Centro de tecnología computacional para el grupo la asunción

Autor: Gonzalo Rodríguez Zapién

Tesis presentada para obtener el título de:
Lic. En Sistemas computarizados [sic]

Nombre del asesor:
Sergio Francisco Barraza Ibarra

UNIVERSIDAD VASCO DE QUIROGA

ESCUELA DE SISTEMAS COMPUTARIZADOS

CENTRO DE TECNOLOGÍA COMPUTACIONAL PARA EL GRUPO LA ASUNCION

TESIS
QUE PARA OBTENER EL TÍTULO DE:
LICENCIADO EN SISTEMAS COMPUTARIZADOS

PRESENTA:
GONZALO RODRÍGUEZ ZAPIÉN

No. DE ACUERDO 952006 **CLAVE 16PSU0014Q**

ASESOR:
ING. Y M. A. SERGIO FRANCISCO BARRAZA IBARRA

MORELIA, MICHOACÁN **DICIEMBRE 2003.**

CON AGRADECIMIENTO:

A Dios por ser la luz en todo mi camino.

A mi mamá por su apoyo con amor, dedicación y paciencia, Incondicional durante mis estudios.

A mi papá por el ánimo con el que siempre me alienta a ser mejor cada día

A mis Hermanos, Nancy y Luis Fernando por creer en mi y brindarme toda su confianza

Al Ingeniero Barraza, por instruirme en cada momento, Para adquirir los elementos necesarios para triunfar en mi profesión

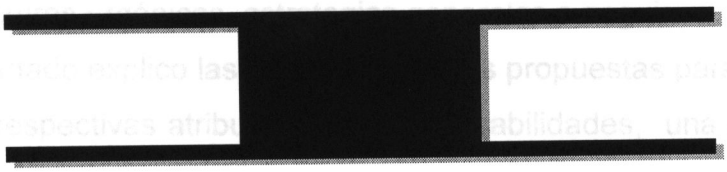
A todos los profesores que me brindaron sus conocimientos, técnicas y consejos, en especial al Ing. Víctor Pineda que más que un maestro es un amigo.

A Laura el amor de mi vida, por su cariño, confianza y apoyo en todo momento para cumplir esta meta.

Al C.P. Francisco Chávez por todo el apoyo que me ha brindado para realizar mis metas y sueños.

"No Dejes Que Nada Ni Nadie Robe Tus Sueños"

INDICE



INTRODUCCIÓN

I. INTRODUCCIÓN

El presente trabajo está integrado por 10 capítulos que comprenden desde los objetivos hasta las conclusiones y recomendaciones.

En el primer capitulo hago referencia a los objetivos que tiene la tesis como trabajo de investigación, la definición general de un centro cómputo, una estructura formal y 2 tipos de estructuras orgánicas, estrategias generales a seguir.

En el segundo apartado explico las áreas funcionales propuestas para el centro de cómputo con sus respectivas atribuciones y responsabilidades, una explicación a detalle y funcional,

El tercer capítulo analiza de manera profunda las consideraciones generales para el centro de cómputo de manera técnica como la selección del área, selección del lugar y así hasta llegar a las consideraciones para el lugar en donde se encontrarán los servidores y granjas de almacenamiento.

En el capitulo cuarto se trata de manera mas detallada el objeto de diseño del centro de cómputo que considera la normativa aplicable para la instalación, la ejecución de un proyecto técnico, del cableado, de los cuartos estratégicos hasta la climatización.

En cuanto a la seguridad informática se menciona en el capítulo V, y en este apartado se describe de manera analítica los elementos técnicos y administrativos a cerca de la seguridad informática tal como las políticas de seguridad, cuantificaciones, clasificación, organización y división de responsabilidades, la seguridad contra incendios, y las alternativas para hacer frente a un desastre o perdida de la información confidencial de la organización.

Debido a la gran cantidad de información a cerca de la seguridad Informática se habla en el capítulo seis a cerca de la seguridad física y contra incendios detallando los planes de contingencia, diagramas de operación para una recuperación y los alcances de los procedimientos en casos de desastres.

Para llegar a los resultados sobre una plataforma confiable de seguridad se habla en el capítulo siete de una aplicación efectiva de la organización por medio del comité de informática de todos los elementos administrativo-informáticos, licitaciones, acciones de desarrollo y la definición de proyectos comunes.

Sobre la completa organización de la organización y mas aún en el área de informática hago mención en el capitulo ocho sobre la auditoría informática que habla a cerca de los lineamientos y procedimientos de una auditoría así como los perfiles requeridos para completar el trabajo de auditoria, las observaciones, las responsabilidades fincadas y el seguimiento de corrección.

Finalmente en el último apartado (Capítulo nueve) se encuentra un ejemplo básico de las políticas y reglamentos que se pueden aplicar a cualquier centro de cómputo, y establece las funciones y atribuciones para los usuarios, el equipo y el área en general de informática

1.1 Objetivo General

La presente investigación establece los lineamientos aplicables al entorno de trabajo para la empresa, organización, entidad, y/o dependencia con el fin de eficientar y conducir al establecimiento y mejoramiento de políticas, sistemas de organización, implantación y capacitación para elevar al máximo la potencia informática y garantizar la operatividad así como el buen funcionamiento, logrando el cumplimiento efectivo y eficiente de las metas del área Informática y mas aún de la organización.

1.2 Objetivos Particulares

- Descubrir la estructura orgánica de un centro de cómputo, fases, ampliaciones y adecuaciones a la organización.

- Resaltar las actividades principales de las áreas funcionales que componen el centro de cómputo

- Identificar los elementos a considerar para el diseño del centro de cómputo, requerimientos técnicos y humanos.

- Establecer lineamientos, reglamentos y políticas informáticas para el funcionamiento óptimo del centro de cómputo.

- Automatizar los requerimientos de información de las áreas dentro de la empresa que necesitan ser satisfechas por el desarrollo de sistemas o del procesamiento de datos correspondientes a otras áreas.

- Justificar las medidas de control en cuanto al costo.

- El logro del compromiso organizacional con la política de seguridad.

- La división y organización de responsabilidades para hacer frente a cualquier adversidad o peligro.

- El establecimiento de un comité de informática para definir proyectos prioritarios, diseño e implementación de instrumentos concertados de políticas.

- La auditoria informática como la revisión y examen sistemático de una actividad o actividades que realiza personal independiente, de la operación dentro de una organización. La Auditoría es de apoyo a la función directiva.

- Obtener y seguir al pié un reglamento de políticas y reglamentos para delimitar funciones y atribuciones acotadas a los trabajadores y usuarios de la organización.

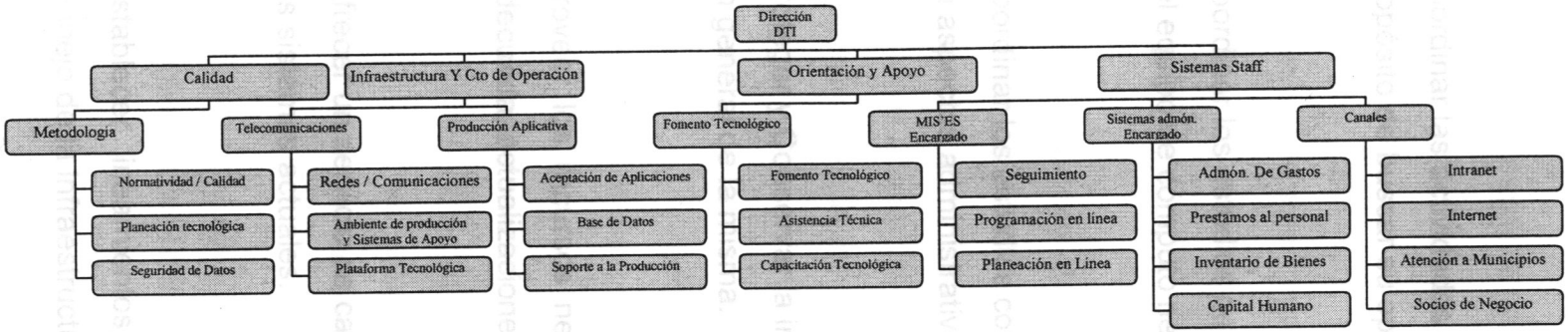
1.3 Centro De Cómputo

Es la entidad dentro de la organización que tiene la finalidad de satisfacer las necesidades de información de la empresa, de manera veraz y oportuna.

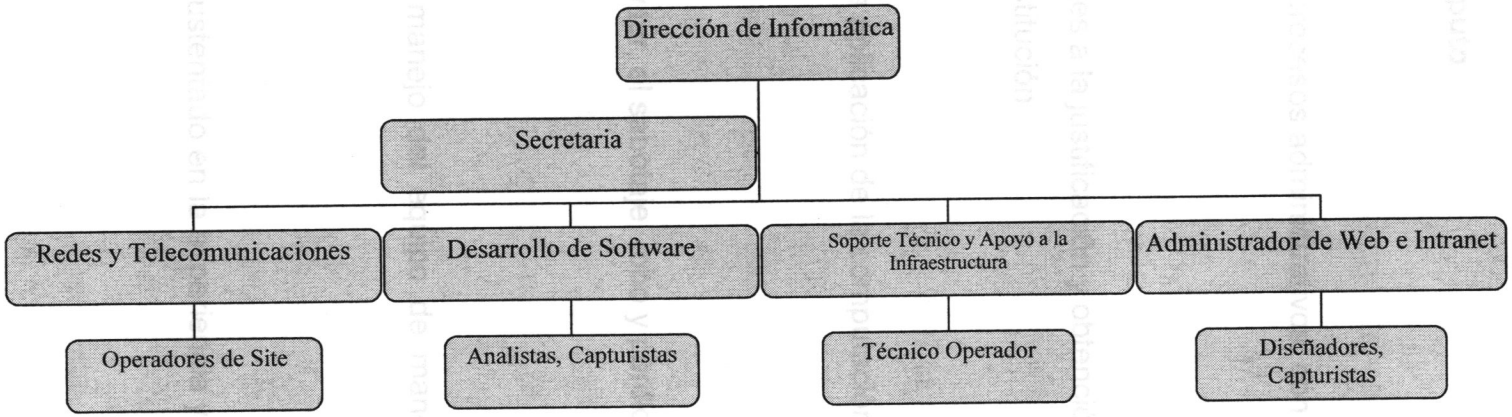
Es la unidad responsable de centralizar, custodiar, y procesar la mayoría de los datos con los que opera la organización.

Sistema de Información es un conjunto de componentes interrelacionados que permiten capturar, procesar, almacenar y distribuir la información para apoyar la toma de decisiones y el control en una institución. Además, para apoyar a la toma de las decisiones, la coordinación y el control, los sistemas de información pueden también ayudar a los administradores y al personal a analizar problemas, visualizar cuestiones complejas y crear nuevas soluciones para satisfacer las necesidades..

1.4 Estructura Ideal Propuesta Para Un Centro De Cómputo.



1.4.1 Estructura Real Para Un Centro de Cómputo Actual.



1.5 Objetivos Sugeridos Para El Centro De Cómputo

1. Coordinar las actividades de análisis en los procesos administrativos, con el propósito de buscar su optimización.

2. Coordinar los estudios de viabilidad tendientes a la justificación y obtención del equipo de cómputo necesario para la Institución.

3. Coordinar los estudios correspondientes a la aplicación de la computación en aspectos administrativos.

4. Proteger y Conservar la información para evitar, el sabotaje, robo y pérdida en general de la misma.

5. Proveer los recursos necesarios para el manejo del equipo de manera adecuada, actualizaciones, Intranet etc....

6. Ofrecer un servicio de calidad informática sustentado en la experiencia y en los sistemas actuales.

7. Establecer lineamientos, políticas, procedimientos, reglamentos para el manejo de la infraestructura actual y futura.

1.6 ESTRATEGIAS GENERALES

Como primeros pasos y para dar soporte estructural al área de Tecnología Informática:

- Tener una estructura de sistemas con responsabilidades acotadas y orientadas a la solución de diferentes problemas.

- Metodología de desarrollo de sistemas.

- Establecer comités de negocio para presentar avance de las iniciativas a atender por sistemas.

- Establecer reunión Ínter staff de sistemas para conocer las necesidades en procesamiento de las diferentes iniciativas de negocio.

- Establecer y normar técnicamente la figura de especialistas de sistemas asignados a direcciones regionales, para descansar en ellos la responsabilidad de atención regional.

Una vez resuelta la estructura de trabajo:

- Realizar un proceso de Planeación Tecnológica, orientado a las necesidades sentidas de la organización a través de los ejecutivos.

- Establecer los objetivos claros y medibles por cada área en base anual, con seguimiento semestral, alineado a los procesos de planeación

DESCRIPCIÓN DEL

ORGANIGRAMA

ESTRUCTURAL Y FUNCIONAL

II. DESCRIPCIÓN DEL ORGANIGRAMA ESTRUCTURAL Y FUNCIONAL

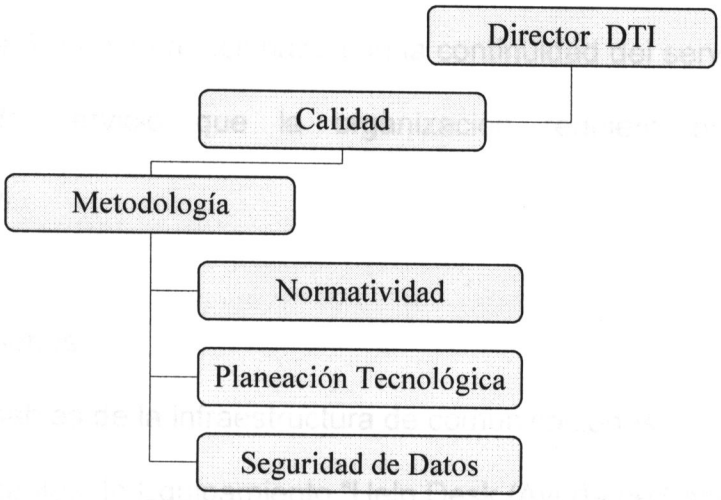
2.1 Calidad

El área de **Calidad,** es una figura muy importante en la organización, cuyo objetivo es el establecimiento de estándares, manuales de procedimientos, reglamentos; su difusión y normalización, así como revisar el cumplimiento en las áreas cuya importancia amerite el uso de los mismos. El éxito del área de calidad es la combinación del éxito de las áreas de infraestructura y desarrollo. Por tanto el establecimiento de una **metodología** es algo básico para el área de sistemas, así como el establecimiento de niveles de servicio, en el que participen usuarios, responsables aplicativos y producción. Por lo anterior, la coordinación y seguimiento a las observaciones de normativa, serán también responsabilidad de esta área.

La seguridad de datos, que debido a la transparencia que debe presentar será también una función de esta área, logrando un control de los recursos del organismo a través de este medio.

La planeación tecnológica, engarza en esta función, debido a la necesidad de dar congruencia a las necesidades identificadas por cada una de las áreas de la Dirección de Tecnología Informática. (DTI en Adelante) Para Definir y Administrar una herramienta de control de versiones para aplicar la liberación de modificaciones y aplicaciones en programas y documentación así como del seguimiento y métricas de los problemas reportados tanto a infraestructura como a orientación.

2.1.1 Estructura propuesta para el área de calidad



2.2.- Infraestructura y centro de operaciones

El área de Infraestructura y Centro de Operaciones, es el soporte de operaciones del organismo, ya que es responsable del buen funcionamiento de las comunicaciones, Hardware y Software.

