Universidad del Azuay

Facultad de Ciencias de la Administración

Escuela de Ingeniería de Sistemas

Auditoria Informática

Ensayo previa la obtención del Titulo de Ingeniero de Sistemas

Autores:

María Fernanda Marín Serrano

José Fernando Zea Montero

Tutor: Ing. Jorge Espinosa I.

Cuenca – Ecuador

2006

Las ideas y opiniones vertidas en el presente ensayo son de exclusiva responsabilidad de sus autores.

María Fernanda Marín Serrano

José Fernando Zea Montero

Dedicatoria

El presente proyecto es dedicado para todas aquellas personas, que siempre me apoyaron, alentaron, ayudaron a levantarme cuando me sentí derrotada, y que con su cariño me enseñaron a crecer como persona y nunca me dejaron desfallecer.

Mi Familia

mafer

A mis padres, mis hermanos que siempre estuvieron apoyándome incondicionalmente en toda mi vida universitaria. A mi esposa Diani y a mi bebe Dani que son mi razón de vivir, y mi inspiración para la obtención de este titulo.

Fher

Agradecimiento

Gracias a Dios por permitirme cumplir un sueño, a mis Padres por creer en mi y apoyarme, a mis hermanos y cuñada por no dejarme perder mi fe, a mis sobrinos por la alegría de su existir, a toda mi familia por su apoyo constante, a mis verdaderos amigos por siempre estar conmigo en todo momento, gracias por todo a mi gran amigo Hernán, a los profesores de la Universidad del Azuay y en especial al Ing. Jorge Espinosa, por ayudarnos a cumplir una meta y convertirse en amigos y a ti por ser una persona incondicional en mi vida.

mafer

Quiero agradecer a mis padres por a ver sido ellos quienes me brindaron esta oportunidad de ser un profesional. A mis abuelos, en especial a mi abuelita quien siempre estuvo pendiente de mis estudios; fueron siempre un pilar importante para este logro personal.

Fher

Índice de Contenidos

Capitulo VI

Control de Acceso Físico **Pág.**

Capitulo V

Aire Acondicionado **Pág.**

Capitulo VI

Instalación Eléctrica **Pág.**

Capitulo VII

Plan de Contingencia **Pág.**

Capitulo VIII

Aplicación Práctica- Aplicación de normas de Auditoria **Pág.**

Índice de Anexos **Pág.**

Introducción

El presente proyecto permitirá definir los criterios de Auditoría de Sistemas a ser aplicados dentro de un Centro de Cómputo en la parte correspondiente a la Seguridad Física, permitiendo de esta manera conocer una serie de aspectos a verificar dentro del mismo.

Pero es importante el indicar, que la utilización de estas normas se las realizarán tomando en cuenta las particularidades y las características del Centro de Cómputo, el valor de la información y la finalidad de la misma.

Para complementar el desarrollo de este proyecto se ha visto necesario el realizar la aplicación práctica correspondiente, para lo cual contamos con la colaboración del Centro de Computo de la Universidad del Azuay, con el fin de evaluar su funcionamiento y detectar posibles deficiencias, así como proponer los aspectos principales que se tiene que mejorar a fin de incrementar su eficiencia o mejorar su funcionalidad y su productividad.

Resumen

El presente proyecto es la recopilación y aplicación de conceptos , normas y procedimientos de una rama de la Auditoría Informática como es la Seguridad Física, que es de suma importancia en los centros de Cómputo instalados o a instalar.

Para lo cual se realiza la elección de normas a ser consideradas para la ubicación del procesador, materiales utilizados para su construcción, equipos detectores y protección contra incendios, sistema de aire acondicionado, instalación eléctrica, sistema de control de acceso, entrenamiento del personal en caso de emergencia y desarrollo del plan de contingencia.

Abstract

The present Project is a summary and aplication of concepts, norms and procedures of one branch of the Informatic Audition such as the physical Security, which is the vital information in computing centers installed and to install.

In order to do the election of the norms to be considered for the placement of the proccesor, materials to be used, smoke detecting systems, air conditioning, electric instalation, acces control system, personnel training and emergency plans

CAPITULO I

Introducción General

1.1 Conceptos de Auditoria

Actividad para determinar, por medio de la investigación, la adecuación de los procedimientos establecidos, instrucciones, especificaciones, codificaciones y estándares u otros requisitos y la eficiencia de su implantación [1].

Esta se encarga de llevar a cabo la evaluación de normas, controles, técnicas y procedimientos que se tienen establecidos en una empresa para lograr confiabilidad, oportunidad, seguridad y confidencialidad de la información que se procesa a través de los sistemas de información. La Auditoría de sistemas es una rama especializada de la Auditoría que promueve y aplica conceptos de Auditoría en el área de sistemas de información teniendo en cuenta que se deben mejorar ciertos aspectos tales como [1]:

- Rentabilidad
- Seguridad
- Eficacia

1

La Auditoría en informática es la revisión y la evaluación de los controles, sistemas, procedimientos de informática; de los equipos de cómputo, su utilización, eficiencia y seguridad, de la organización que participan en el procesamiento de la información.

Esta deberá comprender no sólo la evaluación de los equipos de cómputo, de un sistema o procedimiento específico, sino que además habrá de evaluar los sistemas de información en general desde sus entradas, procedimientos, controles, archivos, seguridad y obtención de información.

[1] www.geocities.com/Athens/9105/audit/audi_2.html

La Auditoría en informática es de vital importancia para el buen desempeño de los sistemas de información, ya que proporciona los controles necesarios para que los sistemas sean confiables y con un buen nivel de seguridad. Además debe evaluar todo (informática, organización de centros de información, hardware y software).

1.2 Objetivos de la Auditoría

- Asegurar una mayor integridad, confidencialidad y confiabilidad de la información mediante la recomendación de seguridades y controles.
- Seguridad del personal, los datos, el software, el hardware y las instalaciones.
- Reducir la existencias de riesgos en el uso de Tecnología de información
- Conocer la situación actual del área informática para lograr los objetivos.
- Seguridad, utilidad, confianza, privacidad y disponibilidad en el ambiente informático.
- Incrementar la satisfacción de los usuarios de los sistemas informáticos.
- Capacitación y educación sobre controles en los Sistemas de Información.

- Dictaminar sobre su confiabilidad, efectividad y eficiencia, y presentar informes de Auditoría con sus conclusiones y recomendaciones dirigidas a la alta dirección, la gerencia de sistemas y los gerentes de las áreas de negocios.
- Asesorar al Departamento de Sistemas en asuntos relacionados con definición, diseño e implementación de controles y seguridades en sistemas de información y tecnología relacionada. [2]

[2] www.auditoriasistemas.com/auditoria_de_sistemas.htm

1.3 Tipos de Auditoría Informática

En Sistemas se desarrollan diferentes actividades y de acuerdo a estas se han establecido las principales divisiones de la Auditoría Informática las cuales son[3]:

- **Auditoría Informática de Producción o explotación** esta se ocupa de revisar lo referido con producir resultados informáticos, listados, impresos, ficheros soportados magnéticamente, ordenes automatizadas para lanzar o modificar procesos, etc.

  La operación, producción dispone de materia prima, que son los datos, que es necesario transformar, los que se someten a controles de calidad e integridad. Esta transformación se lo hace por medio de un proceso informático, para obtener el producto final, de igual manera los resultados son sometidos a varios controles de calidad y finalmente entregados a sus usuarios.

  Auditar la producción, operación o explotación consisten revisar las secciones que las compone y sus interrelaciones, las cuales son: planificación, producción y soporte técnico.
- **Auditoría informática de Desarrollo de proyectos** es una evolución del análisis y programación de sistemas, abarcando muchas áreas, como: prerrequisitos del usuario y del entorno, análisis funcional, diseño, análisis orgánico (preprogamación y programación) pruebas de entrega a explotación o producción y alta para el proceso.

  Dentro de esta fase se somete a un exigente control interno, caso contrario los costos se pueden exceder y producir insatisfacción por parte del usuario.

  Esta Auditoría deberá principalmente comprobar la seguridad de programas garantizando que lo ejecutado por la máquina sea lo solicitado por el usuario.
- **Auditoría Informática de sistemas** esta analiza y revisa los controles y efectividad de la actividad conocida como técnicas de sistemas en todos sus ámbitos y enfocada principalmente en el entorno general de sistemas, el cual incluye sistemas operativos, software básicos, aplicaciones, administración de base de datos, etc.

[3] www.gerencie.com/auditoriasistemas.htm

- **Auditoría informática de Comunicaciones y Redes** se encuentra enfocado directamente con las redes, líneas, concentradores, multiplexores, etc. Para poder realizar este tipo de Auditoría es necesario el contar con expertos en comunicación y redes.

  El auditor deberá solicitar información sobre tiempos de desuso, necesitará la topología de la red de comunicaciones actualizadas, es importante el contar con el información sobre la cantidad de líneas existentes, cómo son y donde están instaladas.
- **Auditoría de la Seguridad informática** esta abarca los conceptos de seguridad física y lógica. La seguridad física está referida a la protección del hardware y los soportes de datos, de igual manera con la seguridad de los edificios e instalaciones dentro de estos, se debe contemplar situaciones dentro de esta como son incendios, sabotajes, robos, catástrofes naturales, etc.

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

  Cuando se audita la seguridad de los sistemas, también se debe tener en cuenta que no existan copias piratas y que la conexión con otras redes no exista la transmisión de virus.
- **Auditoría informática para Aplicaciones en Internet** esta se basa en tomar en cuenta los siguientes puntos que no deben ser olvidados por un Auditor informático.
  - Evaluar las vulnerabilidades y la arquitectura de seguridad implementada
  - Evaluación de riesgos de Internet (operativos, tecnológicos y financieros) y así como su probabilidad de ocurrencia.
  - Verificar la confidencialidad de las aplicaciones y la publicidad negativa como consecuencia de ataques exitosos por parte de hackers

1.4 Justificativos para efectuar una Auditoría

Las razones por las cuales se debe llevar a cabo una Auditoría se consideran las siguientes entre las más importantes[4]:

- Aumento considerable e injustificado del presupuesto del Departamento de Sistemas.
- Desconocimiento en el nivel directivo de la situación informática de la empresa.
- Falta total o parcial de seguridades lógicas o físicas que garanticen la integridad del personal, equipos e información.
- Descubrimiento de fraudes.
- Falta de planificación informática.
- Falta de políticas, normas, reglas, asignación de tareas y adecuada administración del Recurso Humano.
- Descontento por parte de los usuarios por incumplimiento de plazos y mala calidad de resultados.
- Falta de documentación o documentación incompleta que revela la dificultad de evaluar el mantenimiento de los sistemas.

1.5 Normas de Auditoría Informática

Normas Generales para la Auditoría de los Sistemas de Información

Emitidas por el Consejo Normativo de la Asociación de Auditoría y Control de Sistemas de Información

[4] www.auditoriasistemas.com/auditoria_de_sistemas.htm

Introducción

La Asociación de Auditoría y Control de Sistemas de Información ha determinado que la naturaleza especializada de la Auditoría de los sistemas de información y las habilidades necesarias para llevar a cabo este tipo de Auditorías, requieren el desarrollo y la promulgación de Normas Generales para la Auditoría de los Sistemas de Información.

Objetivos

Los objetivos de estas normas son los de informar a los auditores del nivel mínimo de rendimiento aceptable para satisfacer las responsabilidades profesionales establecidas en el Código de Ética Profesional y de informar a la gerencia y a otras partes interesadas de las expectativas de la profesión con respecto al trabajo de aquellos que la ejercen.

Normas Generales para los Sistemas de Auditoría de la Información

1 Título de Auditoría

- **1.1 Responsabilidad, autoridad y rendimiento de cuentas** La responsabilidad, la autoridad y el rendimiento de cuentas abarcados por la función de Auditoría de los sistemas de información se documentarán de la manera apropiada en un título de Auditoría o carta de contratación.

2 Independencia

- **2.1 Independencia profesional** En todas las cuestiones relacionadas con la Auditoría, el auditor de sistemas de información deberá ser independiente de la organización auditada tanto en actitud como en apariencia.
- **2.2 Relación organizativa** La función de Auditoría de los sistemas de información deberá ser lo suficientemente

independiente del área que se está auditando para permitir completar de manera objetiva la Auditoría.

