parecer debería ser la realización de la auditoría informática en seguridad física ya que creo que su primordial ventaja será obtener resultados positivos y efectivos en la protección de las áreas de cómputo.

Además agrego que con este ensayo me he probado que: La Auditoría Informática en Seguridad Física requiere un nivel de perfección que realmente no existe, y de hecho dudo que algún día exista, pero los riesgos deben y pueden ser manejables.

BIBLIOGRAFÍA:

-**ECHENIQUE** García, José Antonio, **Auditoría Informática**, Segunda edición, Mc Graw Hill, México, 2001.

-**PIATTINI** Mario G. y Del Peso Emilio. (2001). **Auditoría Informática. Un enfoque práctico**. (2ª. Ed.), Alfaomega, México, 1998.

-**HERNÁNDEZ** Hernández Enrique, **Auditoría en Informática**, Segunda edición, CECSA, México, 2000.

-OLGUIN, Romo Heriberto. **Organización y Administración de Centros de Cómputo.** Universidad Nacional Autónoma de México, Facultad de Ingeniería. División de Ingeniería Eléctrica. Departamento de Ingeniería en Computación. Primera Edición. México D. F., 1997.

-SUAREZ, Domínguez Federico. **Seguridad en centros de cómputo.** Universidad Juárez de Tabasco, unidad Chontalpa, división de ciencias básicas. Ed. S. I., México D. F., 1991.

-FINE, Leonard H. **Seguridad en los centros de cómputo: Políticas y Procedimientos.** Ed. Trillas, México D.F., 1988.

-BRINK Victor, Witt Herman, **Auditoría Interna Moderna. Evaluación de Operaciones y controles.** Cuarta Edición, ECAFSA, México, 1999.

REFERENCIAS DE PÁGINAS WEB:

http://www.seguridadcorporativa.org consultada el día 5/03/07

http://www.cfsoft.com.ar consultada el día 12/03/07

http://www.arcert.gov.ar consultada el día 12/03/07

http://www.segu.inf.com. consultada el día 24/04/07

http://www.delitosinformaticos.com consultada el día 21/06/07

http://www.riudy.uady.mx consultada el día 12/07/07

http://dmi.uib.es/~bbuades/auditoría/auditoría.PPT consultada el día 9/08/07

http://seguridad.internet2.ulsa.mxconsultada el día 2/09/07