El éxito de esta área está relacionado con la continuidad del servicio, así como de los niveles de servicio que la organización requiere para su correcto funcionamiento.

Telecomunicaciones

Responsables de la infraestructura de comunicaciones

Responsables de Equipamiento "Help Desk (Ayuda de Escritorio) "

Responsable de la operatividad de los equipos propiedad de la Institución;

Por su alcance y complejidad se divide en tres principales ramas:

1).-Redes y Comunicaciones.

2).-Ambientes de producción y sistemas de apoyo y

3).- Plataforma tecnológica (Microsoft, Pc´s etc.)

Producción Aplicativa

Responsable de Definir los criterios para recibir aplicaciones

Responsable de Validar que las aplicaciones cumplan con los estándares así como con la documentación correspondiente y los Procesos de recuperación y contingencia

Bases de Datos

Responsable de definir los estándares en el manejo de bases de datos

Responsables de Garantizar la consistencia en el diseño, así como evitar redundancia de información.

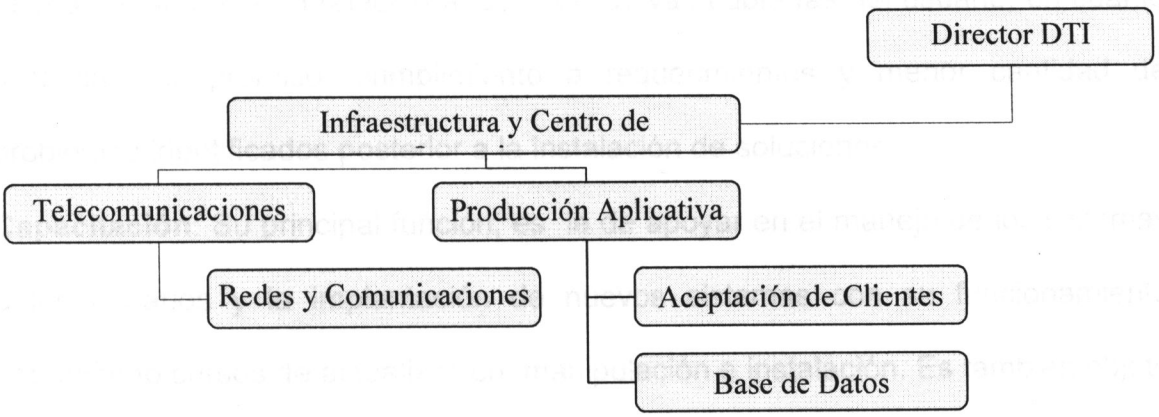
Responsable de revisar el cumplimiento de los diversos desarrollos a estas normas y estándares.

Soporte a la Producción

Encargados de Ejecutar los procesos liberados a producción, así como de aplicar los procesos de recuperación y contingencia.

Resolver problemas de primer nivel, para los problemas reportados.

2.2.1 Estructura propuesta para el área de infraestructura y centro de operaciones

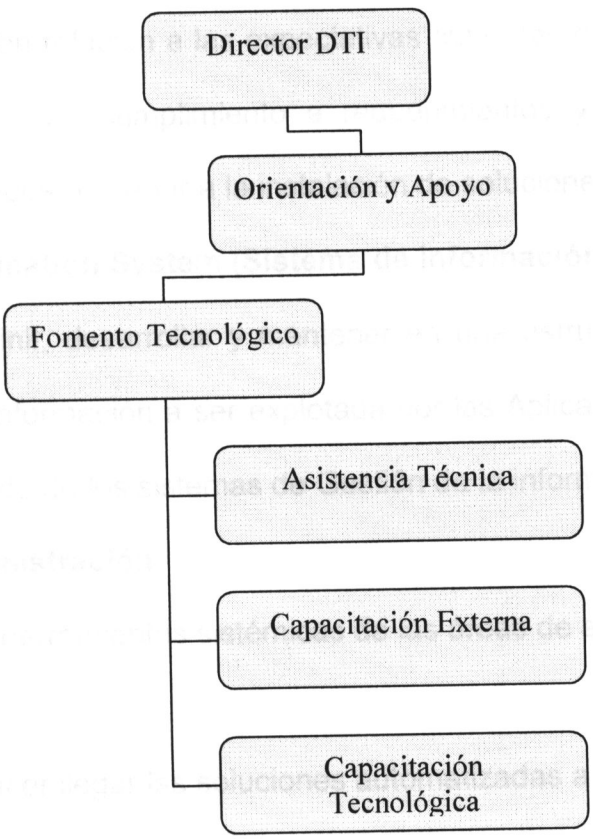


2.3 Orientación y Apoyo

El área de **orientación y apoyo**, tiene como objetivo el atender las necesidades de desarrollos informáticos para las entidades, direcciones y departamentos para la correcta aplicación de los sistemas optimizando el desempeño de sus funciones Esta área, se mide en relación a las expectativas cubiertas del usuario, en cuanto a fechas compromiso, cumplimiento a requerimientos y menor cantidad de problemas identificados posterior a la instalación de soluciones.

Capacitación: Su principal función, es la de apoyar en el manejo de los sistemas a los usuarios y la implantación de nuevos sistemas con su funcionamiento impartiendo cursos de actualización, manipulación e instalación. Es también objeto de ejercer la asistencia técnica en caso de cualquier anomalía en el funcionamiento de los sistemas.

2.3.1 Estructura propuesta para el área de orientación y apoyo



2.4 Sistemas Staff

El área de sistemas STAFF tiene como objetivo el atender las necesidades de Desarrollos informáticos para lograr la administración y explotación de la Información de la organización, así como desarrollar las soluciones requeridas para el control y administración de la misma.

Esta área, se mide en relación a las expectativas cubiertas del usuario, en cuanto a Fechas compromiso, cumplimiento a requerimientos y menor cantidad de problemas Identificados posterior a la instalación de soluciones.

Management Information System (Sistema de información Gerencial)

Encargados de definir, desarrollar y mantener en una estructura de Datos, tipo datawarehouse la información a ser explotada por las Aplicaciones de gestión del organismo encargado de los sistemas de Gestión de la información.

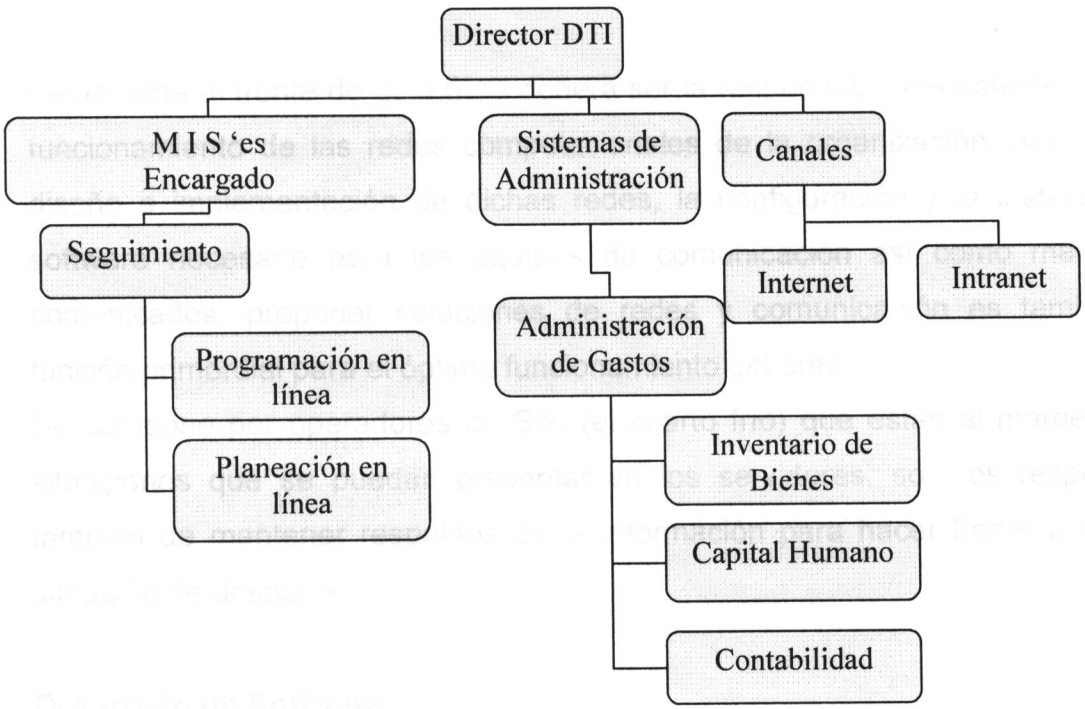
Sistemas de Administración

Encargados de las herramientas sistémicas de las áreas de apoyo

Canales

Responsable de hacer llegar las soluciones automatizadas a los usuarios finales.

2.4.1 Estructura propuesta para el área STAFF



2.5 Descripción del organigrama funcional y estructural aplicado a un centro de cómputo real y actual

Redes y Telecomunicaciones.

La persona al frente de esta área deberá ser la responsable del establecimiento y funcionamiento de las redes computacionales de la organización, así como del diseño e implementación de dichas redes, la configuración y la instalación del software necesario para los equipos de comunicación así como mantenerlos comunicados, proponer soluciones de redes y comunicación es también una función primordial para el óptimo funcionamiento del área.

Se compone por operadores de Site (el cuarto frío) que están al margen de las situaciones que se puedan presentar en los servidores, son los responsables también de mantener respaldos de la información para hacer frente a cualquier situación de desastre.

Desarrollo de Software

El encargado de esta área es el responsable de la elaboración y mantenimiento de los sistemas que operan dentro de la Organización, así como los ya establecidos como el mantenimiento de paquetería comercial, debe tener la habilidad también de interpretar las necesidades de los usuarios para confeccionar las soluciones pertinentes, elabora también el personal dentro de esta área, todos los estudios para la elección y adquisición de software necesario; así como investigar y probar nuevos productos.

Dentro de esta área también laboran capturistas y analistas que son los encargados de la elaboración escrita de los manuales de software, captura de líneas de programación etc.

Soporte Técnico y Apoyo a la Infraestructura.

El jefe de ésta área será el encargado de instalar y mantener el sistema operativo, configurar el software comercial y aplicado, tendrá la habilidad de detectar fallas y llegar a su corrección, se encargará del buen rendimiento del equipo con el que cuenta la organización, configura por 2ª vez las opciones de red como protocolos, direcciones etc. Instala software y repara fallas de hardware.
Esta área se podrá apoyar en las personas de servicio social, operadores técnicos que tengan el conocimiento básico para las funciones diarias del departamento.

Administrador de Web e Intranet

El responsable de esta área deberá contar con los conocimientos necesarios en lenguajes de programación de tipo Web, servidores y bases de datos para el diseño de una plantilla de personal (Capital Humano) por medio de la Web interna (Intranet) animaciones para el diseño de la página de Internet oficial, el diseño de presentaciones, será el responsable también de mantener actualizados los sistemas de ambiente Web.

Secretaria

Es la encargada de auxiliar en los procesos administrativos del área de informática, controla las operaciones de mensajeria, elabora y recibe pedidos, correspondencia, memorandums, faxes, oficios y documentos en general, será la encargada de recibir y contestar las llamadas telefónicas, organiza y mantiene en óptimas condiciones el archivo.

III

ANÁLISIS GENERAL PARA EL CENTRO DE CÓMPUTO

III. ANALISIS GENERAL PARA EL CENTRO DE CÓMPUTO

Por lo anterior, se ven diferentes áreas de oportunidad a cubrir

- Homogeneidad en las plataformas tecnológicas, considerando un incremento en los volúmenes de operación.
- Mecanismos de medición al cumplimiento de las expectativas generadas en los usuarios
- Metodología que haga homogéneo el desarrollo y permita buenas estimaciones de los esfuerzos necesarios para atender los proyectos y requerimientos de nuevas funcionalidades.
- Servicio diferenciado a las áreas de negocio, considerando un enfoque especial al riesgo y al tratamiento integral de los clientes y sus relaciones con la institución.
- Evitar dependencias tecnológicas y humanas, orientando la capacitación del personal.
- Estrategias de redundancia en equipos y aplicaciones.
- Orientar los esfuerzos de forma ordenada.

3.1 Selección del área

El área de sistemas debe en la organización tener múltiples parámetros para su edificación, los cuales aseguran el buen funcionamiento, la confiabilidad y la veracidad de la información si se cumplen al margen de la exigencia de los sistemas; dichos parámetros son: la definición de políticas de seguridad, la organización y la división de responsabilidades. El óptimo desempeño de un Centro de cómputo depende básicamente de una buena planeación en su construcción.

Entre los principales factores a considerar en la planeación de las instalaciones físicas se encuentran los siguientes:

3.2 Preparación del plano de distribución, consideraciones generales.

-Flujo eficiente de trabajo.
-Cercanía de Áreas Interactuantes
- Flujo de trabajo sin retrocesos
- No interferencia del tránsito de personas con el procesamiento
- Cercanía del personal a recursos (consumibles, archivos, equipo,...) de uso frecuente.
- Áreas de almacenamiento/recepción adecuadas
- De consumibles (papel, cintas, disquetes)
- De equipo
- De material de desecho
- Puertas y corredores amplios
- Minimizar las puertas, ventanas y obstrucciones
- Dos salidas en cada área que contenga personal
- Tomas de corriente suficientes y convenientemente localizadas
- Espacio adecuado para mobiliario, equipo y material

- Distribución adecuada de teléfonos
- Áreas que faciliten la observación
- Área para alimentos
- Sanitarios suficientes
- Facilidad de guardarropa
- Espacio para unidad de aire acondicionado y equipo eléctrico
- Posibilidad de modificación y expansión
- Apariencia atractiva

3.4 Selección del área general

- Cercanía de usuarios
- Cercanía de configuración de respaldo
- Corriente eléctrica confiable
- Comunicación confiable
- Vía rápida de acceso
- Evitar zonas con incidencia de desastres naturales
- Evitar zonas propensas a disturbios sociales
- Cercanía de Policía y Bomberos
- Rentas atractivas
- Sistema escolar y servicios comunitarios

3.5 Selección del lugar especifico

- Elevado
- Minimizar el efecto de lluvias
- Evitar la proximidad de aeropuertos
- Evitar Interferencia electromagnética
- Separación de vía rápida
- Transporte comercial cercano
- Estacionamiento

3.6 Selección del edificio especifico

Espacio adecuado:

- Para planta eléctrica de respaldo
- Para sistema de aire acondicionado
- Puertas y pasillos amplios
- Lejanía de inflamables y explosivos
- Control de acceso
- Área para visitas
- Área de comida y Sanitarios
- No más allá de un sexto piso

3.7 Consideraciones especificas para el Site

Espacio adecuado para:

- Operación y Mantenimiento de Equipo
- Mesas de trabajo y/o de transporte
- Gabinetes de almacenamiento
- Almacenamiento/Colocación temporal de discos, cintas y material impreso
- Equipo de pruebas y personal de mantenimiento
- Cables dentro de especificaciones (eléctricos y de datos)
- Panel de control eléctrico accesible y seguro
- Alternar equipo ruidoso con silencioso

3.8 Requerimientos ambientales

- Piso Falso
- Conducción de cables (eléctricos y de datos)
- Inyección de aire acondicionado
- Resguardo de inundaciones
- Características
- Resistente a electricidad estática
- Facilidad de mantenimiento

- Durabilidad
- Apariencia
- Costo
- 40 CMS de elevación
- Soportar Carga (piso falso y piso firme)
- Falso Plafón
- Cableado aéreo
- Extracción de aire (flujo)
- Conductos (canaletas) externos para cableado.
- Temperatura: rango ideal 18 --> 22 C. No es recomendable operar abajo de 10 C ni arriba de 30 C
- Humedad relativa: 50 +- 10 % para evitar tanto condensación como electricidad estática. No es recomendable operar arriba de 80% ni abajo de 20%.