3 Ética y normas profesionales

- **3.1 Código de Ética Profesional** El auditor de sistemas de información deberá acatar el Código de Ética Profesional de la Asociación de Auditoría y Control de Sistemas de Información.
- **3.2 Atención profesional correspondiente** En todos los aspectos del trabajo del auditor de sistemas de información, se deberá ejercer la atención profesional correspondiente y el cumplimiento de las normas aplicables de Auditoría profesional.

4 Idoneidad

- **4.1 Habilidades y conocimientos** El auditor de sistemas de información debe ser técnicamente idóneo, y tener las habilidades y los conocimientos necesarios para realizar el trabajo como auditor.
- **4.2 Educación profesional continua** El auditor de sistemas de información deberá mantener la idoneidad técnica por medio de la educación profesional continua correspondiente.

5 Planificación

- **5.1 Planificación de la Auditoría** El auditor de sistemas de información deberá planificar el trabajo de Auditoría de los sistemas de información para satisfacer los objetivos de la Auditoría y para cumplir con las normas aplicables de Auditoría profesional.

6 Ejecución del trabajo de Auditoría

- **6.1 Supervisión** El personal de Auditoría de los sistemas de información debe recibir la supervisión apropiada para proporcionar la garantía de que se cumpla con los objetivos de la Auditoría y que se satisfagan las normas aplicables de Auditoría profesional.

- **6.2 Evidencia** Durante el transcurso de una Auditoría, el auditor de sistemas de información deberá obtener evidencia suficiente, confiable, relevante y útil para lograr de manera eficaz los objetivos de la Auditoría. Los hallazgos y conclusiones de la Auditoría se deberán apoyar por medio de un análisis e interpretación apropiados de dicha evidencia.

7 Informes

- **7.1 Contenido y formato de los informes** En el momento de completar el trabajo de Auditoría, el auditor de sistemas de información deberá proporcionar un informe, de formato apropiado, a los destinatarios en cuestión. El informe de Auditoría deberá enunciar el alcance, los objetivos, el período de cobertura y la naturaleza y amplitud del trabajo de Auditoría realizado. El informe deberá identificar la organización, los destinatarios en cuestión y cualquier restricción con respecto a su circulación. El informe deberá enunciar los hallazgos, las conclusiones y las recomendaciones, y cualquier reserva o consideración que tuviera el auditor con respecto a la Auditoría.

8 Actividades de seguimiento

- **8.1 Seguimiento** El auditor de sistemas de información deberá solicitar y evaluar la información apropiada con respecto a hallazgos, conclusiones y recomendaciones relevantes anteriores para determinar si se han implementado las acciones apropiadas de manera oportuna.

Fecha de vigencia: 25 de julio de 1997

CAPITULO II

Elementos de Seguridad

2.1 Políticas definidas sobre Seguridad

Por medio de una política de seguridad se puede comunicar con los usuarios, ya que estas establecen un medio de comunicación con el personal relacionando los recursos y servicios informáticos de la empresa [5].

Por medio de las políticas se pueden definir que es lo que deseamos proteger y como lo efectuaremos, ya que el contar con una política de seguridad involucra al personal y de esta manera permite el que cada uno de ellos reconozca que tan importante son los bienes que posee dicha empresa. Por tal razón, las políticas de seguridad deben concluir en una posición consciente y vigilante del personal por el uso y limitaciones de los recursos y servicios informáticos.

Es necesario que dentro de las Políticas de Seguridad se deban considerar los siguientes elementos:

- Alcance de las políticas, incluyendo facilidades, sistemas y personal sobre la cual aplica.
- Objetivos de la política
- Responsabilidades por cada uno de los servicios y recursos informáticos.
- Requerimientos mínimos para la configuración de la seguridad de los sistemas.
- Definición de violaciones y sanciones por no cumplir con las políticas.
- Responsabilidades de los usuarios con respecto a la información a la que tiene acceso.

También se debe explicar que para poder desarrollar las políticas estas deben tener una base sobre las cuales se debe partir para poder tener un soporte en el cual se

[5] www.auditoriasistemas.com/politicas_de_seguridad.htm

trabajará sin olvidar el tipo de limitaciones que tienen para poder aplicar las sanciones correspondientes.

Es importante el redactar estas políticas en un lenguaje libre de tecnicismos, es decir que sea fácil de entenderlo sin que esto provoque algún tipo de problemas por ambigüedad.

Y no debemos olvidarnos que las políticas debe ser actualizadas cada cierto tiempo para que no queden obsoletas dentro de la empresa y de esta manera poder salvaguardar los bienes de la empresa.

Para poder realizar las políticas es necesario que se tomen en cuenta diferentes puntos tales como:

- Evaluar los bienes informáticos de la empresa para poder valorarlos y poder realizar su correspondiente política a seguir.
- Pedir un informe a los departamentos involucrados directamente ya que por su experiencia nos permitirán definir las prioridades dentro de las políticas a definirse.
- Comunicar al personal que labora en los diferentes departamentos para que puedan acatar las políticas que se seguirán y las sanciones que estas implican.
- Determinar a los responsables de cada departamento para que se tome en cuenta las sanciones correspondientes.
- Monitorear constantemente cada uno de los departamentos para poder modificar las políticas cuando sea necesario.
- Explicar el alcance de las políticas para evitar problemas posteriormente.

Por último es importante el indicar cuales son los componentes de una política de seguridad:

- Una política de privacidad
- Una política de acceso
- Una política de autenticación
- Una política de contabilidad
- Una política de mantenimiento para la red
- Una política de divulgación de información

2.2 Organización y división de Responsabilidades

Es importante el realizar una organización y división de responsabilidades ya que esta permite tener un control de la calidad del trabajo. Dentro del área informática los recursos que nos permiten mejorar la calidad del control de la dirección son los siguientes[6]:

- Restringir el acceso a las actividades de operación al personal que prepara los datos.
- Los analistas de sistemas y programadores no deben tener acceso a las actividades de operación y viceversa.
- No debe existir acceso absoluto para los operadores a las funciones de protección de información o departamentos donde se encuentren los archivos maestros.
- Los operadores no deben tener los controles únicos del procesamiento del trabajo y se les debe prohibir que inicien correcciones de los errores.

Se debe considerar que el grado de división entre las diferentes funciones depende del nivel de seguridad que la instalación necesite. Existen elementos claves que se deben manejar dentro de la seguridad requerida y dentro de este contexto estas funciones claves son:

- Desarrollo de los sistemas
- Programación
- Mantenimiento de programas
- Preparación de los datos
- Operaciones Centrales y Remotas
- Control
- Preservación de los archivos

---

[6] http://www.arearh.com/rrhh/descripciondepuestos.htm

Las medidas de seguridad reducirán la flexibilidad en el trabajo pero, mediante el diseño detallado, no se afectará la eficiencia.

Como se dijo anteriormente es sumamente importante el asignar responsabilidades, por lo que es necesario el establecer las áreas por el tipo de persona que se encargará de las funciones de seguridad. Las funciones más importantes son las siguientes:

Supervisor de seguridad. Encargado de evaluar los riesgos y preparar los planes de seguridad, así como supervisar los procesos de selección de productos y los procedimientos de evaluación de las bitácoras de seguridad. De igual manera debe asistir en ella definición de límites para determinar una violación de seguridad, planes de seguridad para el sistema de red y establecer el programa de capacitación para el personal.

Oficial de Seguridad. Evalúa los riesgos de seguridad, dicta acciones contra los intrusos, supervisa la seguridad en tiempo real, así como el sistema de administración de la red. Además, ayuda en la selección de instrumentos, en la evaluación de las bitácoras de vigilancia, en la elaboración de los planes de seguridad.

Auditor de seguridad. Ayuda en la estimación de riesgos de seguridad, en el establecimiento de limites para determinar una violación a la seguridad, en la definición de la relación correcta de precauciones físicas y lógicas, además de evaluar las bitácoras de vigilancia, categorizar los riesgos de seguridad, auxiliar en la selección de instrumentos y escribir los reportes de avance de los planes de seguridad.

Analista de Seguridad. Se encarga de definir las funciones de monitores y vigilancia, evaluar el impacto de las técnicas de seguridad en el desempeño de red y seleccionar los servicios del área de seguridad. De igual manera debe recomendar instrumentos durante el proceso de selección de los mismos, programar los instrumentos y establecer procedimientos para asegurar el sistema de administración de la red.

Coordinador de la seguridad de la red. Controla configuración de la seguridad de la red, las autorizaciones de acceso las aplicaciones, servicios, gateways, routers, bridges y firewalls de la red; realiza el seguimiento del directorio de la red, administra los pases locales y ayuda en la toma de acciones contra los intrusos.

Un elemento muy importante en la seguridad es el garantizar que todo el personal importante o clave tenga una sustitución adecuada, razón por la que se necesita el restringir de manera cuidadosa la definición de personal clave, sin tener que importar el costo que este involucre ya que si la instalación requiere medidas de seguridad de alto nivel, entonces los niveles de gastos deben contemplar la sustitución y el apoyo clave adecuado para estos puesto llamados claves.

2.3 Políticas hacia el personal

En la actualidad se ha tomado conciencia de la contratación del personal y que cumplan con las políticas de integridad, estabilidad y lealtad hacia la empresa por lo que se ha visto necesario el considerar ciertos puntos para poder tener por parte de los empleados la lealtad a la empresa estos son [7]:

Políticas de Contratación. Dentro de las empresas se llevan a cabo ciertos procedimientos de contratación pero es indispensable el cumplir con ciertas características para poder contratar al personal adecuado y estas son:

- Verificación de referencias y antecedentes de seguridad.
- Pruebas psicológicas
- Exámenes médicos.

[7] http://www.minfin.gob.gt/politicas/a13.htm

Procedimiento para evaluar el desempeño. Estas pruebas permiten verificar sus actitudes hacia el trabajo, sus sentimientos hacia la empresa de esta manera podemos examinar como se desenvuelve en las diferentes áreas asignadas.

Políticas con permisos. Esta es una política sumamente importante ya que permite el detectar robos, fraudes y planes de sabotaje, por tal razón es importante el definir que tipos de permiso tendrá cada empleado y en que momento con esto se evitará graves problemas dentro de la empresa.

Rotación de Puestos. Esta es una buena política para evitar fraudes, en especial cuando se trata del personal de puestos altos de confianza, pero se debe tomar en cuenta que este tipo de política es recomendable utilizar en niveles de responsabilidad medio y bajo, pero siempre se debe tener un control mucho mayor cuando se trata de niveles altos ya que el fraude puede ser de gran escala.

Evaluación de las actitudes del personal. Se debe tomar en cuenta que, cuando un empleado esta muy bien motivado es difícil el que pueda ser desleal a su empresa, por lo que es necesario en caso de tener instalaciones grandes y gran cantidad de empleados el realizar encuestas de su satisfacción con el trabajo de esta manera estaremos seguros de que quienes trabajan en la empresa y se encuentran correspondidos por su trabajo y esfuerzo.

2.4 Los Seguros

Dentro del ámbito de los seguros es muy importante el considerar que, muchas de las veces las personas que trabajan dentro de los seguros no tienen el conocimiento necesario para poder entregar lo que se necesita dentro de un centro de cómputo y de igual manera se corre el riesgo por parte de las personas que laboran dentro de un centro de cómputo, motivo por el cual es

necesario el poder tener un entendimiento de los riesgos que esto significa para la empresa y como poderlos evitar.

Por lo tanto es necesario el determinar que es lo que deseamos asegurar y cuales son los puntos o aspectos que se han olvidado para lo que se debe tomar en cuenta[8]:

- Las áreas de riesgo asegurables.
- Los servicios de seguros especializados
- El cambio del tipo de riesgo

Área de riesgo asegurable

- Ambiente
- Equipo
- Programas y datos
- Interrupción comercial y su recuperación
- Personal
- Responsabilidades a terceras personas

Publicadas por el National Computing Centre(NCC) Julio 2003

Servicios de seguros especializados. Son ciertos servicios que ofrecen ciertas instituciones y estos incluyen adopción del personal altamente capacitado en el manejo de computadoras y, en consecuencia de los riesgos inherentes; además varias empresas internacionales de seguros cuentas con pólizas especializadas para usuarios de computadoras.