3.9 Requerimientos de suministro eléctrico

- Reguladores

Suministran voltaje estable a los equipos

- UPS (Sistema no interrumpible de potencia)

Suministran energía eléctrica constante al equipo, soportados por un banco de baterías con una duración nominal de X mins. Existen "On line" y "Stand by" el tiempo de respuesta en caso de apagón es de milisegundos (cero segundos)

- Planta Eléctrica

Generador electromecánico de energía, trabaja en base a algún combustible, su tiempo de respuesta es de segundos. Pueden funcionar en periodos prolongados de tiempo.

- Tierra Física

Instalación eléctrica que permite absorber descargar eléctricas, conformada por 1 varilla de cobre de 3 mts enterrada bajo el nivel del suelo y de preferencia en un lugar con humedad, complementada con sales y carbón para mejorar asimilación de descargas.

NO ES CONVENIENTE usar castillos del edificio, ni tuberías.

3.10 Otros requerimientos

- Minimizar vibraciones, disturbios electromagnéticos y ruido
- Procurar iluminación y atmósfera adecuada para el personal
- Recubrimientos acústicos
- Interruptores seccionales de luz
- Evitar luz solar directa

Para el centro de computo se planeo también una bodega, en la cual se almacenan Consumibles, Memorias, Software, Periféricos con un total de 5 x 4 Mts^2 de extensión total[1]

Site:

- 1 Enlace Spread Spectrum a 3 Mbps
- 2 Enrutador esCisco 3640 con descanalizador.
- 1 Enrutador/comm. server Cisco 2509
- 2 Enrutador/comm. server Cisco 2511
- 9 Enrutadores Cisco 1601.
- 1 Administrador de ancho de banda Packetshaper 2500
- 1 Cache Flow 625 CA.

[1] FIRA- Banco de México. 2003.

OBJETO DE DISEÑO

IV. OBJETO DE DISEÑO

El objeto es establecer los requerimientos funcionales y técnicos mínimos para la implantación de las instalaciones que requieren de una red de transmisión para su funcionamiento. En particular se consideran las instalaciones que proporcionan los siguientes servicios:

- Servicio de telefonía (incluye intercomunicación, busca personas, pase/espere de consultas externas y megafonía general)
- Servicio de transmisión y comunicación de datos
- Servicio de televisión
- Servicio de control de accesos, control de intrusión, control de presencia y vídeo vigilancia
- Servicio de megafonía y vídeo proyección en salón de actos y aulas de formación
- Servicio de sincronización horaria de todas las instalaciones

Quedan fuera del ámbito del presente artículo (por tratarse de instalaciones singulares desde el punto de vista legal que no técnico):

- Servicio de gestión técnica del edificio
- Servicio de control de incendios

4.1 Normativa a tener en cuenta

Para la implantación de los servicios que se abordan (por razones técnicas, de seguridad contra incendios, compatibilidad electromagnética, y confidencialidad), debería ser de obligado cumplimiento en México la siguiente normativa:

- Reglamento de Baja Tensión
- Cableado estructurado de propósito general
- Tecnología de Información - Redes de área local y metropolitana y actualizaciones para las diferentes técnicas de señalización
- Control de Protección de Incendios
- Normativa sobre compatibilidad electromagnética
- Reglamento de protección de datos

Otra normativa a considerar (por razones técnicas) es:

- Cableado de telecomunicaciones para edificios comerciales
- Cableado estructurado de propósito general
- Canalización y zonas para equipos de telecomunicación en edificios comerciales
- Especificaciones adicionales sobre cable UTP
- Especificaciones adicionales sobre cable UTP
- Cableado de instalaciones con fibra óptica

En el proceso de evaluación de alternativas, se tenderá a maximizar la siguiente expresión:

Eficiencia=Prestaciones/Costo _ generalizado

4.2 Ejecución del proyecto técnico

El proyecto de ejecución se debe redactar asumiendo como filosofía general, que este tipo de instalaciones deben incorporar los siguientes principios:

- Toda instalación tiene que ser gestionable.
- Los servicios se deben poder conceder o retirar con criterios administrativos y nunca por restricciones técnicas.
- Los elementos de control y gestión de las diferentes instalaciones (salvo la vídeo-proyección que es una instalación específica de locales concretos) deben estar concentrados en un único local, de acceso físico controlado, siendo posible su gestión desde dicho local o desde cualquier otro, con tal que se disponga de autorización suficiente.
- Los servidores que alojan la información de los diferentes subsistemas de información, que de forma integrada constituyen el sistema de información de la Organización (tanto de su actividad como del propio edificio), deben estar alojados en un único local con acceso físico controlado.
- Las redes de cableado necesarias para soportar las instalaciones descritas, deberán compartir la misma canalización principal, siempre que sean eléctricamente compatibles entre sí.
- La topología física de las redes de transmisión a través de las cuales se soportan los diferentes servicios, será una estrella distribuida. Por tanto obedece a una estructura jerárquica, en la que partiendo de un repartidor principal (en adelante RP) se distribuye radialmente a los repartidores satélites (en adelante RS) y desde éstos, radialmente a los Puntos de Acceso a la Red de Transmisión en el edificio (PUERTA). No se debrá permitir ninguna conexión entre RSs sin pasar por el RP, con el fin de eliminar bucles por diseño.

- La estabilidad de funcionamiento de los diferentes servicios se resolverá por diseño mediante las condiciones de contexto (estabilidad térmica y eléctrica) de la electrónica que soporta cada servicio, o mediante protocolos de supervisión de enlace, pero nunca por redundancia de electrónica que aumente desmesuradamente la complejidad de la gestión y funcionamiento de los mismos. En este sentido estas instalaciones no son distintas de cualesquiera otras, por más que no estén consolidadas aún en la cultura tecnológica actual.

La red de transmisión electrónica necesaria para soportar los diferentes servicios, es infraestructura de edificio al igual que la red de climatización o la red eléctrica y no de organización (personas que lo ocupan), por tanto para su diseño se recomienda usar el mismo criterio que para el resto de instalaciones:

En la realización del diseño se recomienda usar un modelo que considere las siguientes variables:

- Inventario de locales (planos de arquitectura + mobiliario)
- Tipo de local (despacho, Bóveda, consulta, etc.)
- Inventario de servicios necesarios en cada punto, para cada tipo de local
- Densidad de puntos por unidad de superficie para cada tipo de local

En este contexto, punto se refiere a Punto de Entrada a la Red de Transmisión Activa (en adelante PUERTA) y no a los conectores individuales (rosetas).

La topología de las diferentes redes de cableado desde los Puertas (voz, datos, TV, tierra de datos, etc.) será radial hasta los RSs y desde estos, radial hasta el RP, no estando permitido realizar ningún empalme en los conductores que se usen para su ejecución.

4.3 Ejecución del cableado

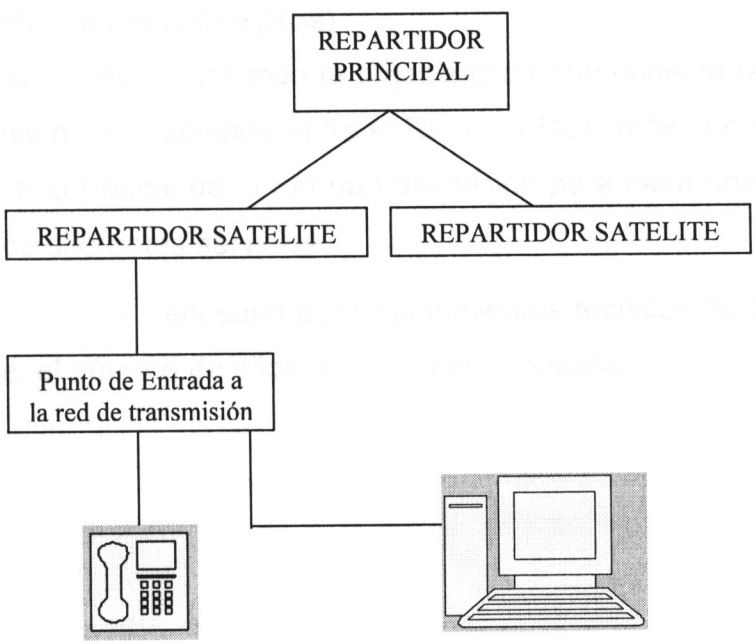
Se deberá utilizar tecnología de cableado integral estructurado para la ejecución de las diferentes redes que se abordan.

Para unir el PUERTAs con el RS, se usarán tantos mazos de cable distintos, como técnicas de señalización para las que se incorpore conector. El número de mazos depende de la configuración del PUERTA, siendo el caso general (ejemplo):

- 1 mazo de 4 pares de cobre de categoría 5 ampliada no apantallado para voz
- 2 mazos de 4 pares de cobre de categoría 5 ampliada no apantallado para datos

Para el conexionado de todos los cables del mismo tipo, se usará el mismo tipo de herramienta

La jerarquía de conexión es como se detalla en el siguiente esquema:



4.4 Cuartos de instalaciones necesarios para la implantación de los servicios

Para la implantación de los servicios que se abordan, son necesarios dos tipos de locales o cuartos de instalaciones:

- Cuartos de instalaciones para alojar la infraestructura de transmisión
- Cuartos de instalaciones para alojar la infraestructura de los servicios

Por razones de funcionalidad, control y seguridad en el acceso, es necesario que algunos de estos locales sean contiguos y estén en la misma planta. A este conjunto de locales les denominaremos Centro Estratégico de Comunicaciones y Almacenamiento Digital (en adelante CECAD)

4.5 Cuartos De Instalaciones Para Alojar La Infraestructura De Transmisión

Para implantar la red de transmisión electrónica en el edificio, son necesarios dos tipos de locales en los que alojar el sistema de conexionado y la electrónica que implementa la red:

- Repartidor Principal (RP)
- Repartidores Satélites (RSs)

El RP es un local único para toda la organización que conecta radialmente todos los RSs del mismo. El cableado entre el RP y los RSs, más la electrónica que los une, constituye la troncal de la red de transmisión para cada uno de los sistemas que soporta los diferentes servicios.

Al ser los RSs un mal necesario por requerimientos técnicos de distancia y no un bien deseable, el número de ellos, será el menor posible.

4.6 Centro Estratégico De Comunicaciones y Almacenamiento Digital (CECAD)

Al conjunto de locales de infraestructura de red o servicios, que deben ser contiguos en la misma planta, se les denominará: Centro Estratégico de Comunicaciones y Almacenamiento Digital (**CECAD**):

- Repartidor Principal (RP)
- Granja de Servidores (GS)
- Sistema de Alimentación Ininterrumpida (SAI)
- Operadores de sistemas y red (OSR)
- Almacén de copias de seguridad (ACS)

Los tres primeros están destinados a contener máquinas y no personas, por tanto se debe evitar la presencia de las mismas por espacios de tiempo prolongados. La mejor forma de resolver esto por diseño, es calibrar los termostatos de estos 3 locales a una temperatura de 20° C, que es ideal para minimizar la fatiga mecánica y electrónica de los componentes de los equipos, al tiempo que es lo suficientemente hostil como para garantizar la no presencia humana por tiempos prolongados.

El local OSR debe tener inspección visual mediante cristal (con barrera térmica) sobre el RP y sobre la GS.

Los tres primeros locales dispondrán de suelo técnico conductivo cuya estructura de soporte apoya sobre pavimento de cemento pulido o equivalente, acabado en pintura anti-polvo. Dispondrá de una rampa de acceso. La estructura metálica del suelo técnico estará puesta a tierra de estructura (no de datos).

4.6.1 Repartidor Principal (Rp)

El RP es el local donde se concentran todas las comunicaciones del edificio (tanto internas como externas) para todos los servicios que se describen, por tanto, es el local que aloja todos los elementos de las troncales de red (cableado y electrónica).

La ubicación de este local en el edificio depende del tamaño y geometría del mismo. En el caso en que todo el cableado del edificio se pueda abordar desde un RP único (se pueda circunscribir el edificio en una esfera de radio 100m, que seria la situación ideal), su ubicación se decide con criterios técnicos y se centrará axialmente en el mismo. En el caso en que por razones de distancia no se pueda abordar el cableado del edificio desde un único repartidor (un edificio muy grande), su ubicación se puede decidir con criterios administrativos (siempre que la distancia mecánica a cualquier RS desde el RP sea inferior a 500 m), esto implica que no debe tener dependencia técnica con el mismo, por tanto se podrá ubicar en la parte más conveniente atendiendo sobre todo a criterios de control, pudiendo compartir espacio físico con uno de los RSs.

Este local se recomienda que tenga al menos una disposición de un punto de drenaje de agua, para evitar el deterioro de los equipos electrónicos en caso de inundación por rotura de alguna conducción de la red de agua limpia o sucia. En el RP se alojan:

- Repartidor de cliente que conecta con el operador público de comunicaciones
- Distribuidor principal del cableado de voz
- Electrónica de voz (central telefónica)

- Distribuidor principal del cableado de datos
- Electrónica de cabecera de la troncal de transmisión de datos (Conmutador principal)
- Electrónica de comunicación externa (conecta con centros de capacitación)
- Distribuidor principal del cableado de TV
- Electrónica de cabecera para captación de canales de TV (terrestres, satélite o cable)
- Distribuidor de tierra de datos para el ámbito del CECAD

Debería estar constituido por tantos armarios rack unidos mecánicamente entre sí, como fuere necesario. Los armarios que alojen electrónica, deben incorporar (en su parte inferior) dos raíles de 10 enchufes conectadas a dos circuitos eléctricos provenientes de 2 mecanismos diferenciales distintos del cuadro de maniobra del SAI. Este requerimiento es para la conexión de las fuentes de alimentación redundantes de la electrónica.

Se recomienda instalar un mueble biblioteca para almacenar manuales y documentación de administración de las redes de cableado y de toda la electrónica que se aloje en el Repartidor Principal.

4.6.2 Granja De Servidores

En este local se ubicarán todos los servidores de datos de la Organización independientemente del área funcional a la que pertenezcan:

- Servidor de nombres para la red local (DNS)+Estafeta correo electrónico
- Servidor de las bases de datos
- Servidor de la base de datos de gestión de suministros y control de stocks

Se deberá instalar un mueble biblioteca para almacenar los manuales y documentación de administración de todos los sistemas.

4.6.3 Cuarto Del Sistema De Alimentación Interrumpida (SAI)

En este local se ubicará el Sistema de Alimentación Ininterrumpida (en adelante SAI) y el cuadro de maniobra que lo gestiona, desde el que se alimenta eléctricamente todo el CECAD.

El aire frío se inyectará a la altura del suelo, con el fin de facilitar la evacuación del calor por convección hacia la canalización de retorno, que estará en la parte superior. La circulación de aire será mediante circuito forzado.

Este local deberá disponer de al menos un punto de drenaje de agua, para evitar explosión o deterioro en caso de inundación por rotura de alguna conducción de la red de agua limpia o sucia.

4.6.4 Cuarto De Operadores De Sistema Y Red

Este cuarto alojará espacio para no más de 2/3 personas, que serán los responsables de operación tanto de la parte de red como de la parte de sistemas, para todos los servicios.