Por lo general un póliza de seguros de equipo de cómputo cubre:

1. **Daños materiales al equipo**

   Cubre cualquier pérdida o daño físico, súbito e imprevisto que requiere de reparación o reemplazo, pero no son considerados:

[8] http://cert.salud.gob.mx/Seguridadfsica.html

- Pérdidas o daños causados por terremoto, temblor, maremoto, erupción volcánica, ciclón, tifón o huracán.
- Pérdidas o daños causados por hurto o robo sin violencia.
- Pérdidas o daños causados por fallo e interrupción en el suministro de corriente eléctrica, gas o agua.
- Pérdidas o daños que sean consecuencia del uso continuo o deterioro gradual debido a consecuencias atmosféricas.

2. **Portadores externos de datos**

   Cubre los daños causados a dispositivos de almacenamiento de datos de igual manera la información contenida en estos.

   Pero excluye cualquier gasto resultante de la incorrecta programación, clasificación pérdidas de información causadas por campos magnéticos y virus informáticos.

3. **Incremento en el costo de operación.**

   Los seguros a los equipos de cómputo se aplican a los bienes que se estén operando que se encuentre en reposo, desmontados para propósitos de limpieza o reparación o durante su traslado dentro del período establecido en la póliza.

   Pero se excluye los causados por:

   - Guerra, invasión , actividades de enemigos extranjeros, hostilidades.
   - Reacciones nucleares, radiación nuclear o contaminación nuclear.

De igual manera existen pólizas adicionales que se pueden contratar que cubren otro tipo de problemas como son:

- Huelgas
- Daños por fallo de la instalación de climatización
- Hurto
- Daños mecánicos y eléctricos internos.

Razón para evaluar todos y cada uno de los tipos de seguros que se necesita para los centros de cómputo, es recomendable el trabajar con

las personas involucradas directamente en el centro de cómputo y no tratar de proponer algo sin una base en la cual se pueda sustentar.

4. **Seguimiento de los cambios en los riesgos**

   Es importante el considerar que muchas de las veces o mejor dicho siempre un centro de cómputo esta en constate cambio por los avances de la tecnología por lo que se debe estar actualizados.

   Para lo que es recomendable es contar con un Comité de seguridad del Centro de cómputo los cuales plantearán sus objetivos los cuales deberían basarse en:

   - Identificar y cuantificar los riesgos directos y consecuentes de la instalación de cómputo en la empresa.
   - Garantizar la existencia de planes de contingencia adecuada.
   - Obtener asesoría y orientación especializados cuando se requiera.

2.5 Auditoría y Control

Es importante que las empresas tengan definida lo que realiza una Auditoría y quienes son los responsables de efectuar periódicamente revisiones para poder realizar un seguimiento del cumplimiento de las normas establecidas por la empresa, especialmente en materia de seguridad, y de participar en la definición de nuevos sistemas.

Es indispensable que dependiendo del tipo de empresa y lo que se desea auditar se contrate a empresas especializadas de igual manera con personas que tengan el suficiente conocimiento del área para de esta manera controlar y prevenir posibles problemas, mejorando así el servicio y garantizando los equipos y la información que se encuentra en el centro de cómputo.

CAPITULO III

3.1 Ubicación física y disposición del Centro de Cómputo

Los lugares donde se deben ubicar los centros de cómputo deben ser acordes con las características del equipo a proteger.

Las condiciones varían dependiendo del tamaño de la empresa y el grado de dependencia que tenga de sus sistemas de cómputo, y como podrían afectar a la empresa en caso de ocurrir algún tipo de peligro.

Se debe considerar que la elección de la ubicación del centro de cómputo debe realizarse buscando un lugar adecuado, el cual debe estar lejos de diferentes áreas de tránsito como son las terrestres y aéreas; de igual manera debe encontrarse en lugares lejanos de radares y equipos de microondas.

Es necesario el que se realicen los estudios necesarios, con respecto al tipo de suelo y los factores ambientales a los cuales puede estar expuesto, para desde un inicio tomar medidas preventivas y de esta manera evitar cualquier tipo de desastre.

3.2 Factores relacionados a la localidad

El momento de la construcción de un centro de cómputo es importante el considerar un factor como es su seguridad y de esta dependerá mucho de donde se lo ubique, por lo que para la selección del local se deben tomar en cuenta dos alternativas:

- Se debe considerar en lo posible todas las condiciones relacionadas con el medio ambiente externo que lo rodearía, de esta manera se podrá tener una visión mucho mas amplia de cual seria el lugar más idóneo para el centro de cómputo.

- Pero, también es importante el entender cuales son las limitaciones a las cuales estamos sujetos, ya que se tendrá que corregir ciertas fallas para poder construir el centro de cómputo en un lugar determinado. De esta manera se realizarán arreglos en base a lo que se tiene por lo que se realizarán las modificaciones necesarias para adecuarlo en dicho lugar por lo que se tomarán las medidas necesarias para prevenir cualquier tipo de riesgo

Por tal motivo es indispensable el planificar cuidadosamente el lugar donde se construiría, su distribución y materiales sin olvidar que se debe realizar un plan de seguridad en un centro de cómputo para poder salvar los recursos que garanticen el funcionamiento de cualquier empresa ya instalada en el sitio o lugar elegido.

Para determinar si se cuenta con un bien local se debe tener en cuenta los aspectos físicos y sus requerimientos:

- **Naturales.**

  Muchas de las veces se está expuesto a peligros cuya ocurrencia se encuentra fuera del alcance del hombre, tales como el frío, el calor, las lluvias, los sismos y peligros del terreno. Para poder prevenir los desastres naturales se necesita una buena elección del lugar donde se ubicará el centro de cómputo.

- **Servicios**

  Es importante el verificar que el lugar donde se llevará a cabo la construcción del centro de cómputo cuente con los servicios básicos, de igual manera se debe verificar que se encuentren en buen funcionamiento y disponibles. Entre los servicios a considerar tenemos: líneas telefónicas, energía eléctrica, facilidades de comunicación, y antenas de comunicación.

- **Seguridad**

  Esta se basa en que la ubicación del centro de cómputo sea en una zona tranquila, que no se encuentre expuesta a riesgos de alto grado, y que no cuenta con las seguridades necesarias. También se debe anticipar que en las cercanías del edificio no existen lugares que propicien incendios fácilmente, debe de considerarse el peligro de inundación para lo que se tomará en cuenta los niveles de la calle en referencia con los del edificio para poder evitar cualquier tipo de problemas y esperando que los desfogues se realicen de manera satisfactoria sin afectar el centro de cómputo.

3.3 Factores relacionados al Centro de Cómputo

La forma como se encuentra construido interiormente el centro de cómputo es igual de importante que la externa, por lo que se debe considerar las características físicas que deben tener las instalaciones para brindar seguridad, dentro de las cuales tenemos [9]:

- **Piso Falso**

  Este debe contar con una resistencia para poder soportar el peso del equipo y el personal, entre otras tenemos:

  - Sellado hermético
  - Modularidad precisa
  - Nivelado topográfico
  - Posibilidad de realizar cambios
  - Debe cubrirlos cables de comunicación
  - Debe proporcionar seguridad al personal
  - Debe permitir un espacio entre los dos pisos para que este sirva de cámara de aire

[9] Especificaciones Técnicas dictadas por el Departamento de Auditoría Informática, Subdirección de Sistemas-DCAA-UNAM Julio 2003, y la TIA/EIA 942

- Con altura recomendada de 30cm cuando el centro de cómputo es de 100 m² y de 40 a 60 cm cuando es mayor a 100 m². Su altura mínima es de 18cm
- Los materiales recomendados son : acero, aluminio o madera resistente al fuego
- Es recomendable el cubrir el piso firme con pintura antipolvo.

- **Cableado**

  Se debe intentar colocar los cables debajo del piso falso, donde es importante ubicar los cables de manera que se aparten :

  - Cables de alto voltaje
  - Cables de bajo voltaje conectados a las unidades de las computadoras.
  - Cables de telecomunicaciones
  - Cables de señales para dispositivos de monitoreo detección de fuego, temperatura, humedad, etc.

- **Paredes y Techo**

  - Esta irán con pintura plástica lavable
  - El techo real, las placas del falso techo y los amarres deberá pintarse, si este se usa como plenum para el retorno del aire acondicionado.
  - La altura entre el piso falso y el techo falso debe estar entre 2.70 y 3.30 metros para permitir la circulación del aire .

- **Puertas de acceso**

  - Serán de doble hoja y con un ancho de 1.40 a 1.60 cm
  - Es necesario la salida de emergencia.
  - Se deberá tomar en cuenta las dimensiones máximas de los equipos en caso de tener que atravesar puertas y ventanas de otros departamentos.

- **Iluminación**
    - No debe ser alimentada de la misma fuente que los equipos de cómputo
    - Evitar la luz directa para poder observar la consola y las señales
    - La distribución de lo iluminación será: 25% para la iluminación de emergencia y se conectará al sistema ininterrumpible.

- **Filtros**
    - Elegir los filtros adecuados
    - Se recomienda los tipos de humificadores de vapor
    - El aire de ventilación será tratado tanto en temperatura y humedad como en filtrado antes de entrar al centro de cómputo

- **Ductos**
    - Deben ser material que no desprenda partículas con el paso del aire.
    - No deberá tener revestimientos internos de fibras.

3.4 Acondicionamiento del local

Consiste en realizar las modificaciones necesarias al lugar donde se ubicará el centro de cómputo, y esta inicia con la distribución del espacio. Por lo que es necesario el adecuarlo según las necesidades [10].

[10] http://www.monografías.com/trabajos/seguinfo/seguinfo/shtml

Necesidades de espacio

Está determinada por las especificaciones técnicas de los equipos, su tamaño debe tener forma y tamaño adecuados, por lo que no es recomendable el trabajar con áreas de formas extrañas, el tratar de no tener problema con las columnas con la finalidad de que estas no estorben, de igual manera es necesario el considerar futuras modificaciones y que se encuentren acorde al espacio. Es necesario el tener un plano en el cual se indique las adecuaciones y los espacios para los cambios y adquisiciones de la empresa en cuando a equipos.

Distribución en planta del local destinado a Centro de Cómputo

Es necesario para esto basarnos en los diferentes planos tanto civiles como arquitectónicos los cuales nos permitirán el tener una mejor visión para la ubicación de los equipos y los elementos de trabajo, los cuales incluyen muchos aspectos que deben ser considerados el momento de distribuir la planta y estos son:

- Plano de plantas: especifica las distribuciones de paredes, dimensiones del lugar, ventanas, puertas, columnas, etc.
- Plano de memoria de cálculo: indica la capacidad que tiene el edificio para soportar una planta.
- Plano de corte hidráulico: permite conocer la distribución de tuberías, tomas de agua, etc.
- Plano de corte sanitario
- Plano de teléfono
- Planos de seguridad: indica las salidas de emergencia, también las vías de desalojo, colocación de mangueras y extintores, timbres, alarmas, etc.
- Plano de energía eléctrica

De igual manera se debe contar con el plano de la distribución del centro de cómputo el cual debe contar con:

- Paredes, puertas y ventanas
- Salidas de emergencia, columna y pilares.

- Control y equipo de aire acondicionado
- Archiveros, escritorios.

Este plano permite:

- Conocer los requerimientos de cable
- Ubicar las diferentes áreas con base en sus actividades y exigencias.
- Encontrar el camino mas corto para los operadores.

CAPITULO IV

Control de Acceso Físico

Es importante asegurarse que los controles de acceso sean estrictos durante todo el día, y que estos incluyan a todo el personal de la institución, especialmente durante los descansos, cambios de turno y durante la noche.

Se debe identificar el personal de informática así como cualquier otra persona ajena al área de trabajo antes de ingresar a esta. El riesgo que proviene de alguien de la organización es tan grande como el de cualquier otro visitante.

Solamente el personal autorizado por medio de un control de acceso o por la gerencia debe ingresar a dichas instalaciones.

5.1 Estructura y disposición del área de recepción

Dentro de los Centro de Computo se cuenta con lugares, de recepción y reposición de información, por lo que estas áreas son consideradas de alta seguridad donde es necesario el estudiar la posibilidad de ataque físico, por lo que se debe implementar diferentes formas de control tales como: dispositivos magnéticos automáticos, identificación del personal que ingresa a esta área, entre otros recursos de recepción, lo que permitirá que se salvaguarde la información de gran importancia.

5.2 Acceso a terceras personas

Se considera como terceras personas a todos aquellos que realicen limpieza, mantenimiento de equipos, y visitantes. Estos y cualquier otra persona ajena al área de trabajo deben ser:

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

Todas aquellas personas ajenas al área de trabajo se deben identificar antes de entrar a ésta.

5.3 Identificación del personal

Se pueden considerar algunos parámetros con lo que se le asocia la identificación del personal tales como: algún documento de identidad que se porte, o sea expresado de manera verbal como número o claves de ingreso, características físicas: neuromusculares y genéticas [11].

Asimismo pueden utilizarse los siguientes elementos:

- Puerta de combinación, requiere de una secuencia de números para permitir el acceso, la cual debe ser cambiada regularmente cuando el empleado termine su función laboral dentro de este centro de cómputo.
- Puerta electrónica, requiere de una tarjeta plástica magnética como llave de entrada.
- Puertas sensoriales, activadas en base a una característica física única del individuo, como pueden ser la huella dactilar, voz, retina, geometría de la mano o bien por la firma.
- Registro de firma de entrada y salida, consiste en que todos los visitantes al centro de computo firmen un registro en el cual conste la hora da entrada, el motivo de su ingreso y la hora de salida.
- Tarjetas de acceso y gafetes de identificación, podría tratarse de simples gafetes visibles o escarapelas del personal, hasta tarjetas con código magnético que permitan el acceso a diferentes áreas. Los dispositivos de lectura de tarjeta pueden ser conectados a un ordenador el mismo que contenga información acerca del individuo. La autorización se puede manejar de manera individual para cada puerta controlando de esta manera la hora y el día de las funciones.
- Equipos de monitoreo, la utilización de dispositivos de circuitos cerrado de televisión, tales como monitores y cámaras deben ser

[11] http://cert.salud.gob.mx/Controldeacceso.html

colocadas en puntos estratégicos para que pueda monitorear el centro.

- Puertas dobles, este equipo es recomendable para lugares de alta seguridad: se trata de dos puertas, donde la segunda solo se pueda abrir cuando la primera este cerrada.
- Alarmas, todas las áreas deben estar protegidas contra robos o acceso físicos no autorizados. Las alarmas contra robo deben ser usadas hasta donde sea posible en forma discreta, de manera que no se atraiga la atención hacia este dispositivo de alta seguridad. Tales medidas no sólo se deben aplicar en el centro de computo si no también en áreas adyacentes.
- Trituradores de papel, los documentos con información confidencial deben ser triturados antes de desecharlos, ya que así no pueden ser reconstruidos, evitando el robo de información.

CAPITULO V

Aire Acondicionado

6.1 Capacidad del equipo

El contar con aire acondicionado se presenta una solución pero al mismo tiempo un problema, en caso de no realizárselo de manera adecuada, ya que es necesario el contar con este tipo de instalaciones en un lugar donde existen computadoras, para una mayor distribución del aire y el calor que los equipos producen, pero al mismo el no realizar una instalación adecuada podría provocar grandes problemas como incendios, o que sus ductos sean susceptibles para ataques físicos.

Por lo que es importante el afrontar los riesgos que estos producen tomando en cuenta:

- En los centro de cómputo grandes al instalar equipos de aire acondicionado de respaldo, se deben establecer aplicaciones de alto riesgo. Es necesario que dentro del centro de cómputo se deba contar con componentes que pueden ser reemplazados fácilmente, con respecto a la instalación o equipo de aire acondicionado.
- Instalar redes de protección en todo el sistema de ductos.
- Instalar extintores y detectores de incendios en los ductos

6.2 Distribución del aire en el Centro de Cómputo

Para realizar una buena instalación del aire acondicionado en el centro de cómputo se debe tomar en cuenta [12]:

[12] MANUAL DE SEGURIDAD FISICA Y AMBIENTACION DE LOS CENTROS DE COMPUTO DE LA SAGAR, ENERO DE 1996.

1. **Capacidad del equipo de aire acondicionado**
    - Disipación térmica de las maquinas
    - Disipación térmica de las personas
    - Cargas latentes, aire de renovación
    - Pérdidas por puertas y ventanas
    - Transmisión de paredes, techos y suelo
    - Disipación de otros aparatos
    - Cargas calorífica del equipo de cómputo y sus periféricos(proporcionadas por el proveedor)
    - El aire acondicionado para el centro de cómputo debe ser independiente del aire general del edificio.

2. **Distribución del aire en la sala**
    - Los componentes de las máquinas se refrigeran mediante la circulación rápida del aire por ventiladores instalados en sus equipos.
    - La entrada de aire debe ser por debajo de las máquinas a través de las rejillas.
    - El aire caliente es expulsado por la parte superior de las máquinas.
    - El sistema de distribución debe planificarse de manera que no exista excesiva velocidad de aire.
    - La ventilación del lugar variará en función del volumen de la sala.
    - Primero se debe renovar el aire cuando esta contaminado

    Distribución por el techo
    - El aire es impulsado por el techo
    - El retorno del aire es por el techo por medio de rejillas colocadas sobre las de salidas del aire caliente.
    - El volumen de aire es menos con el que se trabaja
    - Cuenta con una flexibilidad de cambios de posición de unidades menor.
    - Debe ser estudiado el hecho de no contar con corrientes de aire frió.

Distribución del piso falso

- Como se dijo anteriormente el espacio existente entre el suelo y el piso falso se lo utiliza como cámara de aire.
- El aire se descarga en el centro de cómputo por medio de registros en el suelo.
- El aire retorna al centro por medio de rejillas en el techo.
- Es necesario cierta cantidad de recalentamiento para controlar la humedad relativa del aire en el piso falso.
- Se debe colocar de manera precisa las rejillas y los retornos para no provocar tiros de aire frío a caliente.

Dos canalizadores

- Por medio de una unidad de controles separados suministra aire y filtrados a las tomas de aire de los dispositivos de cómputo.
- Mientras que la otra unidad suministra aire directamente a la sala por canalización diferente y absorbe el resto de la carga de calor.

CAPITULO VI

Instalación Eléctrica

En un centro de cómputo es sumamente importante la instalación eléctrica, ya que el funcionamiento del mismo depende de este, y el fallo de esta puede llegar a provocar graves daños.

Es importante el conocer cuales son los voltajes con los que trabaja cada uno de los equipos de un centro de cómputo, los mismos que se encuentran especificados por el proveedor.

7.1 Corriente Regulada

Dentro de los centros de cómputo los equipos tienen ciertas tolerancias debido a los cambios de voltaje, por lo que es necesario su correcto funcionamiento, para lo que es necesario el contar con un regulador de voltaje.

El regulador de voltaje se encuentra diseñado para trabajar en un rango de voltaje determinado, ya que el voltaje que se recibe es regular se lo deja pasar hacia la carga, caso contrario en caso de existir variaciones que se encuentran dentro del límite, este es elevado o disminuido para poder pasarlo como voltaje, vale decir que siempre y cuando los voltajes de entrada y salida se encuentren entre los limites definidos por el fabricante del regulador.

En el mercado podemos encontrar reguladores que aceptan voltajes desde 95 a 145 volts, que permiten una salida de 115 volts, y que cuentan con un sistema que los desactiva automáticamente en caso de que el voltaje se sobrepase [13].

[13] www.auditoriasistemas.com/auditoria_de_sistemas.htm

7.2 Sistema de corriente Ininterrumpida

Tiene las siguientes funciones:

- Regula la cantidad de energía eléctrica que llega al equipo de procesamiento de datos.
- En caso de ocurrir una falla de suministra de energía este la proporcionará.
- En caso de existencia de una planta generadora de energía, esto le dará tiempo para que alcance su carga plena.

Se puede considerar tres tipos de sistemas de corriente ininterrumpida [14]:

Básico: este proporciona energía a un limitado número de dispositivos, incluido la unidad de procesamiento y los controladores de los medios de almacenamiento, este sistema funciona por unos minutos, en caso de no regresar la energía en dicho lapso de tiempo, se debe respaldar la información y luego proceder a apagar el equipo.

Completo: este permite que el equipo funciones de manera oportuna y ordenada. Es necesario que los controladores de los medios de almacenamiento y el procesador se encuentren conectados a él.

Redundante: es un sistema de corriente ininterrumpida adicional en caso de que se produzca algún tipo de fallo con la principal, es utilizada para centro de cómputo con un nivel de seguridad muy alto lo que implica un alto costo.

[14] Especificaciones Técnicas dictadas por el Departamento de Auditoría Informática, Subdirección de Sistemas-DCAA-UNAM Julio 2003, y la TIA/EIA 942

Es necesario el realizar consideraciones en la planeación del uso de este sistema las cuales son:

- Considerar que el tiempo de interrupción en el suministro de energía eléctrica es variable.
- Permite contar con un tiempo determinado para poder apagar el equipo de manera oportuna y adecuada.
- El costo de un sistema de corriente ininterrumpida se incremente de acuerdo al tiempo que es capaz de soportar.
- Es necesario el realizar un estudio para seleccionar el sistema adecuado en función del sistema necesitado.
- Es necesario el contar con la modularidad de los sistemas de corriente ininterrumpida, lo que permitirá una sencilla reposición de partes.

Existen cierta especificaciones dadas por el proveedor del sistema para poder salvaguardar el equipo y la información pero adicional a esta información tamben se debe tener en cuenta la cantidad de energía que suministra el equipo adicional de carga ininterrumpida.

Dentro de un sistema **básico** de corriente ininterrumpida, la capacidad es de 5 a 10 minutos. En un sistema **completo** varía en función de los diferentes requerimientos tales como el tamaño dela memoria principal y la configuración del sistema.

Es importante el poder saber y consultar con el proveedor el tiempo que necesita para poder recargarlo con lo necesario, debe ser considerado el hecho de que estas deben localizarse en un cuarto separado y ventilado y seguir las recomendaciones establecidas por el proveedor.

Al seleccionarse el lugar del sistema de corriente ininterrumpida este debe cumplir con ciertos factores tales como [15]:

1. **Temperatura de las baterías.** Estas deben instalarse en un ambiente frío y seco sin la existencia de algún tipo de calor radiante. La temperatura ambiente de diseño para éstas es generalmente mas baja que la mínima aceptable para el sistema de corriente ininterrumpida, pero debe tomarse en cuenta que las temperaturas mas bajas afectan su capacidad y las más altas afectan su vida.

2. **Ventilación.** Esta es una indicación dada por el proveedor en el cual se especifica la salida de calor e indica el uso de ductos o ventiladores y cuando es necesario determina la altura que debe existir.

3. **Niveles de Acústica.** Es indicada por el proveedor los niveles ambientales con los que mas se trabaje, pero sin depender solamente del ruido ocasionado, sino también por factores como absorción y reflexión de paredes.

4. **Seguridad.** Es recomendable el colocar este sistema en un cuarto separado, con un agente neutralizante cercano tales como agua, extintores en caso de emergencia.

5. **Capacidad de carga del piso.** El lugar donde se encuentre el sistema debe contar con consideraciones estructurales que vienen determinadas por el fabricante de esta manera se lo hará de acuerdo a las necesidades requeridas.

[15] [15] Especificaciones Técnicas dictadas por el Departamento de Auditoría Informática, Subdirección de Sistemas-DCAA-UNAM Julio 2003, y la TIA/EIA 942

7.3 Planta generadora de Energía

Al trabajar con un centro de cómputo es necesario contar con una planta generadora de energía para obtener mayor seguridad en los procesos operativos, instalaciones físicas y equipos eléctricos [16].

Componentes

En un centro de cómputo se requiere un generador exclusivo para el equipo de cómputo, sus respectivos periféricos, el aire acondicionado del centro, para la iluminación de emergencia.

Al contar con un sistema de este tipo se debe trabajar con un dispositivo automático, ya que la fuente es monitoreada en forma continua y en caso de ocurrir un fallo esta inicia automáticamente la planta de emergencia. Esta permite el poder trabajar de manera segura y sin la posibilidad de perder algún equipo o información.

Se puede clasificar a estos sistemas dependiendo de su fuente de alimentación:

- **Diesel** utiliza motores que pueden alcanzar su carga máxima en menos de 10 segundos, su capacidad varía entre los 2.5 KW. El costo del diesel puede ser variable, existe mayor posibilidad de reparación.

- **Gasolina.** Satisfacen necesidades de 100Kw de salida, inicia rápidamente. Como desventaja son sus altos costos de operación, mayor peligro por el tipo de combustible utilizado, menor almacenamiento y menor tiempo de mantenimiento.