4.6.5 Cuarto Almacén De Copias De Seguridad

Este cuarto alojará el armario ignífugo para almacenar:

- Las copias de seguridad
- Los kits originales de todo el software
- Los documentos con las contraseñas de administración de todos los equipos de la organización
- La llave maestra de todas las cerraduras de todos los locales de las instalaciones

4.7 Repartidores Satélites (Rss)

Cuando por razones de distancia, no es posible abordar todo el cableado del edificio desde un repartidor único (que es la situación ideal), son necesarios cuartos de instalaciones intermedias, denominadas Repartidores Satélites (RSs). Los locales de los RSs no requieren suelo técnico (falso suelo).

4.8 Cuarto De Control De Vídeo-Vigilancia Y Control De Intrusión (Bunker)

En este local se alojará:

- Monitores de vídeo conectados a cámaras perimetrales, puertas con control de accesos, locales de instalaciones, etc.
- Monitores de vídeo conectados a la matriz de conmutación de vídeo
- Consola del sistema de control de video-vigilancia y control de intrusión
- Operadores de seguridad
- Caja fuerte para alojar armas y munición

4.9 Propiedades Que Deben Incorporar Los Cuartos De Instalaciones

Seguridad En El Acceso

Para los locales del CECAD y RSs se sugiere una puerta blindada con cerradura específica de seguridad y llaves maestras, así como paredes con dimensión suficiente. Así mismo incorporarán terminal del sistema de control de accesos, que actuará sobre el cerradero (sobre la cerradura seguirá actuando la llave), la alimentación eléctrica del mismo provendrá del SAI.

Climatización

Los siguientes locales:

- Repartidor principal
- Granja de servidores
- Cuarto del SAI

Dispondrán de un sistema de climatización que sólo producirá frío, incluso en el caso en que la temperatura exterior al edificio sea inferior a la del interior del mismo (típicamente época de invierno). Aparte de la climatización con renovación de aire, incluirá baterías de apoyo con control de humectación.

El control del sistema será tal que se garantice su funcionamiento siempre que haya suministro eléctrico y la impulsión del aire frío se realizará por el falso suelo, lo que permitirá distribuir frío directo mediante rejillas a los servidores en la granja de servidores y a los armarios en el RP.

Alimentación Eléctrica

En el CECAD se aloja electrónica que es crítica para el funcionamiento de la organización, por lo que debe ser alimentado eléctricamente desde una línea proveniente de un cuadro general del edificio y protegida por un grupo electrógeno en conmutación automática. Esta línea llegará a un conmutador de 3 posiciones (SAI, cero, línea) en el cuadro de maniobra del SAI, desde el que se alimentará a un Sistema de Alimentación Ininterrumpida (en adelante SAI), cuya salida volverá al cuadro de maniobra en el que, al tratarse de una fuente de energía autónoma, pasará por dispositivos diferenciales y desde éstos a los disyuntores (tiene por objeto abrir el paso de la corriente eléctrica) magnetotérmicos bipolares que alimentarán los circuitos finales instalados en el CECAD.

El SAI actuará como protector de sobretensiones y aislamiento galvánico en la alimentación a los equipos finales que soportan los servicios (servidores, conmutadores, enrutadores, etc.).

La tensión de salida del SAI estará referenciada a la tierra de datos, con el fin de garantizar el perfecto funcionamiento de la electrónica y de los mecanismos diferenciales.

En los RSs se instalará un SAI con la misma gestión y funcionalidad que en el RP.

SEGURIDAD

V. SEGURIDAD INFORMÁTICA

"La seguridad efectiva en la computación debe garantizar la prevención y detección de un accidente o un ataque, la existencia de medidas claramente definidas para afrontar el desastre cuando ocurra y si existe una interrupción del procesamiento, restablecerlo". [2]

Para el análisis de la seguridad informática se requiere un enfoque amplio que abarque cierto número de aspectos relacionados entre sí de manera metódica. Y hay dos grandes áreas que se deben incorporar a tal enfoque:

1. Aspectos Administrativos
2. Aspectos Técnicos y de Procedimiento

Los aspectos clave se pueden resumir de la manera siguiente:

Elementos Administrativos:

- Política definida sobre seguridad en computación
- Organización y división de las responsabilidades
- Seguridad física y contra incendios
- Políticas hacia el personal
- Seguros.

Elementos Técnicos y de Procedimiento:

- Seguridad de los sistemas (equipo y programación, redes)
- Seguridad de las aplicaciones, incluyendo la seguridad de los datos y los archivos.
- Estándares de programación y operación de los sistemas.
- Función de la auditoria interna y externa.
- Plan y simulacro para desastres.

[2] H Fine, Leonard, *Seguridad en centros de cómputo* – p. 24

El estudio de estas áreas revelará que ninguna es por si sola, de importancia exclusiva: en una instalación específica una de ellas puede tener mayor importancia que otra o bien; requerir de mayor atención, pero la ausencia de un elemento puede vaciar el concepto de seguridad total asi como el manejo y control de la misma.

(Figura 1.1) 3

La figura anterior muestra una viga sostenida por nueve columnas, cada una de las cuales representa un elemento del concepto de seguridad total y su objetivo es que las columnas sostengan la viga en posición horizontal respecto al piso. Y la debilidad de alguna de las columnas obligará a reforzar las otras a fin de conservar la viga en forma horizontal. La debilidad de dos o mas columnas causaría el movimiento y quizá la ruptura o caída de la viga. De esta manera, resulta claro que, no se puede eliminar ninguna columna ni excluirla de la estructura, ya que tendría un efecto sobre otras áreas.

---

[3] **Ibidem**, p. 18

La viga y las columnas se encuentran sobre suelo firme, pero existe una red de seguridad para sostener la viga en caso de desastre. Se trata del plan de desastre o contingencia para la instalación.

Políticas De Seguridad

El establecimiento de las políticas de seguridad tiene como premisa el resguardo y la vigilancia del correcto funcionamiento del centro de cómputo así como las medidas de solución posibles en caso de desastre. Para el establecimiento de dichas políticas se requiere un estudio detallado y preciso de variables que nos llevarán a un resultado completo y nos darán un amplio panorama de fortalezas y debilidades de la organización y directamente del centro de cómputo. Para dicho estudio se mencionan los siguientes conceptos:

Para la elaboración de la política de seguridad, el primer paso es hacer una relación de los aspectos sensibles dentro de la organización, tanto físicos (equipos Almacén, routers, etc.), como lógicos (aplicaciones, bases de datos, etc...).

5.1 Cuantificación de los Riesgos Para la Seguridad en Informática

Esta sección es una de las partes más importantes para la elaboración de las políticas informáticas, ya que la falta de éstas, de una manera cuantificada es causa para que no se acepten muchas recomendaciones importantes sobre seguridad en el centro de cómputo.

La cuantificación de los riesgos de seguridad implica ciertos pasos: [4]

1. Clasificación general de las instalaciones en términos de riesgo alto, medio y bajo.
2. Identificación de las aplicaciones que constituyen riesgos altos.

[4] **Idem,** p. 24

3. Cuantificación del impacto producido por la suspensión prolongada del procesamiento en las aplicaciones de alto riesgo.
4. Formulación de las medidas necesarias para lograr un nivel de seguridad adecuado, es decir, en equilibrio con los niveles de riesgo.
5. Justificación de las medidas de seguridad en cuanto al costo que representan.

A continuación se mencionan las características principales de los puntos numerados con anterioridad en lo referente a los pasos que implica la seguridad en informática.

5.2 Clasificación de las instalaciones

Las instalaciones de alto riesgo tienen como atributo principal el manejo de información nacional, así como confidencial, de cifras, valores competitivos en el mercado o bien de interés nacional. Y que el retraso de la información puede ocasionar una amenaza potencial para la subsistencia del centro de cómputo.

Las instalaciones de riesgo medio y bajo son de difícil detección ya que lo que en realidad interesa es el impacto que puede tener en el buen estado o la subsistencia de la empresa en caso de interrupción prolongada en el centro de cómputo.

Para la clasificación precisa de los centros de cómputo se recomienda el llenado de un "Formulario de Inventario" que asegura la correcta aplicación de los procedimientos de seguridad.

Analizando los diversos aspectos que se toman en cuenta para la precisión de la clasificación por instalaciones y se enumeran a continuación aspectos claves para determinar dicho plan de trabajo:

	Aspectos clave SÍ / NO	Adecuado SÍ / NO
Política de seguridad - Existe una política de seguridad definida - La Responsabilidad de la formulación de la política de está asignada. - Conciencia y compromiso por parte de la alta gerencia. - El alcance de las pérdidas se ha definido. **Organización y división de responsabilidades** - La responsabilidad de la seguridad se ha asignado. - Descripciones claras de puestos. - Inclusión de la seguridad en las descripciones de puestos. - División de responsabilidades entre las funciones clave. - Sistemas de verificación interna bien definidos. **Seguridad de los sistemas** - Las fallas en el equipo están definidas - Las fallas en los programas están definidas. - Seguridad de terminales. - Seguridad de redes. - Equipo de Respaldo. **Seguridad de las Aplicaciones** - Controles de usuario. - Controles del área de procesamiento. - Planes de contingencia en la aplicación - Seguridad de datos y archivos.		

	Aspectos clave SÍ / NO	Adecuado SÍ / NO
Seguridad Física		
- Acceso del personal		
- Alarmas.		
- Ubicación.		
- Construcción.		
- Disposición.		
Seguridad contra incendios		
- Detección de Incendios.		
- Extinción de incendios.		
- Nexos con el cuartel de bomberos.		
- Rutina contra incendios.		
Estándares		
- Métodos y supervisión		
- Documentación.		
- Duplicados de respaldo.		
Políticas hacia el personal		
- Políticas de contratación.		
- Procedimientos para evaluar el desempeño.		
- Permisos		
- Rotación de puestos.		
Seguros		
- Equipo		
- Programas		
- Personal		
- *Pérdida de utilidades*		
Auditoria		
- Habilidades		
- Técnicas especializadas		

5.3 Identificación de las aplicaciones de riesgo alto, medio y bajo.

Aun dentro de las instalaciones provistas de un alto nivel de seguridad no todas las aplicaciones son de alto riesgo, por eso es necesario analizar mejor la seguridad e identificar las aplicaciones según su nivel de riesgo.

Para este efecto es necesario ponderar las aplicaciones en orden tabular y descendente según su nivel de importancia y así se facilita la identificación de las aplicaciones hacia donde se deben dirigir la mayoría de los esfuerzos.

Un aspecto importante a considerar es la cuantificación del riesgo, pero a la vez es también un factor extremadamente difícil que requiere de persistencia pero sin embargo se debe lograr y una sugerencia es la entrevista directa con gerentes afectados por una suspensión en el procesamiento y pedirles que cuantifiquen dichos daños.

Para obtener el consenso sobre los niveles de riesgo, es necesario lograr un compromiso de la gerencia con el nivel de riesgo definido. Y se considera importante organizar reuniones gerenciales para informar sobre las expresiones sobre riesgos debidamente tabulados, según se hallan definido, el propósito de la reunión será lograr el consenso sobre los niveles de riesgo, que por lo general se representan como rangos más que como cifras absolutas y de tal manera se puede ver que la expresión del riesgo en esta forma permite justificar de manera objetiva el costo de las medidas de seguridad.

5.4 Evaluación de las medidas de Seguridad

En esta etapa de revisión preliminar de la seguridad en el centro de cómputo en muchas ocasiones no es posible obtener todas las recomendaciones detalladas. Y solo se logrará una vez que se lleve a cabo la revisión a fondo de la seguridad. Sin embargo, es posible definir la estrategia global que se debe seguir para afrontar los niveles de riesgo definidos. Esta estrategia recomienda incluir los siguientes puntos:[5]

1.- Aplicaciones programas y archivos específicos.

2.- Planes de detección y métodos para prevenir abusos o desastres.

3.- Prioridades, o sea, acciones que se requieren a corto plazo y los elementos que se deben considerar de manera detallada a mediano y largo plazos.

5.5 Justificación de las medidas de Seguridad en cuanto al costo.

Todas las etapas anteriores conducen en forma natural hacia la recolección y la presentación de todos los informes necesarios para una decisión bien fundada sobre los costos y los beneficios de la estrategia de la seguridad. Por lo tanto toda la información que se obtenga y las decisiones que se tomen se deben documentar de manera progresiva y esto se puede consolidar en un informe final ante la gerencia. Y es conveniente convocar una reunión de la gerencia involucrada para evaluar tanto los hallazgos como las recomendaciones a fin de que se obtenga una decisión en consecuencia, y se apruebe un plan de acción destinado a la investigación y la aplicación más detalladas. Así esta práctica constituye un marco de trabajo para el método que se acepte y los niveles de costo en los cuales se incurra sin solicitudes redundantes a la gerencia.

5.6 El logro del compromiso con la política de seguridad

Como lo he mencionado en puntos anteriores el compromiso debe ser general para todos los trabajadores del área y de la dependencia u organización. Pero es de vital importancia establecer el compromiso con los niveles gerenciales, dado que finalmente ellos serán quienes tomen las medidas y presupuesto necesario para el establecimiento de la seguridad Informática, sin embargo esta tarea puede resultar difícil al menos que dicha línea organizacional haya participado en el establecimiento de todas las fases anteriores. Por lo tanto podrá resultar

[5] **Ibidem**, p. 28

provechoso establecer un comité de seguridad que nos conduzca a un mayor seguimiento de rutinas y a niveles de compromiso más altos.
Después de analizados los puntos anteriores podremos entonces de manera mas confiable y consiente establecer niveles de seguridad necesarios.
El establecimiento de las políticas de seguridad varía dependiendo de las necesidades de la organización, su composición, nivel de regulación, dependencia y presupuesto, ya que son factores primordiales para un trabajo de dicha magnitud y asegure la más mínima tecnología.

5.7 Organización Y División De Responsabilidades

La forma en que se organizan las actividades en el centro de cómputo comprende distintos conceptos en cuánto a la seguridad que se requiere para el pleno desempeño de las funciones.
La división de Responsabilidades, los sistemas de control interno, asignar responsabilidades para salvaguardar la seguridad del centro de cómputo y la sustitución del personal clave son aspectos que pueden afectar la seguridad

La División de Responsabilidades permitirá dentro del centro de cómputo una revisión y balance exhaustivo en lo que se refiere a la calidad del trabajo estableciendo restricciones y accesos a las personas correspondientes y evitar acceso innecesario a información.
Se puede establecer también un amplio margen de actividades que se pueden organizar y dar pauta a los tipos de divisiones de responsabilidades existentes reforzando las funciones claramente definidas y autónomas y pueden ser actividades como: el desarrollo de los sistemas, control, el procesamiento de archivos, la clasificación de la información, operaciones etc....

Asignación de Responsabilidades en cuánto a la Seguridad, en esta consignación los aspectos mas relevantes se detallan en las políticas de seguridad, en las

asignadas por un comité de informática y la existencia de planes contra desastres y/o incendios, detectando las exigencias del centro de cómputo para que se cumplan con las estadísticas esperadas en cuanto a los niveles de seguridad propios.

Un elemento que es clave para la seguridad del centro de cómputo es garantizar que todo el personal clave tenga una sustitución adecuada, aunque muchas veces es difícil de cumplir con este requisito, al menos se debe contar con una restricción cuidadosa, la definición del personal clave.

5.8 Sistemas de Control Interno

Los Sistemas de Control Interno son la combinación de la división de responsabilidades y los sistemas de verificación interna, este último teniendo como característica principal que son comprobaciones de que se cuenta con una recolección precisa y ordenada de los datos y con la división de responsabilidades correspondientes.

La típica verificación documentada de evidencias requiere que:

1.- Las modificaciones de los programas se autoricen y se prueben de manera adecuada, para obtener niveles óptimos de resultados.

2.- Se documente de manera adecuada y progresiva a los sistemas nuevos a través del trabajo de desarrollo, y se realice una prueba antes de entregar el trabajo a la producción.

5.9 De los Virus y Otros Medios de Propagación

Definición

Desde hace algunos años los virus son la mayor amenaza para los sistemas informáticos y la principal causa de pérdidas económicas en las empresas. Un virus es una parte de código de un programa de computadora que es capaz no sólo de duplicarse a sí mismo sino también de "pegarse" a otro programa sin que el usuario se dé cuenta de esto. Un Caballo de Troya es un programa que parece legítimo pero contiene rutinas que causan daño a otros programas o datos dentro del sistema cuando se corren. Un gusano es un programa que hace uso de software de red y de alguna instalación de comunicaciones para replicarse a si mismo y moverse de sistema en sistema. El gusano realiza alguna actividad a cada sistema al que accesa, tal como consumir recursos de procesamiento o depositar virus; los gusanos toman ventaja de las fallas de seguridad de los sistemas operativos. Mientras que un virus se difunde infectando otros programas en una computadora o red, un gusano se difunde sin infectar a los programas.

Otro punto que ha potenciado el avance de los virus es su forma de infección, ya que en un principio su dispersión se realizaba por medio del intercambio de disquetes u otros medios físicos, pero hoy en día gracias a Internet, un virus recién desarrollado en Japón puede infectar miles de computadoras en todo el mundo en cuestión de segundos así como afectar de manera directa al centro de cómputo causando daños o desperfectos en la operación de lo servidores

5.9.1 Daños que puede hacer un virus a los sistemas

- Software
  - Modificación de programas para que dejen de funcionar
  - Modificación de programas para que funcionen erróneamente
  - Modificación sobre los datos
  - Eliminación de programas y/o datos
  - Acabar con el espacio libre en el disco rígido
  - Hacer que el sistema funcione mas lentamente
  - Robo de información confidencial
- Hardware
  - Borrado del BIOS
  - Quemado del procesador por falsa información del sensor de temperatura
  - Rotura del disco rígido al hacerlo leer repetidamente sectores específicos que fuercen su funcionamiento mecánico

Medios de propagación:

- Disquetes u otro medio de almacenamiento removible
- Redes de computadoras
- Mensajes de correo electrónico
- Software bajado de Internet
- Discos de demostración y pruebas gratuitos

Síntomas que indican la presencia de Virus....

- Cambios en la longitud de los programas
- Cambios en la fecha y/u hora de los archivos
- Retardos al cargar un programa
- Operación más lenta del sistema
- Reducción de la capacidad en memoria y/o disco rígido
- Sectores defectuosos en los disquetes
- Mensajes de error inusuales
- Actividad extraña en la pantalla
- Fallas en la ejecución de los programas
- Fallas al bootear el equipo
- Escrituras fuera de tiempo en el disco

5.9.2 Tipos de Virus por su destino de infección

Infectores de archivos ejecutables

- Afectan archivos de extensión EXE, COM, BAT, SYS, PIF, DLL, DRV
- Infectores directos

El programa infectado tiene que estar ejecutándose para que el virus pueda funcionar (seguir infectando y ejecutar sus acciones destructivas)

Infectores residentes en memoria. El programa infectado no necesita estar ejecutándose, el virus se aloja en la memoria y permanece residente infectando cada nuevo programa ejecutado y ejecutando su rutina de destrucción.

Infectores del sector de arranque.

Tanto los discos rígidos como los disquetes contienen un Sector de Arranque, el cual contiene información específica relativa al formato del disco y los datos almacenados en él. Además, contiene un pequeño programa llamado Boot Program que se ejecuta al bootear desde ese disco y que se encarga de buscar y ejecutar en el disco los archivos del sistema operativo. Este programa es el que muestra el famoso mensaje de "Non-system Disk or Disk Error" en caso de no encontrar los archivos del sistema operativo. Este es el programa afectado por los virus de sector de arranque. La computadora se infecta con un virus de sector de arranque al intentar bootear desde un disquete infectado. En este momento el virus se ejecuta e infecta el sector de arranque del disco rígido, infectando luego cada disquete utilizado en la PC. Es importante destacar que como cada disco posee un sector de arranque, es posible infectar la PC con un disquete que contenga solo datos.

Macrovirus

Son los virus más populares de la actualidad. No se transmiten a través de archivos ejecutables, sino a través de los documentos de las aplicaciones que poseen algún tipo de lenguaje de macros. Entre ellas se encuentran todas las pertenecientes al paquete Office (Word, Excel, Power Point, Access) y también el Corel Draw.

Cuando uno de estos archivos infectado es abierto o cerrado, el virus toma el control y se copia a la plantilla base de nuevos documentos, de forma que sean infectados todos los archivos que se abran o creen en el futuro. Los lenguajes de macros como el Visual Basic For Applications son muy poderosos y poseen capacidades como para cambiar la configuración del sistema operativo, borrar archivos, enviar e-mails, etc.

De Actives Agents y Java Applets.

En 1997, aparecen los Java applets y Actives controls. Estos pequeños programas se graban en el disco rígido del usuario cuando está conectado a Internet y se ejecutan cuando la página web sobre la que se navega lo requiere, siendo una forma de ejecutar rutinas sin tener que consumir ancho de banda. Los virus desarrollados con Java applets y Actives controls acceden al disco rígido a través de una conexión www de manera que el usuario no los detecta. Se pueden programar para que borren o corrompan archivos, controlen la memoria, envíen información a un sitio web, etc.

De HTML.

Un mecanismo de infección más eficiente que el de los Java applets y Actives controls apareció a fines de 1998 con los virus que incluyen su código en archivos HTML. Con solo conectarse a Internet, cualquier archivo HTML de una página web puede contener y ejecutar un virus. Este tipo de virus se desarrollan en Visual Basic Script. Atacan a usuarios de Win98, 2000 y de las últimas versiones de Explorer. Esto se debe a que necesitan que el Windows Scripting Host se encuentre activo. Potencialmente pueden borrar o corromper archivos.

Trojanos/Worms

Los troyanos son programas que imitan programas útiles o ejecutan algún tipo de acción aparentemente inofensiva, pero que de forma oculta al usuario ejecutan el código dañino.Los troyanos no cumplen con la función de autorreproducción, sino que generalmente son diseñados de forma que por su contenido sea el mismo usuario el encargado de realizar la tarea de difusión del virus. (Generalmente son enviados por e-mail)

5.9.3 Tipos de virus de computación por sus acciones y/o modo de activación

Bombas

Se denominan así a los virus que ejecutan su acción dañina como si fuesen una bomba. Esto significa que se activan segundos después de verse el sistema infectado o después de un cierto tiempo (bombas de tiempo) o al comprobarse cierto tipo de condición lógica del equipo. (bombas lógicas). Ejemplos de bombas de tiempo son los virus que se activan en una determinada fecha u hora determinada. Ejemplos de bombas lógicas son los virus que se activan cuando al disco rígido solo le queda el 10% sin uso, etc.

Camaleones

Son una variedad de virus similares a los caballos de Troya que actúan como otros programas parecidos, en los que el usuario confía, mientras que en realidad están haciendo algún tipo de daño. Cuando están correctamente programados, los camaleones pueden realizar todas las funciones de los programas legítimos a los que sustituyen (actúan como programas de demostración de productos, los cuales son simulaciones de programas reales).

Un software camaleón podría, por ejemplo, emular un programa de acceso a sistemas remotos realizando todas las acciones que ellos realizan, pero como tarea adicional (y oculta a los usuarios) va almacenando en algún archivo los diferentes logins y password para que posteriormente puedan ser recuperados y utilizados ilegalmente por el creador del virus camaleón.

Reproductores

Los reproductores (también conocidos como conejos-rabbits) se reproducen en forma constante una vez que son ejecutados hasta agotar totalmente (con su descendencia) el espacio de disco o memoria del sistema.
La única función de este tipo de virus es crear clones y lanzarlos a ejecutar para que ellos hagan lo mismo. El propósito es agotar los recursos del sistema, especialmente en un entorno multiusuario interconectado, hasta el punto que el sistema principal no puede continuar con el procesamiento normal.

Gusanos (Worms).

Los gusanos son programas que constantemente viajan a través de un sistema informático interconectado, de PC a PC, sin dañar necesariamente el hardware o el software de los sistemas que visitan.

La función principal es viajar en secreto a través de equipos anfitriones recopilando cierto tipo de información programada (tal como los archivos de passwords) para enviarla a un equipo determinado al cual el creador del virus tiene acceso.

Backdoors

Son también conocidos como herramientas de administración remotas ocultas. Son programas que permiten controlar remotamente la PC infectada. Generalmente son distribuidos como troyanos. Cuando un virus de estos es ejecutado, se instala dentro del sistema operativo, al cual monitorea sin ningún tipo de mensaje o consulta al usuario. Incluso no se lo vé en la lista de programas activos.

Los Backdoors permiten al autor tomar total control de la PC infectada y de esta forma enviar, recibir archivos, borrar o modificarlos, mostrarle mensajes al usuario, etc....

5.9.4 Estrategias de infección usadas por los virus

Añadidura o empalme:

El código del virus se agrega al final del archivo a infectar, modificando las estructuras de arranque del archivo de manera que el control del programa pase por el virus antes de ejecutar el archivo. Esto permite que el virus ejecute sus tareas específicas y luego entregue el control al programa. Esto genera un incremento en el tamaño del archivo lo que permite su fácil detección.

Inserción:

El código del virus se aloja en zonas de código no utilizadas o en segmentos de datos para que el tamaño del archivo no varíe. Para esto se requieren técnicas muy avanzadas de programación, por lo que no es muy utilizado este método.

Reorientación:

Es una variante del anterior. Se introduce el código principal del virus en zonas físicas del disco rígido que se marcan como defectuosas y en los archivos se implantan pequeños trozos de código que llaman al código principal al ejecutarse el archivo. La principal ventaja es que al no importar el tamaño del archivo el cuerpo del virus puede ser bastante importante y poseer mucha funcionalidad.

Su eliminación es bastante sencilla, ya que basta con rescribir los sectores marcados como defectuosos.

Polimorfismo:

Este es el método mas avanzado de contagio. La técnica consiste en insertar el código del virus en un archivo ejecutable, pero para evitar el aumento de tamaño del archivo infectado, el virus compacta parte de su código y del código del archivo anfitrión, de manera que la suma de ambos sea igual al tamaño original del archivo. Al ejecutarse el programa infectado, actúa primero el código del virus descompactando en memoria las porciones necesarias. Una variante de esta técnica permite usar métodos de encriptación dinámicos para evitar ser detectados por los antivirus.

Sustitución:

Es el método mas tosco. Consiste en sustituir el código original del archivo por el del virus. Al ejecutar el archivo deseado, lo único que se ejecuta es el virus, para disimular este proceder reporta algún tipo de error con el archivo de forma que creamos que el problema es del archivo.

Ejemplos de virus y sus acciones

- Happy99: Programa enviado por mail, abre una ventana con fuegos artificiales. Manipula la conectividad con Internet.
- Melissa: Macrovirus de Word. Se envía a sí mismo por mail. Daña todos los archivos .doc
- Chernobyl (W95.CIH): Borra el primer Mb del HD, donde se encuentra la FAT. Obliga a formatear el HD. Además intenta rescribir el BIOS de la PC lo que obliga a cambiar el mother. Se activa el 26 de abril.
- Michelangelo: Virus de boot sector. Se activa el 6 de marzo. Sobre escribe la FAT, dejando el disco inutilizable.

- WinWord.Concept: Macrovirus que infecta la plantilla Normal.dot., hace aparecer mensajes en la pantalla y mal funcionamiento del Word.
- FormatC: Troyano que infecta el Word, al abrir un archivo infectado formatea el disco rígido.
- Back Orifice2000 (BO2K): Funcionalmente es un virus y sirve para el robo de información. Permite tomar control remoto de la PC o del servidor infectados, con la posibilidad de robar información y alterar datos.
- VBS/Bubbleboy: Troyano que se ejecuta sin necesidad de abrir un attachment, y se activa inmediatamente después de que el usuario abra el mail. No genera problemas serios.

5.9.5 Virus falsos: HOAX

Definición:
Falsas alarmas de virus

Ejemplos: Join The Crew, Win a Holiday, Solidaridad con Brian

Medidas de prevención para los virus falsos:

Responder esas cadenas, ya que crea saturación de los servidores de mail y, además son usadas para levantar direcciones de e-mails para luego enviar publicidades.

Email Bombing and Spamming

Descripción
E-mail bombing es el envío reiterado de un mismo mail a una cuenta en particular. E-mail spamming es una variante del bombing, es el envío de e-mail a cientos o miles de usuarios. El problema se acrecienta si alguien responde el mensaje a todos.

Spamming y bombing pueden ser combinados con e-mail spoofing, que consiste en alterar la dirección del emisor del destinatario, haciendo imposible conocer quien originó la cadena. Cuando una gran cantidad de mensajes son dirigidos a un mismo servidor, este puede sufrir un DoS (Denial of Service), O que el sistema se caiga como consecuencia de utilizar todos los recursos del servidor, o completar el espacio en los discos.

Pasos para evitarlos

En principio es imposible de prevenir ya que cualquier usuario de e-mail puede spam cualquier otra cuenta de e-mail, o lista de usuarios.

Se deben activar las opciones de filtrado de mensajes

Práctica de seteo de opciones de filtrado de mensajes

Evitar:

Responder esas cadenas, ya que crea saturación de los servidores de mail y además son usadas para levantar direcciones de e-mails para luego enviar publicidades.

Definición:

Un "script" es un tipo de programa de computación usado en la programación de sitios web. (Ej.: Javascript, Perl, Tcl, VBScript, etc). Un script consiste en comandos de texto. Cada vez que el browser recibe estos comandos, los interpreta y los ejecuta. Esto significa que un script puede ser incluido en cualquier página web como si fuese texto. En principio un script no es necesariamente un programa maligno, sino que se utiliza su funcionalidad con fines malignos.

5.9.6 Medidas antivirus

Un programa antivirus por muy bueno que sea se vuelve obsoleto muy rápidamente ante los nuevos virus que aparecen día a día, por tanto se pueden tomar medidas para prevenir y / o detectar los virus.