- **Gas.** Utiliza turbina de gas que requieren de 30 a 90 segundos para alcanzar su carga plena, no se puede encontrar turbinas en tamaños

[16] [16] Especificaciones Técnicas dictadas por el Departamento de Auditoría Informática, Subdirección de Sistemas-DCAA-UNAM Julio 2003, y la TIA/EIA 942

menores a 500Kw, encontrándolos por lo general con capacidad de 600 Kw. Estas turbinas operan con menos ruido y vibraciones que las de diesel, y por lo general los costos de instalación son menores.

7.4 Sistema de conexión a tierra

La idea de contar con un sistema de protección es prevenir fallar a tierra en el propio diseño, operación y mantenimiento de sistema y equipos eléctricos[17].

Para esto se requiere:

- **Equipo protector de circuitos.** Se puede trabajar con diferentes tipo de circuitos de protección, entre los más conocidos tenemos los fusibles, los corto circuitos con series y el equipo interruptor de circuitos para dispositivos. Para poder definir cual es el que se necesita dentro de un centro de cómputo es necesario el realizar un análisis detallado de cada sistema y lo que se va a proteger.

- **Sistema y equipo a tierra.** Un sistema a tierra hace referencia a la forma en la cual el conductor de circuito de un sistema es efectivamente conectado a tierra. Cuando se habla de equipo a tierra este es la unión de todos los circuitos conductores de cada circuito del equipo con los conductores del equipo a tierra.

  El sistema de conexión a tierra previene y protege contra peligros de choque eléctrico. Las conexiones eléctricas del conductor a tierra, su condición y su capacidad de carga de corriente son factores importantes en el suministro de una vía de baja resistencia para corriente de fuga y falla.

[17] [17] Especificaciones Técnicas dictadas por el Departamento de Auditoría Informática, Subdirección de Sistemas-DCAA-UNAM Julio 2003

Es importante para poder tener una efectiva conexión a tierra se debe tener en cuenta dos puntos importantes como son [18].

- **Seguridad.** El sistema de tierra protege al personal de operación y mantenimiento, en caso de que exista un cambio de voltaje.

- **Compatibilidad electromagnética.** Disminuye la posibilidad de interferencia proporcionando un punto de referencia en común.

En el camino del conducto de tierra, no deben conectarse:

1. Estructuras metálicas (tuberías de agua, construcciones de acero).
2. La conexión para el sistema de cómputo para tierra física debe ser única.
3. El tipo de cable a ser utilizado debe ser aislado y del mismo calibre que el del neutro y el de las fases.
4. Para la conexión se necesita instalar una varilla de cobre enterrada en el piso, esta debe tener una longitud mínima de 2 metros un diámetro de 2.3 centímetros

Existen muchas razones por la que se tienen conectados a tierra el equipo eléctrico o los sistemas de instalación de alambres y son porque:

- Ofrece una ruta para una falla de corriente.
- Garantiza la seguridad del personal
- Reduce la carga estática
- Reduce la señal eléctrica de ruido

[18] [18] Especificaciones Técnicas dictadas por el Departamento de Auditoría Informática, Subdirección de Sistemas-DCAA-UNAM Julio 2003

7.5 Recomendaciones

Para poder realizar la instalación eléctrica en un centro de cómputo se debe tomar en cuenta las siguientes consideraciones [19]:

- Las variaciones del voltaje no debe exceder + 15% o – 18% del voltaje nominal y debe regresar al rango estándar de voltaje en menos de ½ segundo.

- La variación de voltaje entre fases no tendrá que ser mayor del 2.5% de la media aritmética de las tres fases.

- La frecuencia de la línea debe mantenerse dentro de + - ½ hertz (ciclos por segundo).

- El contenido máximo de armónicos del voltaje de la fuente de alimentación del equipo no debe exceder + - 5% cuando el equipo esté en operación.
- La acometida de energía eléctrica que alimente al equipo de cómputo debe ser independiente y no la conectará ninguna otra carga, con el objeto de evitar interferencias.

- La sección de los conductores eléctricos de la acometida debe calcularse para la potencia consumida por el equipo de cómputo, considerando un 30% adicional como margen de seguridad y posible ampliación.

- Los conductores eléctricos deberán ir dentro de una tubería apropiada, de manera que se evite campos electromagnéticos.

- Los circuitos deberán ir protegidos en mangueras flexibles o bajo tubo traqueal.

[19] [19] Especificaciones Técnicas dictadas por el Departamento de Auditoría Informática, Subdirección de Sistemas-DCAA-UNAM Julio 2003

- En caso de utilizar cajas de conexión bajo el piso falso, estas deben contar con etiquetas de identificación.

- Es necesario la existencia de enchufes auxiliares monofásicos a 127v. distribuidos en la centro de cómputo y que provengan de una alimentación distinta a la del equipo de cómputo.

- Se debe instalar un equipo regulador donde se presente frecuentemente las variaciones.

7.6 Riesgo de inundación

Este tipo de situación no solamente se da por el hecho de estar en un lugar donde el clima pueda perjudicar o dañar un centro de cómputo razón por la cual se tiene que tener una planificación del lugar donde se ubicará el centro de cómputo tomando en cuenta que si se encuentra en este tipo de zonas no deberá ser en sótanos o lugares muy bajos.

Pero de igual manera se puede originar este tipo de problemas por ruptura de cañerías o por el bloqueo de drenaje. Razón por la cual la ubicación de las tuberías en la construcción de las instalaciones de cómputo es una decisión importante, ya que no se debe colocar estas encima de las áreas donde se encuentran los equipos.

Cuando se encuentra con un drenaje bloqueado su riesgo es mayor en caso de que el centro este ubicado en el sótano.

Por lo que es importante el instalar detectores de agua o de inundación, así como bombas de emergencia.

7.7 Protección, detección y extinción de incendios

Es indispensable contar con protección contra el fuego, la cual es lograda por medio de una correcta construcción del centro de cómputo. Sin embargo, existen materiales combustibles por lo que es necesario disponer con el equipo contra incendio de manera inmediata y que permita el control del fuego con relativa facilidad

Para la construcción del centro de cómputo es necesario el tomar en cuenta los siguientes elementos [20]:

- Las paredes del centro de cómputo deben ser de materia no combustible. Pero en caso de tener ventanas es indispensable el contar con ventanas irrompibles lo cual mejorará la seguridad.

- El techo y techo falso debe ser de material no combustible o resistente al fuego.

- El techo del área de almacenamiento de discos deben ser impermeables.

- Los detectores de humo y fuego deben ser colocados en relación con los sistemas de aire acondicionado.

- El detector de humo debe ser capaz de detectar los distintos tipos de gases que desprendan los cuerpos, ya que los producidos por un cortocircuito tal vez no sean detectados.

- Los detectores de humo y calor deben ser instalados en el centro de cómputo cercano a las áreas de oficina y dentro del perímetro físico de las instalaciones.

[20] [20] Especificaciones Técnicas dictadas por el Departamento de Auditoría Informática, Subdirección de Sistemas-DCAA-UNAM Julio 2003, y la TIA/EIA 942

- Se debe colocar detectores de humo y calor bajo el piso y en los ductos del aire acondicionado.

- Se debe conectar la alarma de incendios con la alarma central o directamente con el departamento de bomberos.

Los requerimientos antes indicados es importantes que no solamente se apliquen el área comprendida del centro de cómputo, sino de igual manera en las áreas adyacentes.

Existen distintos tipos de extintores los cuales pueden ser de agua, espuma o polvo seco esto dependerá del material contra el cual se desea extinguir el fuego para lo que se presentará un cuadro de referencia para el uso de diferentes tipo de extintores.

TIPO DE MATERIAL	**TIPO DE EXTINTOR**			
	AGUA	**CO2**	**ESPUMA**	**POLVO SECO**
Materias secas (papel medera tela, etc)	EXCELENTE Achorro o pulverizada, satura el material, refrigera y evita la reignicion	Para fuego de pequeña importancia. Debe emplearse inmediatamente despues del agua	EXCELENTE Cubre y humedece la materia inflamada	En fuegos de pequeña importancia. Se empla Inmediatamente despues del agua
Líquidos inflamables (gasolina, aceites, pintura, etc)	Con los liquidos menores y volátiles: AGUA PULVERIZADA Con los restantes : NO	EXCELENTE Sofoca y refrigera. Es mas indicado su uso en locales cerrados	EXCELENTE Cubre el fuego impide la combustion	EXCELENTE
Material Eléctrico (motores, cuadros, transformadores, etc)	NO USARLO	EXCELENTE No es conductor no deja residuos y no deteriora	NO El agua que contiene puede ser	SI No es conductor ni deja residuos

Es necesario el ubicar los extintores apropiados en lugares de acceso inmediato y señalarlos. De igual manera, toda información o recomendación relativa a la seguridad debe ser claramente visible; en este caso deben existir indicadores de prohibición de fumar. Es indispensable el tener un control regular del funcionamiento de los extintores y el equipo contra incendios.

Deben documentarse y definir los procedimientos que deben seguirse en caso de incendios, para lo cual es necesario el realizar simulacros de incendio para de esta manera entrenar al personal.

Es importante el contar con la participación del departamento de bomberos para el diseño y aplicación de procedimientos para detectar, prevenir y extinguir incendios.

7.8 Mantenimiento

Es importante que una empresa deba disponer de los servicios de mantenimiento, en función de sus características y posibilidades. Los servicios deben abarcar los equipos informáticos como los equipos auxiliares como son: electricidad, agua, aire acondicionado, etc.

La limpieza dela instalación del centro de cómputo es importante por:

- Permite reflejar una actividad disciplinada. Ya que la seguridad es una actividad mental y refleja el que los procedimientos utilizados son efectivos y adecuados.

- El mal mantenimiento crea condiciones para la ruptura de la seguridad, cuando dentro del área del centro de cómputo no se cumplen con las reglas bases.

Es muy importante el mantener limpio el centro de cómputo, pero se debe tener en cuenta al personal de limpieza que del agua y el detergente son agentes que afectan los equipos por lo que se debe trabajar con materiales que no puedan dañar al equipo y esta instrucción o información se la debe entregar al personal de limpieza por medio de un entrenamiento o preparación para este trabajo.

El buen mantenimiento refleja la actividad general de las personas en una empresa: simboliza una buena administración y aumenta la seguridad en computación.

CAPITULO VII

Plan de contingencia

Es muy común trabajar con la posibilidad o riesgo de un desastre, los accidentes pueden surgir en cualquier momento sea por un mal manejo de la administración, por negligencia, por ataques deliberados, por fraudes, sabotajes, o un simple daño de un equipo.

Es por eso que la organización tiene que ser capaz de evitar un desastre, debe poseer los controles, las funciones y dispositivos necesarios, para que no deje de operar, en caso de que un siniestro ocurra, debe contar con un plan de contingencia, el cual permita que en el menor tiempo posible se pueda restaurar el equipo, minimizando las consecuencias en caso de un desastre.

7.1 Objetivo

El objetivo principal de un plan de contingencia es permitir que la organización y sus actividades sigan operando con relativa normalidad en caso de que ocurra un percance, de forma de que en el menor tiempo posible se pueda restaurar las operaciones normales del centro de cómputo, minimizando el impacto del desastre ocurrido.

El plan de contingencias dependerá de la naturaleza de cada organización, se deben establecer procesos que sean indispensables para la compañía, teniendo en cuenta el costo del plan de recuperación para poder restablecer los procesos críticos de la organización cuando allá ocurrido una paralización de las operaciones.

Este plan de contingencias debe abarcar varias acciones a realizar para que sea más seguro:

- Prevención: es decir que debería ser como un plan de respaldo
- Detección: durante el trabajo, que seria un plan de emergencia y
- Recuperación: seria un plan de recuperación luego de ocurrido un desastre

7.2 Etapas y características

Para que un plan de contingencias sea eficiente este debería cumplir con algunas etapas y características. Entre las etapas del proyecto del plan de contingencia están:

- Estudio del impacto del desastre en la organización.
- Elección de la mejor estrategia a llevarse acabo.
- Elaboración del plan.
- Prueba.
- Mantenimiento.

De igual manera el plan de recuperación debería cumplir con ciertas características para que al momento de ser implementado sea de lo más eficaz posible, estas características son:

- Actual, conforme con las necesidades de la empresa.
- Entendible, que sea comprendido por el personal de la organización
- Factible, que este plan sea posible llevarlo acabo de acuerdo con la realidad de la empresa.
- Probado, se debe realizar una prueba del plan, para saber si este es efectivo.
- Documentado todo lo obtenido por el plan.