- Desactivar arranque desde disquete en el setup para que no se ejecuten virus de boot.
- Desactivar compartir archivos e impresoras.
- Analizar con el antivirus todo archivo recibido por e-mail antes de abrirlo.
- Actualizar antivirus.
- Activar la protección contra macrovirus del Word y el Excel.
- Ser cuidadoso al bajar archivos de Internet (Analizar si vale el riesgo y si el sitio es seguro)
- No enviar información personal ni financiera a menos que sepa quien se la solicita y que sea necesaria para una transacción u operación.
- No compartir discos con otros usuarios.
- No entregar a nadie claves de acceso, incluso si es requerido por cualquier otro medio.
- Realice backups

5.10 Firewalls y Seguridad en Internet

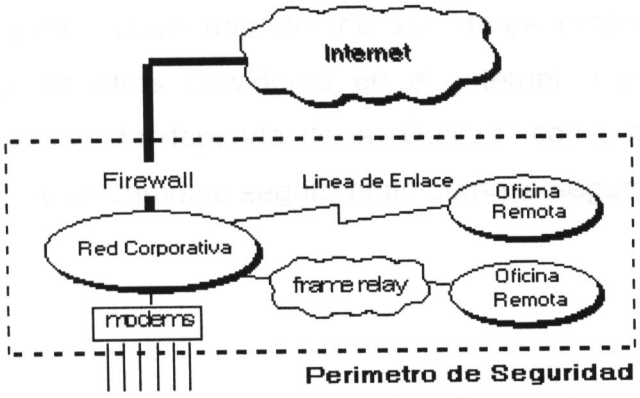
La seguridad ha sido el principal concerniente a tratar cuando una organización desea conectar su red privada al Internet. Sin tomar en cuenta el tipo de negocios, se ha incrementado el numero de usuarios de redes privadas por la demanda del acceso a los servicios de Internet tal es el caso del World Wide Web (WWW), Internet Mail (e-mail), Telnet, y File Transfer Protocol (FTP). Adicionalmente los corporativos buscan las ventajas que ofrecen las paginas en el WWW y los servidores FTP de acceso publico en el Internet.

Los administradores de red tienen que incrementar todo lo concerniente a la seguridad de sus sistemas, debido a que se expone la organización privada de sus datos así como la infraestructura de su red a los Expertos de Internet (*Internet Crakers*). Para superar estos temores y proveer el nivel de protección requerida, la organización necesita seguir una política de seguridad para prevenir el acceso no-autorizado de usuarios a los recursos propios de la red privada, y protegerse contra la exportación privada de información. Todavía, aun si una organización no esta conectada al Internet, esta debería establecer una política de seguridad interna para administrar el acceso de usuarios a porciones de red y proteger sensitivamente la información secreta.

5.10.1 Firewalls

Un Firewall en Internet es un sistema o grupo de sistemas que impone una política de seguridad entre la organización de red privada y el Internet. El firewall determina cual de los servicios de red pueden ser accesados dentro de esta por los que están fuera, es decir quien puede entrar para utilizar los recursos de red pertenecientes a la organización. Para que un firewall sea efectivo, todo tráfico de información a través del Internet deberá pasar a través del mismo donde podrá ser inspeccionada la información. El firewall podrá únicamente autorizar el paso del tráfico, y el mismo podrá ser inmune a la penetración.

Desafortunadamente, este sistema no puede ofrecer protección alguna una vez que el agresor lo traspasa o permanece entorno a este.



(Figura 1.2) La Política De Seguridad Crea Un Perímetro De Defensa.

Esto es importante, ya que debemos de notar que un firewall de Internet no es justamente un ruteador, un servidor de defensa, o una combinación de elementos que proveen seguridad para la red. El firewall es parte también de una política de seguridad completa que crea un perímetro de defensa diseñada para proteger las fuentes de información. Esta política de seguridad como ya se mencionó, podrá incluir publicaciones con las guías de ayuda donde se informe a los usuarios de sus responsabilidades, normas de acceso a la red, política de servicios en la red, política de autenticidad en acceso remoto o local a usuarios propios de la red, reglas de encriptación de datos y discos, normas de protección de virus, y entrenamiento. Todos los puntos potenciales de ataque en la red podrán ser protegidos con el mismo nivel de seguridad. Un firewall de Internet sin una política de seguridad comprensiva es como poner una puerta de acero en una tienda.

5.10.2 Beneficios de un firewall en Internet

Los firewalls en Internet administran los accesos posibles del Internet a la red privada. Sin un firewall, cada uno de los servidores propios del sistema se exponen al ataque de otros servidores en el Internet. Esto significa que la seguridad en la red privada depende de la "Dureza" con que cada uno de los servidores cuenta y es únicamente seguro tanto como la seguridad en la fragilidad posible del sistema.

El firewall permite al administrador de la red definir un "choke point" (envudo), manteniendo al margen los usuarios no-autorizados (tal, como., hackers, crakers, vándalos, y espías) fuera de la red, prohibiendo potencialmente la entrada o salida al vulnerar los servicios de la red, y proporcionar la protección para varios tipos de ataques posibles. Uno de los beneficios clave de un firewall en Internet es que ayuda a simplificar los trabajos de administración, una vez que se consolida la seguridad en el sistema firewall, es mejor que distribuirla en cada uno de los servidores que integran nuestra red privada.

El firewall ofrece un punto donde la seguridad puede ser monitoreada y si aparece alguna actividad sospechosa , este generara una alarma ante la posibilidad de que ocurra un ataque, o suceda algún problema en el transito de los datos. Esto se podrá notar al acceder la organización al Internet, la pregunta general es "si" pero "cuando" ocurrirá el ataque. Esto es extremadamente importante para que el administrador audite y lleve una bitácora del tráfico significativo a través del firewall. También, si el administrador de la red toma el tiempo para responder una alarma y examina regularmente los registros de base. Esto es innecesario para el firewall, desde que el administrador de red desconoce si ha sido exitosamente atacado.

Concentra la seguridad Centraliza los accesos

Genera alarmas de seguridad Traduce direcciones (NAT)

Monitorea y registra el uso de Servicios de WWW y FTP.

Internet.

(Figura 1.3)

5.10.3 Beneficios De Un Firewall De Internet.

El Internet ha experimentado una crisis en las direcciones, logrando que el direccionamiento IP sea menos generoso en los recursos que proporciona. Por este medio se organizan las compañías conectadas al Internet, debido a esto hoy no es posible obtener suficientes registros de direcciones IP para responder a la población de usuarios en demanda de los servicios. Un firewall es un lugar lógico para desplegar un Traductor de Direcciones de Red (NAT) esto puede ayudar aliviando el espacio de direccionamiento acortando y eliminando lo necesario para re-enumerar cuando la organización cambie del Proveedor de Servicios de Internet (ISPs)

Un firewall de Internet es el punto perfecto para auditar o registrar el uso del Internet. Esto permite al administrador de red justificar el gasto que implica la conexión al Internet, localizando con precisión los cuellos de botella potenciales del ancho de banda, y promueve el método de cargo a los departamentos dentro del modelo de finanzas de la organización.

Un firewall de Internet ofrece un punto de reunión para la organización. Si una de sus metas es proporcionar y entregar servicios información a consumidores, el firewall de Internet es ideal para desplegar servidores WWW y FTP.

El firewall puede presentar los problemas que genera un punto de falla simple. Enfatizando si este punto de falla se presenta en la conexión al Internet, aun así la red interna de la organización puede seguir operando - únicamente el acceso al Internet esta perdido.

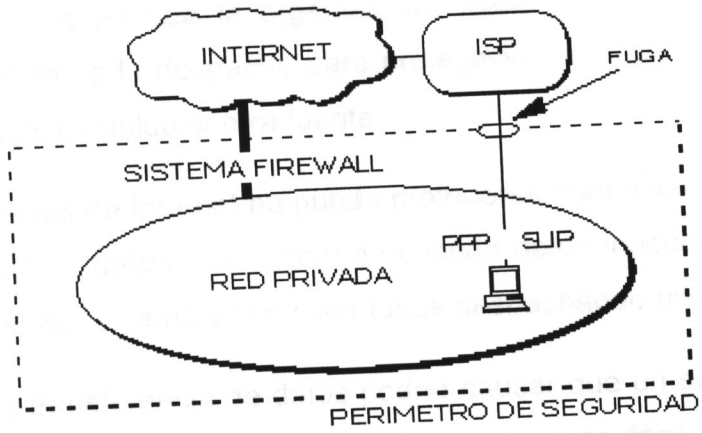
La preocupación principal del administrador de red, deben ser los múltiples accesos al Internet, que se pueden registrar con un monitor y un firewall en cada punto de acceso que posee la organización hacia el Internet. Estos dos puntos de acceso significa dos puntos potenciales de ataque a la red interna que tendrán que ser monitoreados regularmente.

5.10.4 Limitaciones de un firewall

Un firewall no puede protegerse contra aquellos ataques que se efectúen fuera de su punto de operación. Por ejemplo, si existe una conexión dial-out sin restricciones que permita entrar a nuestra red protegida.

El usuario puede hacer una conexión SLIP o PPP al Internet. Los usuarios con sentido común suelen "irritarse" cuando se requiere una autenticación adicional requerida por un Firewall Proxy Server (FPS) lo cual se puede ser provocado por un sistema de seguridad circunvecino que esta incluido en una conexión directa SLIP o PPP del ISP.

Este tipo de conexiones derivan la seguridad provista por firewall construido cuidadosamente, creando una puerta de ataque. Los usuarios pueden estar consientes de que este tipo de conexiones no son permitidas como parte de integral de la arquitectura de la seguridad en la organización.



(Figura 1.4) Conexión Circunvecina al Firewall De Internet.

El firewall no puede protegerse de las amenazas a que esta sometido por traidores o usuarios inconscientes. El firewall no puede prohibir que los traidores o espías corporativos copien datos sensitivos en disquetes o tarjetas PCMCIA y substraigan estas del edificio.

El firewall no puede proteger contra los ataques de la "Ingeniería Social", por ejemplo un Hacker que pretende ser un supervisor o un nuevo empleado despistado, persuade al menos sofisticado de los usuarios a que le permita usar su contraseña al servidor del corporativo o que le permita el acceso "temporal" a la red.

Para controlar estas situaciones, los empleados deberían ser educados acerca de los varios tipos de ataque social que pueden suceder, y a cambiar sus contraseñas si es necesario periódicamente.

El firewall no puede protegerse contra los ataques posibles a la red interna por virus informativos a través de archivos y software. Obtenidos del Internet por sistemas operativos al momento de comprimir o descomprimir archivos binarios, el firewall de Internet no puede contar con un sistema preciso de SCAN para cada tipo de virus que se puedan presentar en los archivos que pasan a través de el.

La solución real esta en que la organización debe ser consciente en instalar software anti-viral en cada despacho para protegerse de los virus que llegan por medio de disquettes o cualquier otra fuente.

Finalmente, el firewall de Internet no puede protegerse contra los ataques posibles en la transferencia de datos, estos ocurren cuando datos inocuos son enviados o copiados a un servidor interno y son ejecutados despachando un ataque.

Por ejemplo, una transferencia de datos podría causar que un servidor modificara los archivos relacionados a la seguridad haciendo más fácil el acceso de un intruso al sistema, el desempeño de los servidores Proxy en un servidor de defensa es un excelente medio de prohibición a las conexiones directas por agentes externos y reduce las amenazas posibles por los ataques con transferencia de datos.

5.10.5 Herramientas del hacker

Es difícil describir el ataque "típico" de un hacker debido a que los intrusos poseen diferentes niveles de técnicos por su experiencia y son además motivados por diversos factores. Algunos hackers son intrigosos por el desafío, otros más gozan de hacer la vida difícil a los demás, y otros tantos substraen datos delicados para algún beneficio propio.

5.10.6 Recolección de información del Hacker

El primer paso es saber en que forma se recolecta la información y además que tipo de información es. La meta es construir una base de datos que contenga la organización de la red y colectar la información acerca de los servidores residentes.

Esta es una lista de herramientas que un hacker puede usar para colectar esta información:

- El protocolo SNMP puede utilizarse para examinar la tabla de ruteo en un dispositivo inseguro, esto sirve para aprender los detalles más íntimos acerca del objetivo de la topología de red perteneciente a una organización.
- El programa TraceRoute puede revelar el numero de redes intermedias y los ruteadores en torno al servidor especifico.
- El protocolo Whois que es un servicio de información que provee datos acerca de todos los dominios DNS y el administrador del sistema responsable para cada dominio. No obstante que esta información es anticuada.
- Servidores DNS pueden ser accesados para obtener una lista de las direcciones IP y sus correspondientes Nombres (Programa Nslookup).
- El protocolo Finger puede revelar información detallada acerca de los usuarios (nombres de Login, números telefónicos, tiempo y última sesión, etc.) de un servidor en específico.
- El programa Ping puede ser empleado para localizar un servidor particular y determinar si se puede alcanzar. Esta simple herramienta puede ser usada como un programa de escaneo pequeño que por medio de llamadas a la dirección de un servidor haga posible construir una lista de los servidores que actualmente son residentes en la red.

5.10.7 Bases para el diseño decisivo del firewall

Cuando se diseña un firewall de Internet, se tiene que tomar algunas decisiones que pueden ser asignadas por el administrador de red:

- Posturas sobre la política del Firewall.
- La política interna propia de la organización para la seguridad total.
- El costo financiero del Proyecto "Firewall".
- Los componentes o la construcción de secciones del Firewall.

5.10.8 Políticas del firewall.

Las posturas del sistema firewall describen la filosofía fundamental de la seguridad en la organización. Estas son dos posturas diametralmente opuestas que la política de un firewall de Internet puede tomar:

- "No todo lo específicamente permitido esta prohibido"
- "Ni todo lo específicamente prohibido esta permitido"

La primera postura asume que un firewall puede obstruir todo el trafico y cada uno de los servicios o aplicaciones deseadas necesariamente para ser implementadas básicamente caso por caso.

Esta propuesta es recomendada únicamente a un limitado número de servicios soportados cuidadosamente seleccionados en un servidor. La desventaja es que el punto de vista de "seguridad" es más importante que - facilitar el uso - de los servicios y estas limitantes numeran las opciones disponibles para los usuarios de la comunidad. Esta propuesta se basa en una filosofía conservadora donde se desconocen las causas acerca de los que tienen la habilidad para conocerlas.

La segunda postura asume que el firewall puede desplazar todo el tráfico y que cada servicio potencialmente peligroso necesitara ser aislado básicamente caso por caso. Esta propuesta crea ambientes más flexibles al disponer más servicios para los usuarios de la comunidad. La desventaja de esta postura se basa en la importancia de "facilitar el uso" que la propia - seguridad –

del sistema. También además, el administrador de la red esta en su lugar de incrementar la seguridad en el sistema conforme crece la red. Desigual a la primer propuesta, esta postura esta basada en la generalidad de conocer las causas acerca de los que no tienen la habilidad para conocerlas

5.10.9 Política interna de la seguridad

Tan discutidamente escuchada, un firewall de Internet no esta solo - es parte de la política de seguridad total en una organización -, la cual define todos los aspectos en competentes al perímetro de defensa. Para que esta sea exitosa, la organización debe de conocer que es lo se esta protegiendo. La política de seguridad se basara en una conducción cuidadosa analizando la seguridad, la asesoría en caso riesgo, y la situación del negocio. Si no se posee con la información detallada de la política a seguir, aun que sea un firewall cuidadosamente desarrollado y armado, estará exponiendo la red privada a un posible atentado.

5.10.10 Costo del firewall

¿Cuanto esta dispuesta a ofrecer la organización? por su seguridad, un simple paquete de filtrado firewall puede tener un costo mínimo ya que la organización necesita un ruteador conectado al Internet, y dicho paquete ya esta incluido como estándar del equipo. Un sistema comercial de firewall provee un incremento mas a la seguridad pero su costo puede ser de $32,000 hasta $240,000 pesos dependiendo de la complejidad y el número de sistemas protegidos. Si la

organización posee al experto en casa, un firewall casero puede ser construido con software de dominio publico pero este ahorro de recursos repercuten en términos del tiempo de desarrollo y el despliegue del sistema firewall. Finalmente requiere de soporte continuo para la administración, mantenimiento general, actualización de software, reparación de seguridad, e incidentes de manejo.

5.10.11 Componentes del sistema firewall

Después de las decisiones acerca de los ejemplos previos, la organización puede determinar específicamente los componentes del sistema. Un firewall típico se compone de uno, o una combinación, de los siguientes obstáculos.

- Ruteador Filtra-paquetes.
- Gateway a Nivel-aplicación.
- Gateway a Nivel-circuito.

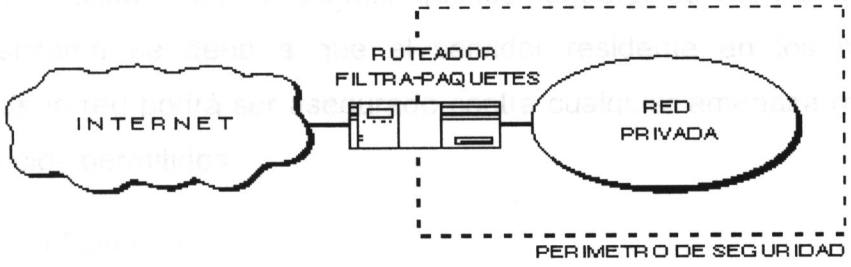
por lo que resta de este subtema, se discutirá cada una de las opciones para la edificación de obstáculos y se describirá como se puede trabajar junto con ellos para construir un efectivo sistema firewall de Internet.

Edificando obstáculos: ruteador filtra-paquetes

Este ruteador toma las decisiones de rehusar/permitir el paso de cada uno de los paquetes que son recibidos. El ruteador examina cada datagrama para determinar si este corresponde a uno de sus paquetes filtrados y que a su vez haya sido aprobado por sus reglas. Las reglas de filtrado se basan en revisar la información que poseen los paquetes en su encabezado, lo que hace posible su desplazamiento en un proceso de IP. Esta información consiste en la dirección IP fuente, la dirección IP destino, el protocolo de encapsulado, la interface de entrada del paquete, y la interface de salida del paquete. Si se encuentra la correspondencia y las reglas permiten el paso del paquete, este será desplazado

de acuerdo a la información a la tabla de ruteo, si se encuentra la correspondencia y las reglas niegan el paso, el paquete es descartado.

Si estos no corresponden a las reglas, un parámetro configurable por incumplimiento determina descartar o desplazar el paquete.



(Figura 1.5) Ruteador Filtra-Paquetes.

Gateways a nivel-aplicación:

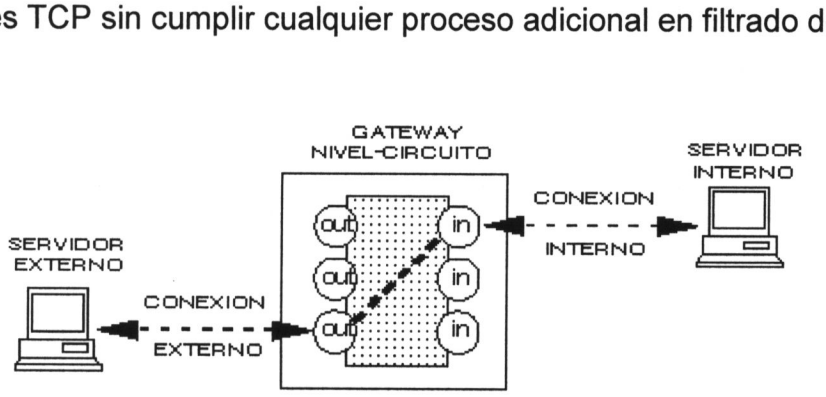
Los gateways nivel-aplicación permiten al administrador de red la implementación de una política de seguridad estricta que la que permite un ruteador filtra-paquetes. Mucho mejor que depender de una herramienta genérica de filtra-paquetes para administrar la circulación de los servicios de Internet a través del firewall, se instala en el gateway un código de propósito-especial (un servicio Proxy) para cada aplicación deseada. Si el administrador de red no instala el código Proxy para la aplicación particular, el servicio no es soportado y no podrán desplazarse a través del firewall.

Servidor de defensa:

Un ruteador filtra-paquetes permite la circulación directa de los paquetes dentro y fuera del sistema, diferente a esto el Gateway a nivel-aplicación deja que la información circule entre los sistemas pero no permite el intercambio directo de paquetes. El principal riesgo de permitir que los paquetes se intercambien dentro y fuera del sistema se debe a que el servidor residente en los sistemas de protección de la red podrá ser asegurado contra cualquier amenaza representada por los servicios permitidos.

Gateway a nivel-circuito:

Un Gateway a nivel-circuito es en si una función que puede ser perfeccionada en un Gateway a nivel-aplicación. A nivel-circuito simplemente trasmite las conexiones TCP sin cumplir cualquier proceso adicional en filtrado de paquetes.



(Figura 1.6) Gateway Nivel-Circuito.

La Ilustración, muestra la operación de una conexión típica Telnet a través de un Gateway a nivel-circuito. Tal como se menciono anteriormente, este gateway simplemente trasmite la conexión a través del firewall sin examinarlo adicionalmente, filtrarlo, o dirigiendo el protocolo de Telnet. El gateway a nivel-circuito acciona como una cable copiando los bytes antes y después entre la conexión interna y la conexión externa. De cualquier modo, la conexión del sistema externo actúa como si fuera originada por el sistema de firewall tratando de beneficiar el encubrir la información sobre la protección de la red.

El Gateway a nivel-circuito se usa frecuentemente para las conexiones de salida donde el administrador de sistemas somete a los usuarios internos. La ventaja preponderante es que el servidor de defensa puede ser configurado como un Gateway "híbrido" soportando nivel-aplicación o servicios Proxy para conexiones de venida y funciones de nivel-circuito para conexiones de ida.

Esto hace que el sistema de firewall sea fácil de usar para los usuarios internos quienes desean tener acceso directo a los servicios de Internet mientras se proveen las funciones del firewall necesarias para proteger la organización de los ataques externos.

VI. Seguridad Física Y Contra Incendios

El concepto de seguridad física y contra incendios es una parte muy importante dentro de las medidas de seguridad del centro de cómputo, aunque es un concepto en el que se tienen amplias medidas adecuadas de protección no siempre resultan ser así [6]

Existen diversos conceptos que se encuentran implícitos en la seguridad física y contra incendios como son:

La ubicación, el acceso, el mantenimiento, la protección, detección y extinción de incendios.

Los elementos señalados con anterioridad deben ser provistos por las brigadas que se conformen en el centro de cómputo para evadir los riesgos e incrementar los niveles de seguridad.

6.1 Los Seguros

Los seguros son un factor muy importante para el desarrollo de las actividades normales en el centro de cómputo que muchas veces se deja por un lado debido a la falta de comunicación entre las empresas aseguradoras y los gerentes en línea o bien los comités de seguridad informática.

Sugiero como primer punto instalar un comité de seguros que reúna a todas las personas de las áreas que se pueden llegar a afectar en un momento dado para poder garantizar que todos los riesgos asegurables se revisen de manera periódica y se llegue así al mejoramiento de la comunicación.

Existen 3 aspectos importantes para asegurar un área en específico del centro de cómputo y son:

[6] Rodríguez, Luis A, *Seguridad de la Información en Sistemas de Cómputo* – p. 49

1.- Los problemas tradicionales como: el entendimiento cabal sobre los riesgos y sus consecuencias.
2.- Las áreas de riesgo asegurables que comprende aspectos como: el ambiente, el equipo, los riesgos por cubrir, los programas y los datos, efectos de las interrupciones, el personal y la responsabilidad a terceras personas.
3.- Los servicios de un seguro especializado: en este aspecto se contempla la gama de servicios y ofertas que manejan las compañías aseguradoras y elegir la mas conveniente para la empresa y principalmente para el centro de cómputo.

6.2 Seguridad De Los Sistemas

La seguridad en los sistemas se refiere a todo lo relacionado con el equipo de cómputo que maneja la institución.
Y esta seguridad incluye:

- Seguridad en la red
- Seguridad en el equipo.
- Seguridad en las terminales.
- Seguridad en los programas de uso general.

La seguridad en la red constituye un área muy complicada en donde un grupo minorista de conocedores en la materia tienen el control debido a la complejidad de las mismas, el riesgo mas elevado al que se enfrentan las redes es al acceso no permitido con el propósito de obtener información confidencial o bien obtener los medios necesarios para tener el control sobre accesos remotos a cuentas bancarias y otro tipo de información financiera.

La seguridad en el equipo es uno de los aspectos muy importantes dentro de la visión de la seguridad en el centro de cómputo ya que el estado en el que se encuentren se proyectaran los resultados de manera veraz y oportuna, los riesgos que existen en el equipo son muy variados y sus causas pueden ser por la mala operación, la cual crea riesgo de negligencia o accidente, por lo tanto es recomendable elaborar, definir e incluir en un manual de operaciones para el personal. Y hasta donde sea posible, vigilar en todo momento el equipo por medio de la observación y/o pruebas sorpresas.

La seguridad en las terminales; es sin duda un aspecto muy importante dentro de la seguridad computacional, aunque siempre se le ha catalogado como equipos poderosos con sistemas complejos, pero para la revisión de seguridad es considerable tratarlas como computadoras pequeñas.

En este aspecto hay que revisar varios elementos para asegurar la calidad de la seguridad, como primer elemento está la ubicación de las terminales con respecto a los usuarios simples, el conocimiento general de dónde se encuentran y el acceso físico a la terminal, lo cual es aconsejable utilizar tarjetas de acceso, claves, huellas digitales etc.... otro aspecto clave es el control sobre la operación no autorizada de la terminal por otros medios de identificación, es recomendable contar con equipo, programas y otros medios de verificación que permitan garantizar que los controles mencionados anteriormente se reforzaran.

La seguridad en los programas de uso general es de vital importancia ya que de la correcta operación de los mismos se llega a un nivel de alta confiabilidad.

La mayoría de los sistemas ya existentes no cuentan con la seguridad necesaria para operar así que la que se requiera implementar tendrá que ser sobre una estructura ya existente.

Las "puertas falsas" representan una amenaza fundamental para la seguridad de los sistemas por lo tanto en la seguridad de programación se pretende:

1. Restringir el acceso a programas y archivos.
2. Asegurar que los operadores trabajen sin la supervisión minuciosa y no modificar los programas ni los archivos
3. Asegurar la utilización de los datos, archivos, y programas correctos en el procesamiento.

En general las tres áreas antes mencionadas han tenido grandes avances y mejoramientos, pero se corre el riesgo de que aún existan muchas "puertas falsas" que aún no se identifican.

6.3 Planes Y Simulacros

La mayoría de las instituciones, tienen la seguridad de que cuentan con planes necesarios para hacer frente a cualquier situación que se les pudiese presentar, pero esta comprobado que muchas de estas estrategias no hacen la fuerza necesaria antes dichos desastres ya que no están bien estructurados y en algunos casos son superficiales.

Una de las principales objeciones para llevar a cabo los simulacros son los costos que representan, pero el precio varía de acuerdo a la magnitud de la prueba.

Para poder realizar un buen plan de simulacros es necesario contemplar los tipos de desastre que puedan surgir, un alcance bien proyectado de la planeación contra desastres, las aplicaciones que están en proceso de desarrollo, aplicaciones terminadas y los simulacros mismos.

6.4 Tipos De Desastre

Se manifiestan de múltiples formas y su magnitud puede afectar:

1.- Destrucción total o parcial de los recursos de procesamiento de datos.

2.- Mal funcionamiento o destrucción de recursos ambientales destinados al procesamiento centralizado de datos como pudieran ser la energía, el aire acondicionado etc....

3.- Destrucción total o parcial de procedimientos manuales del usuario, utilizados para la captura de la información de entrada para los sistemas de cómputo.

4.- Pérdida del personal de cómputo clave.

5.- Interrupción por huelga.

Se sugiere en general que los procedimientos de planeación contra desastres se tienen que considerar cuidadosamente ya que los tipos de desastres que se presentan en este trabajo de investigación para cada suceso recomiendan compilar y analizar planes específicos para cada situación.

6.5 La Planeación Contra Desastres

En este punto se considera que se deben salvaguardar tanto los sistemas que están en desarrollo como los que están en operación siendo estos últimos de vital importancia se consideran ciertas áreas para asegurar, las cuales se recomiendan:

1.- Toda la documentación existente a cerca de los sistemas, la programación y operaciones.

2.- La mayoría de los recursos que abarquen:

- Todo tipo de equipo
- El ambiente necesario para el equipo
- Los datos y archivos
- Programas
- Papelería

En cuánto al equipo se debe de asegurar todo el que se esté utilizando en todas las etapas del desarrollo de los sistemas:

- Equipo de terminal
- Equipo de Procesamiento
- Equipo ambiental (aire acondicionado, energía)
- Recursos de distribución

De los Datos y Archivos, para la organización es primordial tener al día, en orden, y de manera sistematizada la información; por lo tanto se recomienda tener respaldo digital y en papel (legible para la computadora) los manuales de operación en los cuartos protegidos con la finalidad de evitar que en el caso de una pérdida material se evite el tiempo de recaptura de la información.

De la Papelería, para surtir de manera continúa la papelería se lleva un considerable lapso de tiempo, por tanto es necesario que el área de informática pueda contar con existencias de papelería de emergencia, las cuales es recomendable guardar en otro lugar para evitar dificultades y acarrear a la destrucción del depósito central de papelería que por lo general incluye: Datos Fuente y Documentos de Informes y resultados como pudieran ser facturas y balances.

6.6 Alcance de los Procedimientos en caso de desastres

Paras este procedimiento se requiere que cada aplicación o sistema cuente con lo procedimientos por escrito. Ya que en ellos se deberán diferenciar los diversos tipos de desastres que pueden ocasionar la pérdida. Por tanto es necesario especificar con claridad:

1.- Las responsabilidades en caso de desastre y la organización que entra en vigencia

2.- Y la acción inmediata a seguir:

* Organización y responsabilidades para los procedimientos de recuperación.
* Clasificación por tipo de desastre
* Evaluación de daños
* Determinación de Prioridades
* Información de la situación a los usuarios y a la gerencia general
* Plan de acción para la recuperación.

3.- Los planes contra desastres deben ser los mas detallados que sea posible. Las personas tienden a olvidar cuando sucede un desastre no hay tiempo para pensar en que hacer en ese momento. Muchas veces es posible anticiparse a la mayoría de situaciones y éstas deben estar cubiertas en el plan contra desastres.

4.- Todo el personal requiere de adiestramiento regular en el plan contra desastres. Muchas veces se pasa por alto el hecho de que muchas instituciones de procesamiento de datos, el número de empleados es alto, pero se debe considerar que tiene la organización más por ganar aun cuando el personal es mayor para hacer frente a cualquier situación de desastre.

5.- La aplicación de las prácticas que son convenientes para aumentar la seguridad se debería hacer como rutina, un ejemplo claro de esta situación es cerrar las cajas de seguridad para datos en medios magnéticos después de que los archivos o discos se hayan recuperado.

Los planes y documentación contra desastres es conveniente que los sepa un pequeño grupo del personal, pero lo suficientemente grande como para garantizar

una extensa diversificación. Aunque por otro lado la información excesiva constituye una amenaza para la seguridad.

6.7 Plan de Contingencia

Un plan de contingencia o bien un plan de recuperación en caso de desastres es una guía para la restauración rápida y organizada de las operaciones de cómputo después de una suspensión. Especifica quién hace que y como. Los objetivos de dicho plan son los de restablecer, lo mas pronto posible, el procesamiento de aplicaciones críticas para posteriormente restaurar totalmente el procesamiento "normal". Un plan de contingencia no duplica un entorno comercial normal, pero si minimiza la pérdida potencial de activos y mantiene a la empresa operando, al tomar acciones decisivas basadas en la planeación anticipada.
Planteando la definición de otro modo es un programa de recuperación de la organización, la base de este plan es una decisión de la organización sobre que aplicaciones del procesamiento de datos son las mas importantes de proteger y recuperar.