En una organización un plan de contingencia bien desarrollado debe contemplar los aspectos operacionales como administrativos.

- Operacional cada persona de la organización debe saber que hacer, y de igual manera saber a que persona se debe llamar en caso de un desastre.
- Administrativos contemplan varios puntos, como puede ser identificación de tareas críticas de la empresa, responsable de los medios de respaldo, localización del Software de reemplazo, acciones a ser tomadas en cada daño parcial, etc.

7.3 Consideraciones

Para el correcto desarrollo de un plan de contingencias, y para que su implementación sea eficaz en caso de un desastre se deben tener en cuenta las siguientes acciones a ser realizadas:

- Nombrar o designar un grupo que se encargue de la elaboración del plan de contingencia.
- Dar prioridad a las acciones propuestas por el plan de continencia, sobre como se lleva la organización tradicionalmente.
- Que los niveles del plan de contingencia sean considerados vitales para el negocio, y de igual manera los documentos generados en una situación de emergencia.
- Tener en cuenta los factores externos que puedan entorpecer las operaciones de la empresa al momento de realizar el plan de contingencia.

7.4 Plan de recuperación en caso de desastre

Las acciones que se establecen en el plan de recuperación en caso de que ocurra un desastre se las implementa como medidas previsoras, y solo entran en funcionamiento en caso de que ocurra una calamidad y esta sea constatada.

Al presentarse cualquier contingencia, se establecen los recursos y la metodología necesaria para poder restablecer los servicios de cómputo de forma oportuna para que de esta forma la organización siga trabajando con relativa normalidad.

7.5 Responsabilidad del plan de respaldo

Dentro del centro de cómputo debe existir personal que sea responsable y que se haga cargo de:

- Especificar las mejores tácticas de respaldo, que conjuntamente con el usuario, verificarán su validez y eficacia.
- Validar el contenido de los respaldos, y que estos sean actuales, creando los programas necesarios para su procesamiento.
- Al mismo tiempo, con el usuario buscar la mejor táctica, para seguir operando normalmente, en caso de que se presente un desastre,
- Construir los mecanismos de respaldo necesarios para resguardar las contingencias peligrosas en los sistemas y equipos de cómputo, diseñando los programas que permitan lograr este objetivo.

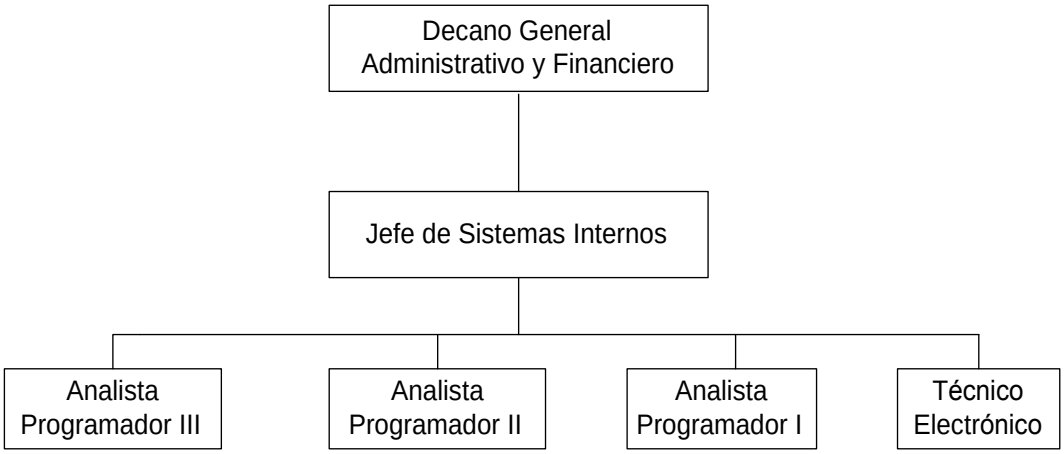
CAPITULO VIII

Aplicación Práctica – Aplicación de las Normas de Auditoría

La presente aplicación fue desarrollada, en el Centro de Cómputo de la Universidad del Azuay, la misma que nos brindó toda la ayuda necesaria, permitiendo de esta manera el colaborar con la investigación y mejora de estas instalaciones.

8.1 Análisis del Centro de Cómputo

Organigrama del Centro de Cómputo



El Centro de Cómputo de la Universidad del Azuay cuenta con el organigrama anteriormente indicado; en el mismo podemos observar como están delegadas las funciones del personal, que se encuentra laborando en dicho centro. Podemos notar que en el centro de cómputo existe un Jefe de Sistemas Internos, quien se encuentra trabajando directamente bajo el mando del Departamento Administrativo y Financiero de la Universidad.

El Jefe de Sistemas Internos tiene bajo su mando a los Analistas Programadores I, II, III y el Técnico Electrónico.

8.2 Entrevista con el personal

El Centro de Cómputo de la Universidad , nos presenta un organigrama el cual, ha permitido tener una mayor visión de las responsabilidades y funciones de cada uno de los miembros que laboran dentro de las instalaciones:

Jefe de Sistemas Internos

Su función es la de planificar, organizar y coordinar las actividades Administrativas de Sistemas Internos.

Analista Programador III

Es quien se encarga de diseñar y desarrollar los sistemas requeridos por la Universidad.

Analista Programador II

Es la persona que está encargada de analizar y desarrollar las aplicaciones requeridas por la Universidad.

Analista Programador I

Es la persona que se encuentra a cargo del mantenimiento de los sistemas desarrollados en la Universidad y dar el soporte requerido a todos los usuarios de los sistemas.

Técnico Electrónico

Persona responsable de mantener en buenas condiciones los equipos de cómputo de la Universidad.

8.3 Aplicación de Cuestionarios

CUESTIONARIO AUTORIZACION DE ACCESOS AL CENTRO DE COMPUTO

EMPRESA AUDITADA Universidad del Azuay
FECHA DE AUDITORIA 14 Marzo 2006
SUPERVISOR Ma. Fernanda Marín S.
AUDITOR Fernando Zea M

	PREGUNTAS	SI	NO	N/A	OBSERVACIONE
1	Se cuenta con medidas de seguridad en el Centro de cómputo?	X			
2	Existe una persona responsable de la seguridad del Centro de Cómputo en las horas laborables? Indique quien:		X		
3	Existe vigilancia para el Centro de Cómputo luego de la jornada de trabajo? Indique quien o como:	X			Guardias de vigilancia en turnos rotativos y conserje
4	Son controladas las visitas y demostraciones Al Centro de Cómputo?	X			
5	Se restringe el acceso al Centro de Cómputo a personas ajenas a la Dirección de Informática? Indique de que forma:	X			Existe una puerta que permanece cerrada bajo vigilancia de la secretaria
6	Existe un registro de las personas que ingresan a las Instalaciones?		X		
7	Se registran las acciones de las operaciones para evitar que realicen algunas pruebas que puedan dañar los sistemas?	X			
8	Existe una división de responsabilidades en las diferentes áreas del Centro de Cómputo para tener un mejor control de la seguridad?	X			
9	Existe algún tipo de mecanismo de seguridad para lugares restringidos?		X		
10	Describa brevemente la construcción del Centro de Computo, de preferencia proporcionando planos y materiales con que fue construido y el equipo (muebles, sillas, etc.) dentro del Centro Computo?				

Anexo 2 Ref. 8-11

CUESTIONARIO DE DETECCION DE HUMO, FUEGO Y EXTINTORES EN EL CENTRO DE COMPUTO

EMPRESA AUDITADA Universidad del Azuay
FECHA DE AUDITORIA 14 Marzo 2006
SUPERVISOR Ma. Fernanda Marín S.
AUDITOR Fernando Zea M

	PREGUNTAS	SI	NO	N/A	OBSERVACIONES
1	Existen sistemas de detección de humo, fuego u otro tipo de censores?		X		
2	Existen extintores de fuego a. Manuales ( ) b. Automáticos ( ) c. No Existen ( )		X		
3	En caso de existir extintores manuales, se adiestra al personal en el manejo de los extintores?			X	
4	Los extintores, manuales o automáticos son a base de: a. Agua ( ) b. Gas ( ) c. Otros ( )			X	
5	En caso de existir extintores automáticos son activados automáticamente por detectores automáticos de fuego?			X	
6	Dentro del Centro de Cómputo, se tienen paredes o materiales no inflamables?		X		
7	Se ha tomado algún tipo de medida para minimizar la posibilidad de fuego - Evitando Artículos inflamables en el cuarto de máquinas - Prohibiendo Fumar - Vigilando y manteniendo el sistema eléctrico - No se ha previsto		X		
8	Existe salidas de emergencia?		X		
9	En caso de salidas de emergencia estas cuentan con la señalización adecuada?			X	

10	El personal tiene el conocimiento para saber que hacer en caso de emergencia		**X**		
11	Se cuenta con medios adecuados para extinción de fuego dentro del Centro de Cómputo? Especifique			**X**	
12	Existen los suficientes carteles que recuerden las prohibiciones de fumar, consumir alimentos y bebidas dentro del Centro de Cómputo para evitar cualquier tipo de daño en los equipos?		**X**		

Anexo 2 Ref. 8-12

CUESTIONARIO DE SERVIDORES Y MINICOMPUTADORAS EN EL CENTRO DE COMPUTO

EMPRESA AUDITADA Universidad del Azuay
FECHA DE AUDITORIA 15 Marzo 2006
SUPERVISOR Fernando Zea M
AUDITOR Ma. Fernanda Marín S.

	PREGUNTAS	**SI**	**NO**	**N/A**	**OBSERVACIONES**
1	Se cuenta con un inventario de todos los equipos que forman parte del Centro de Cómputo?	**X**			
2	Con que frecuencia es revisado el inventario?			**X**	
3	Existe un control de los equipos que poseen garantía, para poder hacer uso de esta?	**X**			
4	Cuando la garantía de los equipos termina, estos pasan a formar parte de algún plan de mantenimiento?		**X**		
5	Existe servicio de mantenimiento para todos los equipos?	**X**			
6	Con que frecuencia se realiza los mantenimientos - Cada año - Cada cuatro meses (ciclo) - Otra (especifique)	**X**			No existe fecha, o período específico
7	Existen procedimientos para la adquisición de nuevos equipos?	**X**			Mejor oferta

	Describa el procedimiento				
8	Se cuenta con algún tipo de criterios de evaluación para saber el rendimiento de los equipos que se piensa adquirir y si es la mejor elección?		**X**		
9	Existen equipos que requieran características ambientales especiales? Indique el Equipo	**X**			Servidores
10	Se tiene sistemas de seguridad para evitar que se sustraiga algún equipo de las instalaciones? Cuales		**X**		
11	Existen bitácoras de fallas detectadas en los equipos?		**X**		

Anexo 2 Ref. 8-13

CUESTIONARIO DE DISTRIBUCION Y CONSTRUCCION DEL CENTRO DE COMPUTO

EMPRESA AUDITADA Universidad del Azuay
FECHA DE AUDITORIA
SUPERVISOR María Fernanda Marín S.
AUDITOR Fernando Zea M.

	PREGUNTAS	SI	NO	N/A	OBSERVACIONES
1	Las instalaciones (cubículos y oficinas) fueron diseñadas o adaptadas para funcionar como Centro de Cómputo?	**X**			
2	La distribución del espacio es adecuada, de manera que facilite el trabajo y no Exista distracciones?	**X**			
3	El espacio es suficiente para que permita una circulación fluida?	**X**			
4	Son funcionales los muebles con los que cuenta el Centro de Cómputo: archiveros, mesas de trabajo, sillas, escritorios, etc.?		**X**		
5	Existen lugares de acceso restringido?	**X**			Servidores
6	La iluminación es adecuada para el buen desarrollo del trabajo?		**X**		
7	Se cuenta con iluminación de emergencia?		**X**		
8	Existe un lugar asignado para los medios				

	de almacenamiento de información?	X			
9	Existe un lugar asignado para la papelería y utensilios de trabajo?		X		
10	Se cuenta con piso falso?		X		
11	El piso es antiestático?		X		
12	Considera usted que el Área de Trabajo no se encuentra sobresaturada?		X		
13	La limpieza de las instalaciones son adecuadas y oportunas?		X		

Anexo 2 Ref. 8-14

CUESTIONARIO DE INSTALACION ELECTRICA EN EL CENTRO DE COMPUTO

EMPRESA AUDITADA Universidad del Azuay
FECHA DE AUDITORIA 15 Marzo 2006
SUPERVISOR Fernando Zea M.
AUDITOR Ma. Fernanda Marín S.

	PREGUNTAS	**SI**	**NO**	**N/A**	**OBSERVACIONES**
1	Existe instalación con tierra física para todos los equipos?	X			
2	La instalación con tierra física es ocupada en otras partes del edificio?	X			
3	La instalación eléctrica se realizó específicamente para el Centro de Cómputo?		X		
4	La instalación eléctrica del Centro de Cómputo es independiente del resto del edificio?			X	
5	Están plenamente los cables identificados (positivo, negativo y tierra)?		X		Solamente la Instalación Eléctrica Regulada
6	Existe otro tipo de instalación eléctrica, dentro del Centro de Cómputo, que no corresponda a la alimentación de los equipos?		X		
7	La iluminación está alimentada por la misma acometida que los equipos?	X			
8	El cableado esta dentro de paneles y canales eléctricos	X			
9	Existen planos actualizados de la instalación				

	Eléctrica		**X**		
10	Se utiliza dentro del Centro de Cómputo material antiestático		**X**		
11	Se cuenta con reguladores para los equipos	**X**			
12	Existe protección contra corto circuito	**X**			
13	La acometida llega a un tablero de Distribución	**X**			
14	El tablero se encuentra visible y de fácil Acceso	**X**			
15	Se cuenta con interruptores generales	**X**			
16	Existen interruptores de emergencia	**X**			
17	Los interruptores tienen su identificación		**X**		
18	Existe algún tipo de equipo de energía auxiliar?		**X**		
19	Algunas lámparas se encuentran conectadas a la planta de emergencia del Centro de Cómputo?		**X**		

Anexo 2 Ref. 8-15

CUESTIONARIO DE SEGURIDAD DE LA RED DEL CENTRO DE COMPUTO

EMPRESA AUDITADA Universidad del Azuay
FECHA DE AUDITORIA 16 Marzo 2006
SUPERVISOR Fernando Zea M
AUDITOR Ma. Fernanda Marín S.

	PREGUNTAS	**SI**	**NO**	**N/A**	**OBSERVACIONES**
1	Existen planos de la topología del Centro de Cómputo?		**X**		
2	Existe nomenclatura para explicar el plano?			**X**	
3	Están identificados perfectamente los equipos involucrados en la red?	**X**			
4	Existen planos detallados de cada segmento de la red?		**X**		
5	Existe un procedimiento para asignar las direcciones dentro de la red?	**X**			

6	Existen inventarios de los equipos y las direcciones asociadas a cada equipo?	**X**			
7	Para el cableado de la red se siguió algún tipo de estándar? Especifique	**X**			568
8	Dentro del Centro de Cómputo existen diferentes estándares?		**X**		
9	Están definidos los protocolos que se utilizan en cada segmento de la red?	**X**			
10	Se revisa el cableado en caso de daño?	**X**			
11	Este se encuentra en zonas de acceso continuo (pasillos)?		**X**		
12	Se encuentran los cables de la red protegidos en canaletas?	**X**			
13	Los puntos de red no usados son deshabilitados o resguardados físicamente?		**X**		
14	Los usuarios(personal de sistemas) tiene diferentes passwords, sobre diferentes segmentos de la red?		**X**		

Anexo 2 Ref. 8-16

8.4 Preparación y presentación de Informes

A partir de la información obtenida por los Formularios desarrollados por los empleados del Centro de Cómputo, estos nos permiten entregar los siguientes resultados:

Seguridad de Acceso al Centro de Cómputo

Luego de un análisis estadístico de los cuestionarios, estos nos han permitido tener una visión mucho más amplia de los factores seguridad

concerniente al Acceso al Centro de Cómputo, por lo que en un gran porcentaje nos permite saber que existe la seguridad, pero no es la suficiente, ya que la persona encargada del control de acceso en primera instancia, no cuenta con un registro de visitas al Centro de Cómputo, lo que provoca grandes problemas.

Otro inconveniente es el contar solamente con una puerta que permite el ingreso al Centro de Cómputo, lo que provoca que quien visite dicho lugar, se encuentre obligado a pasar por los puestos de trabajo de los Analistas Programadores y cerca del lugar donde se encuentran los servidores, lugar que de igual manera está protegido por una puerta de madera sin las seguridades del caso.

Es necesario el indicar que la vigilancia del centro de cómputo en horarios no laborables, se encuentran a cargo de guardias de vigilancia quienes realizan sus turnos rotativos, y el conserje del edificio, el mismo que pernocta en el edificio.

Dentro del Centro de Cómputo se cuenta con censores en puertas y alarmas, pese a estas seguridades implementadas, se ha visto la falta de una persona responsable de la seguridad, es decir quien controle que todos los censores, alarmas, puertas y demás mecanismos de seguridad utilizados, se encuentren activados para evitar cualquier tipo de pérdidas tanto materiales como de información.

Anexo 1 Ref. 8-01 y Ref. 8-02

Detección de humo y fuego, extintores dentro del Centro de Cómputo

La información obtenida ha permitido el considerar este punto de gran importancia ya que la aplicación de medidas de seguridad para contrarrestar, este tipo de desastres no existe en el Centro de Cómputo.

Dentro de las instalaciones las cuales no cuentan con salida de emergencia, no existe ningún tipo de extintores para poder combatir el fuego, que puede ser de diferentes tipos; cabe recalcar que los materiales con los que han sido construidos y adecuadas las instalaciones son inflamables, lo que pone en peligro a quienes laboran y la información almacenada.

La falta de carteles que recuerden las diferentes prohibiciones tales como no fumar, no consumir alimentos, no ingerir bebidas en las instalaciones, presenta un gran problema ya que este podría ser un factor para propiciar cualquier tipo de desastre de gran envergadura.

Es necesario que se considere la instrucción del personal, para poder saber que hacer en caso de desastre, es decir se podrá conocer las medidas y las responsabilidades que cada uno de quienes trabajan tiene, en caso de presentarse algún tipo de desastre, lo que permitiría el salvar muchas vidas y salvaguardar la información, equipos, y materiales del Centro de Cómputo

Servidores y Minicomputadoras del Centro de Cómputo

Los datos con los que se cuenta luego de la aplicación de los cuestionarios, ha permitido el conocer que la seguridad implementada, no es completa ya que cumple ciertos puntos pero otros necesitan ser reforzados.

El inventario con el que cuenta el Centro de Cómputo de los servidores y minicomputadoras, no es revisado con frecuencia, provocando falta de control tanto en los equipos existentes y las nuevas adquisiciones.

Al trabajara con la vigencia de las garantías de los equipos, esto nos permite controlar los equipos existentes, sus funciones y el mantenimiento del mismo, caso contrario sucede con un equipo que su garantía ha caducado, para el cual sería necesario el trabajar con un plan o programa de

mantenimiento cuando su garantía ha caducado, lo que permitiría un mejor control del uso y estado de los equipos.
Anexo 1 Ref. 8-03 y Ref. 8-04

Distribución y Construcción del área del Centro de Cómputo

El área en la que se labora es de suma importancia ya que esta permite desempeñarse de la mejor manera, sin ningún tipo de molestias o interrupciones a quienes laboran en dicho lugar.

En el cuadro estadístico aplicado a este cuestionario, demuestra la falta de una distribución conveniente en el centro de cómputo para poder conseguir el mejor desempeño por parte de quienes laboran dentro de estas instalaciones.

Las instalaciones del Centro de Cómputo, fueron adaptadas para que funcione como tal, realizando un trabajo que ha facilitado mucho la labor de sus empleados, permitiendo fluidez para la circulación, evitando distracciones.

La funcionalidad de los muebles es beneficioso tanto para, el personal como para los equipos y los periféricos, situación que incomoda mas cuando se refiere a lugares restringidos.

La iluminación adecuada para quienes laboran en el Centro de Cómputo es sumamente importante, para poder desarrollar de mejor manera su trabajo, por lo que es necesario el contar con un suministro de energía de emergencia.

La asignación de un espacio para los medios de almacenamiento de información, permite el tener fácil acceso a la información que estos contengan, también es importante el tener un lugar adecuado para colocar la

papelería y los utensilios de trabajo, ya que esto ayudaría a mantener un orden y control de lo utilizado y las necesidades.

La falta de cielo y techo falso en un Centro de Cómputo, podría provocar el maltrato de los cables, al trabajar con piso falso este podría ser antiestático, el mismo que es beneficioso especialmente para el área del Técnico Electrónico, lugar donde se brinda el mantenimiento respectivo de los equipos.

La limpieza debe ser oportuna y adecuada, ya que se posee ciertos equipos que son muy sensibles, de esta manera se evitará que los equipos puedan sufrir daños por una limpieza inadecuada o por el polvo.
Anexo 1 Ref. 8-05, Ref. 8-06, Ref. 8-07 y Ref. 8-08

Instalación Eléctrica en el Centro de Cómputo

En referencia a este cuestionario se debe tomar en cuenta ciertos puntos a ser analizados, para poder mejorarlos, ya que los resultados obtenidos permiten apreciar, que muchos de las situaciones del ámbito eléctrico no están realizadas con la suficiente seguridad.

El contar con un plano de la instalación eléctrica del Centro de Cómputo, permitirá realizar futuros cambios sin ningún tipo de inconvenientes.

Todos los equipos del centro de cómputo cuentan con su respectiva instalación a tierra física, la misma que debe ser de uso exclusivo, al igual que la instalación eléctrica, ya que el Centro es totalmente independiente del edificio donde este funciona, es importante el indicar que no se debe compartir la misma acometida tanto para la iluminación como para los equipos.

Los cables con los que se cuenta en el centro de cómputo, deben contar con identificación necesaria, permitiendo así un mayor control en caso de emergencia.

Los paneles y canales eléctricos utilizado permite mayor seguridad, al igual que la visibilidad y el fácil acceso de los interruptores generales y de emergencia, los mismo que para su identificación deben ser etiquetados.
Anexo 1 Ref. 8-09 y Ref. 8-10

Seguridad de la Red del centro de Cómputo

La topología con la que se trabaja en el centro de cómputo debe ser especificada en un plano, el que permita conocer cada uno de los segmentos de la red, en caso de cambios tener una base para poder realizarlos, con su respectiva nomenclatura.

Por medio de un procedimiento de asignación de dirección de red, utilizado en el Cetro de cómputo, este permite el identificar los equipos involucrados en la red y con esto tener un inventario de los equipos y las direcciones asociadas a cada equipo.

La frecuencia con la que se revisa el cableado debe ser especificada y no solamente en caso de daño, para lo cual se puede implementar procedimientos de prevención.
En caso de existir puntos de red no utilizados, estos deben ser resguardados físicamente o deshabilitados, para evitar inconvenientes o daños en red, o intrusos. El trabajar con diferentes passwords, asignadas en función de las responsabilidades, minimizaría riesgos de intrusos en el sistema.

Conclusiones

Luego de concluido nuestro estudio de aplicación de controles internos de seguridad al centro de cómputo de la Universidad del Azuay, hemos determinado que no existe el debido control en lo que se refiere a seguridades internas, tanto físicas como reglamentarias; pudiendo dar como concepto "seguridad ineficiente".

En cuanto al lugar físico no existe suficiente espacio de trabajo para el personal, no existe una logística adecuada para el ingreso de personas particulares al centro de cómputo y hace falta un control total en cuanto a riesgos de trabajo (incendios, ventilación); también hace falta espacio para el archivo, suministros, refacciones, computadores en adecuación, etc.

En cuanto a la parte reglamentaria, no existe un manual interno de trabajo en el que se dictamine leyes u órdenes; que indique las responsabilidades y prohibiciones en las que se tengan que amparar los empleados y trabajadores del centro de cómputo.

Recomendaciones

Para el Centro de Cómputo de la Universidad del Azuay, podemos dar algunas recomendaciones, que se podrían tomar en cuenta para el mejor desempeño del mismo. Entre lo más importante que podríamos sugerir es que se debe tomar medidas inmediatas para mejorar el ingreso y la seguridad interna de dichas instalaciones.

En lo que respecta al espacio físico del área de trabajo, se debe readecuar la distribución de los puestos de trabajo y el área de mantenimiento, para que de ésta manera se permita un mayor orden, de igual manera se debe reorganizar todo el espacio donde se encuentran los suministros, refacciones, archivo, impresoras, etc., con muebles apropiados y necesarios para lograr este objetivo.

Recomendamos delegar un equipo de personas conocedoras del tema de riesgos de trabajo conjuntamente con autoridades de la Universidad, para que realicen un estudio y análisis de los factores de seguridad física; y de ésta manera poder implementar una política de seguridad que sirva de prevención ante peligros de trabajo, y otras situaciones propias al desarrollo de las labores que se llevan a cabo en el centro de cómputo (incendios, accidentes laborales, etc.).

Para finalizar debemos tomar en cuenta que todo ente productivo, siempre está basado en normas, leyes y reglamentos; por lo que nosotros aconsejamos emitir un reglamento interno para uso exclusivo del centro de cómputo; en el mismo que se dictamine instrucciones; que indiquen compromisos y exclusiones a las que se tendrán que acoger el personal que realiza actividades en dicho centro.

9.2 Bibliografía

- www.geocities.com/Athens/9105/audit/audi_2.html.
  CONCEPTOS BASICOS DE AUDITORIA
  ROJAS MORALES, Fernando
  [Consulta 15 Enero 2006]
- AUDITORIA INFORMATICA. Un enfoque práctico. DEL PESO, Emilio, PIATINI, Mario, Edición. Rama [s.a]
- CONTRERAS, Martínez Alejandra Diana. Sistema de seguridad en los centros de cómputo. Universidad Nacional Autónoma de México, Licenciatura en Administración, México D.F. 1995
- www.auditoriasistemas.com/auditoria_de_sistemas.htm
  Auditoria de Sistemas
  [Fecha de Ingreso 6 de diciembre de 2005]
- www.adacsi.org.ar/modules.php?name=Content&pa=showpage&pid=15
  [Fecha de Ingreso 6 de Diciembre de 2005]
- Guía Avanzada Administración de Sistemas Linux,
  CARLING. M, DEGLER, STEPHEN. DENNIS JAMES. Prentice Hall Iberia, Madrid, 1999.
- http://www.minfin.gob.gt/politicas/a13.htm Guía para pruebas de Áreas de Cómputo [Fecha de ingreso 18 de Diciembre de 2005]
- **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
- http://cert.salud.gob.mx/Controldeacceso.html
  Control de Acceso.
  [Fecha de Ingreso 18 de Febrero de 2006]
- Especificaciones Técnicas dictadas por el Departamento de Auditoría Informática, Subdirección de Sistemas-DCAA-UNAM Julio 2003
- www.auditoriasistemas.com/politicas_de_seguridad.htm
  Auditoria de Sistemas
  [Fecha de Ingreso Diciembre 6 de 2005]

Anexo 1

Acceso al Centro de Cómputo

Ref. 8-01 Puerta Exterior

Ref. 8-02 Puerta de Acceso Interno

Minicomputadoras y Servidores

Ref. 8-03 Servidor Principal Secundarios

Ref. 8-04 Servidores

Distribución del Espacio en el Centro de Cómputo

Ref. 8-05 Pasillo de Ingreso

Ref. 8-06 Área de Trabajo
Analistas I, II y III

Ref. 8-07 Área de Trabajo
Técnico Electrónico

Ref. 8-08 Área Trabajo
Técnico Electrónico

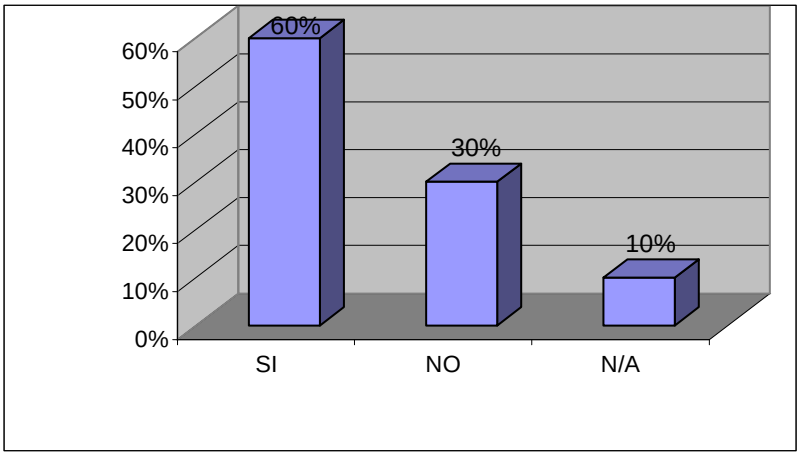
Instalación Eléctrica en el Centro de Cómputo

Ref. 8-09 Tablero de Acometida Eléctrica

Ref. 8-10 Tomas Eléctricas

Anexo 2

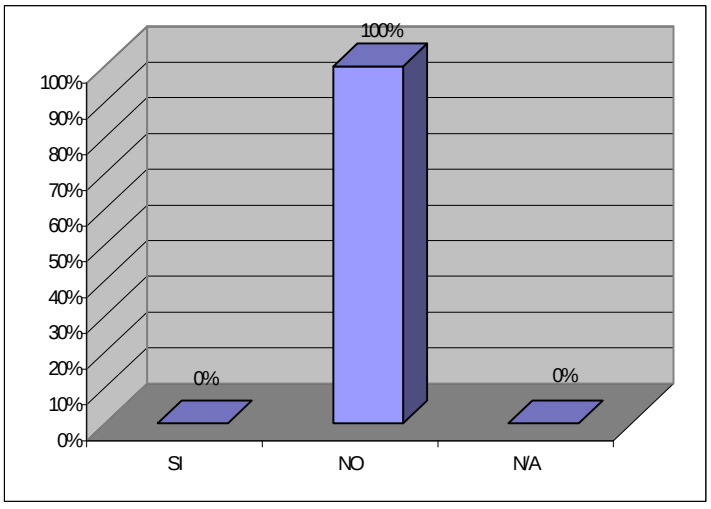
SEGURIDAD DE AUTORIZACION DE ACCESOS AL CENTRO DE COMPUTO



Ref. 8-11

Este cuadro permite el apreciar, que la seguridad existente en el Centro de Cómputo no es completa y puede ser violada, además de que existen ciertas medidas que no se han aplicado para poder tener mayor control en el Acceso a las instalaciones

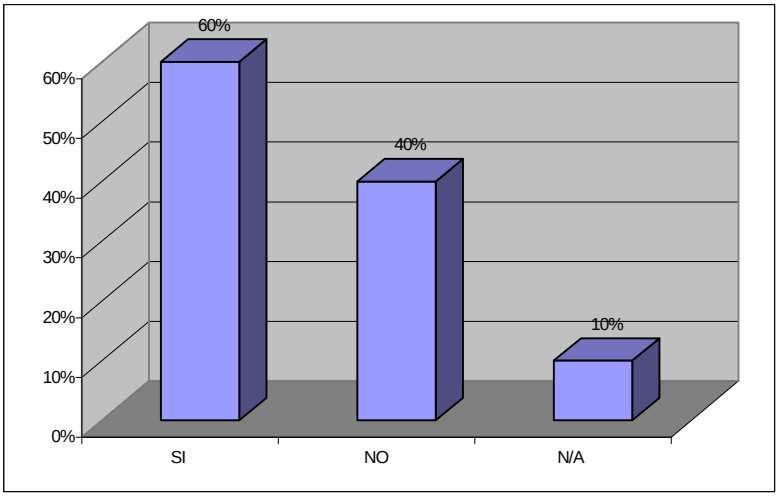
DETECCION DE HUMO Y FUEGO, EXTINTORES DENTRO DEL CENTRO DE COMPUTO



Ref. 8-12

El cuadro, demuestra la inexistencia de medidas a ser tomadas, para prevenir desastres provocados por fuego, y en otros casos la falta de estas medidas, sugiera que ciertos aspectos de control no son aplicados.

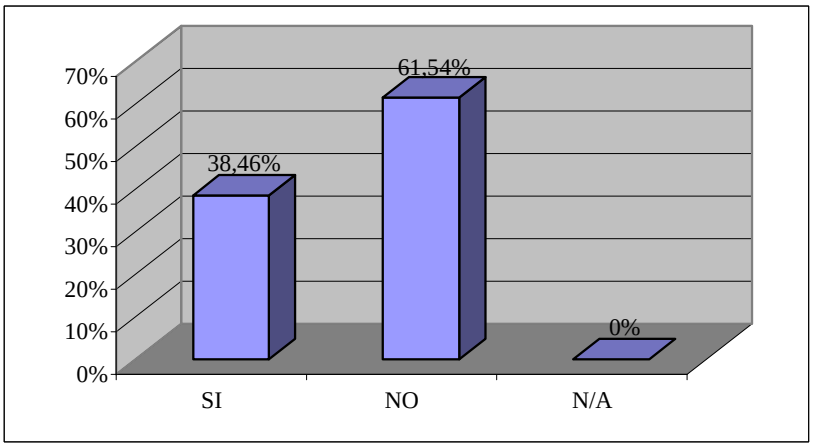
SEGURIDAD DE LAS MINICOMPUTADORAS Y SERVIDORES DEL CENTRO DE COMPUTO



Ref. 8-13

El cuadro permite comprender que la seguridad implementada en las minicomputadoras y servidores no es suficiente ni la más efectiva.

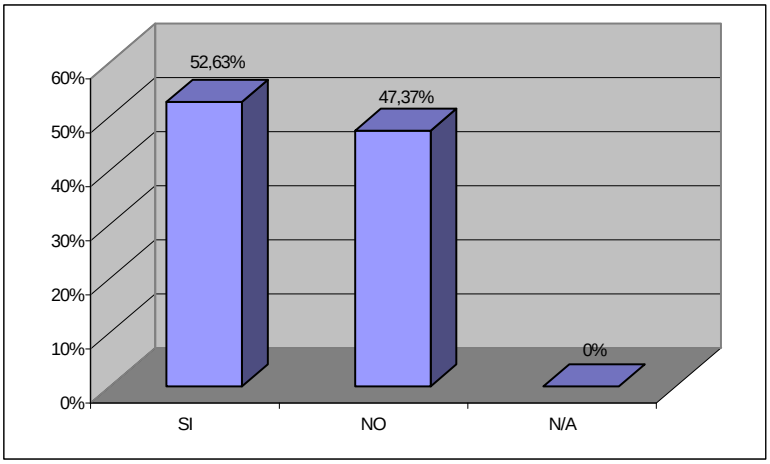
DISTRIBUCION DEL ESPACIO EN EL AREA DEL CENTRO DE COMPUTO



Ref. 8-14

El cuadro permite comprender que las instalaciones donde funciona el Centro de Cómputo no cumple con todas las facilidades para poder trabajar de una mejor manera, lo que complica el desempeño del personal

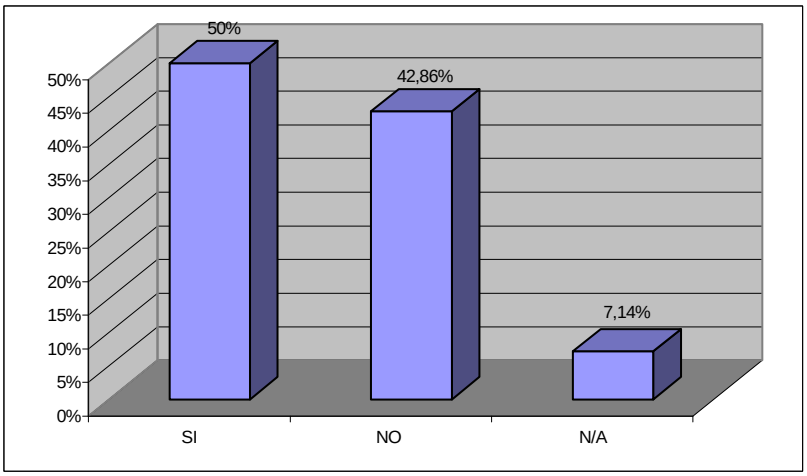
INSTALACION ELECTRICA EN EL CENTRO DE COMPUTO



Ref. 8-15

La instalación eléctrica, pretende cumplir con las normas exigidas, pero aun presentan problemas ya que los problemas se encuentran a la par con las soluciones

SEGURIDAD DE LA RED DEL CENTRO DE COMPUTO



Ref. 8-16

La red, no cuenta con toda la seguridad requerida por lo que, es necesario el implementar normas que ofrezcan las seguridades necesarias