6.8 Contexto de la Planeación de Contingencia

- Aseguradores: Como anteriormente se explicó en el **capítulo XII** punto 12.1 la importancia de los seguros, con los cuales se transfiere el riesgo en lugar de asumirlo o minimizarlo.

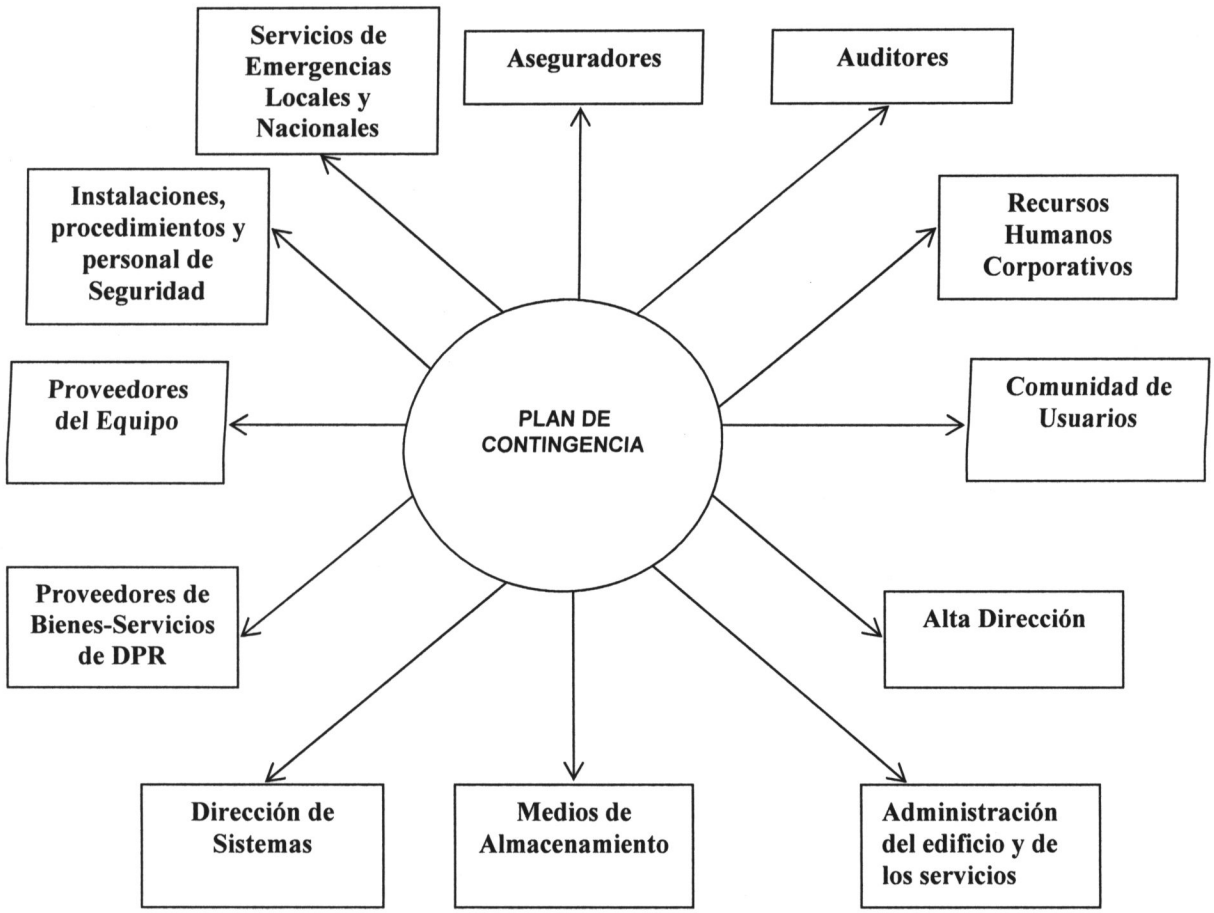
- Recursos Humanos Comparativos: Ya se mencionó también la importancia de la participación activa de todas las áreas de la orgnización y la división de responsabilidades.

- Administración del Edificio y de los Servicios: Sobre todo en los casos en que la organización no es propietaria del edificio en que se asienta, es importante que

establezca contacto con la inmobiliaria o el arrendatario con respecto a temas como el funcionamiento de la electricidad, el aire acondicionado etc....

- Proveedores de Bienes y Servicios de DRP (Disaster Recovery Planning); se refieren principalmente a los servicios de backup site y almacenamiento de medios de información, así como consultoría en planes de contingencia.

A continuación se muestra la plétora de entidades que conforman el medio ambiente en el que se desarrolla el esfuerzo de la planeación de contingencia:



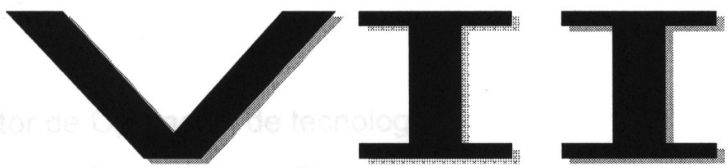
(fig 13.1)

Disaster Recovery Plan

(Plan De Recuperación contra Desastres)

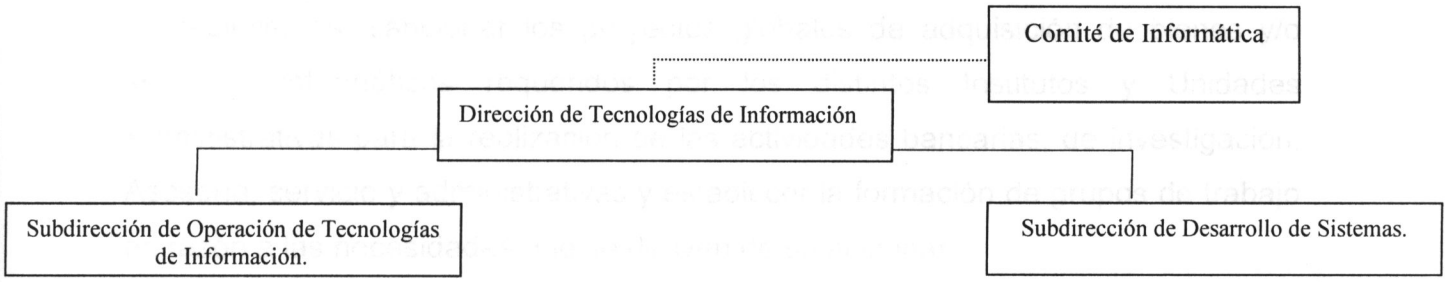
"Un plan de contingencia es un plan escrito en el que se detallan acciones, procedimientos y recursos que deben usarse durante un desastre que cause destrucción parcial o total de los servicios de computación. En este plan se define que tareas son críticas, quien es el responsable de todos los aspectos del proceso de recuperación, y cómo va a funcionar la organización mientras los sistemas están siendo reparados o transportados a un nuevo local"[7]

[7] Rodríguez, L. A, *Seguridad de la Información en Sistemas de Cómputo* – p. 161



EL COMITÉ DE INFORMÁTICA

VII. El Comité De Informática



El **comité de Informática**, se encuentra en línea staff a la dirección y está conformado por: [8]

- Subdirector de Operación de tecnologías.
- Subdirector de Desarrollo de Sistemas.
- Administrador de la Infraestructura.
- Administrador de la Base de Datos
- Encargado de Operación y Producción.
- Lideres de Proyectos.
- Planeación Tecnológica.
- *Desarrollo de Sistemas.*
- Administrador de Ambientes Web.

[8] Referencia del Banco de México - FIRA

7.1 Responsabilidades

El objetivo del Comité será el de establecer las políticas, normas, lineamientos y procedimientos; sancionar los proyectos globales de adquisición de bienes y/o servicios informáticos requeridos por los distintos Institutos y Unidades Administrativas para la realización de las actividades bancarias, de investigación, Asesoría, servicio y administrativas y establecer la formación de grupos de trabajo *en razón a las necesidades que se deriven de su accionar.*

Dar seguimiento a los proyectos que permitan la adecuada aplicación y aprovechamiento de esta tecnología en el quehacer que desarrollan las Instituciones y Unidades Administrativas de la banca, para mejorar la calidad de los servicios que proporcionan.

En concreto sus principales actividades serian:

- Identificación de la problemática y propuesta de solución
- Definición de proyectos prioritarios
- Diseño e implementación de instrumentos concertados de política informática que promuevan el desarrollo y uso adecuado de la tecnología
- *Concertar acciones para el desarrollo de proyectos comunes y/o de interés general.*
- *Elaborar y/o actualizar el Programa Institucional de Desarrollo Informático de la organización*

7.2 Adquisición De Software

Par la adquisición de nuestro Software contamos con 4 opciones:

- Desarrollo Interno
- Desarrollo por Contrato
- Paquete Adquirido
- Sistema Transportado

Desarrollo Interno: La institución recurre a sus propios miembros del personal para la planificación, la definición, el análisis, el diseño y la ejecución de las aplicaciones. Puede contratarse personal nuevo o existente en sistemas de información y tecnología.

Desarrollo por Contrato: Esta opción implica contratar a una organización para el desarrollo de Software para el diseño y la implementación de las aplicaciones necesarias para la institución teniendo como principal ventaja Control estricto en los costros del desarrollo.

Paquete adquirido: Incluye todo esquema mediante el cual la organización adquiere los programas de computación y, con frecuencia, también los requisitos asociados para la Instalación de otra organización bajo un contrato de compra o licencia, esto es de aplicación para un sistema informático interno o para el uso.

Sistema Transportado: En esta opción incluimos la adquisición de un sistema "como es" de otra organización donde se desarrollo el sistema y se encuentra en producción. Esta opción requiere la implementación con equipos Internos o compartir los medios de computación y la red con la organización de Origen.

7.3 Adquisición De Hardware

Para la adquisición de hardware, la Institución bancaria efectúa una Licitación que contiene el número de equipos, características etc. de acuerdo a las necesidades del área con el siguiente Formato

I. OBJETO DEL PROCESO

La presente Licitación tiene por objeto la adquisición de Hardware.

II. DESCRIPCIÓN BÁSICA DEL OBJETO DEL CONCURSO

La presente licitación busca seleccionar a una empresa que provea de partes y piezas computacionales.

III. CÓDIGO DEL OBJETO DEL PROCESO:

523904

IV. VALOR REFERENCIAL:

Monto Económico

V. FUENTE DE FINANCIAMIENTO:

Recursos Directamente Recaudados

VI. LUGAR DE ENTREGA DEL BIEN:

VII. BASES:

1. Costo
2. Lugar de Venta y Entrega
3. Horario de Atención

VIII. CALENDARIO

1. Convocatoria Pública
2. Venta de Bases
3. Presentación de Consultas
4. Absolución de Consultas
5. Observación a las Bases
6. Integración de las Bases
7. Presentación de Propuestas
8. Evaluación de Propuestas
9. Otorgamiento de la Buena Pro

7. 4 Análisis Para El Diseño De Los Sistemas

El comité de informática en conjunto con el líder de proyectos supone las siguientes etapas para el desarrollo de los mismos.

Identificación de Metas Globales

Reconocimiento del programa.

Evaluación y Síntesis del Sistema.

Modelado

Especificación

Revisión.

Estudio de Viabilidad

Viabilidad económica. (Evaluar Costos comparándolos con ingresos o beneficios).

Viabilidad Legal (Leyes e Infracciones).

Análisis Costo – Beneficio.

Modelado de la arquitectura del sistema.

Creación de un modelo idéntico pero de menor escala.

Especificaciones del Sistema.

Ingeniería de Hardware.

Ingeniería de Software.

Ingeniería de Bases de datos.

Ingeniería Humana.

Desarrollo.

Diseño de los datos Necesarios.

Datos necesarios

Diseño Arquitectónico.

Relación entre cada uno de los elementos estructurales.

Diseño de la Interfaz.

Comunicación del sistema con operadores, usuarios y consigo mismo.

Diseño de Procedimientos.

Transformación de elementos estructurales.

El diseño = La Calidad

Proceso y modelado a la vez.

Diseño de Salida

Resultados e Información generados.

Diseño de Archivos

Naturaleza y Contenido

Datos Incluidos

Longitud del registro.

Secuencia de registros en los archivos.

Diseño de Interacciones con las Bases de Datos.

Administradores.

Usuarios.

Implantación

Responsabilidad a Grupos

Estrategias para el entrenamiento.

Plan de Conversión.

Formulación de medidas de desempeño.

Capacitación.

Capacitación a usuarios del Sistema.

Objetivos de la capacitación.

Evaluación del Sistema.

Evaluación Operacional.

Impacto Organizacional.

Desempeño del desarrollo.

Prueba del Sistema

VIII

AUDITORÍA INFORMÁTICA

VIII. AUDITORIA INFORMATICA

Este es un tema esencial dentro de las organizaciones para garantizar la efectividad de los procesos y procedimientos generales y en esencia los de seguridad.

Con frecuencia y dependiendo de la magnitud de las organizaciones se cuentan con la opción de dos tipos de auditores; los Internos y Externos, los primeros tienen un acercamiento mas continuo con la organización, por lo tanto son de su conocimientos todos lo documentos, hechos, y en general todo lo relacionado con los movimientos de la organización.

En muchas ocasiones el trabajo del auditor externo se puede facilitar si la organización y en específico el auditor interno mantiene en orden los procedimientos y pocas serán ya las áreas por cubrir de los auditores externos.

La auditoría Informática se puede definir como la revisión y examen sistemático de una actividad o actividades que realiza personal independiente, de la operación dentro de una organización. La Auditoría es de apoyo a la función directiva.

A medida que la auxilie en la toma de decisiones, evite desperdicios, dispendios, deficiencias, desviaciones y mejore la gestión. Induzca a la corrección y ponga en vigor las propuestas para la optimización de las operaciones.

Está orientada a la verificación, examen, evaluación de la organización la planeación de los controles internos, para el efectivo logro de las metas y objetivos de la dependencia o entidad sujeta a revisión.

Cada uno de estos términos se pueden considerar como diversas etapas consecutivas y secuenciales, referentes a:

- La comprobación
- Investigación
- Análisis
- Prueba de las operaciones
- Calificación y cuantificación de las operaciones y sistemas de control

Lo anterior con el objetivo de comprobar:

- Si son adecuadas.
- Si son o no suficientes o excesivas,
- Si favorecen la productividad y
- Si realizan con apego a la normatividad vigente.

El último fin de la auditoría informática es determinar el grado de economía, impacto, efectividad, eficacia y eficiencia en el manejo del los recursos para el efectivo logro de la seguridad, metas y objetivos.

8.1 Objetivos De La Auditoría Informática [9]

A) Verificar, examinar y evaluar:

Si los recursos informáticos, financieros, humanos y materiales son adquiridos en términos de economía y seguridad en Cantidad, Calidad y Costo, y Si se manejan con eficiencia, garantizando que los mismos resulten suficientes y no excesivos. Guardando una adecuada relación entre el costo de los bienes producidos y los beneficios de su utilización, para alcanzar de manera eficaz los objetivos y metas.

B) Determinar errores, excesos e irregularidades:

En sus causas y efectos, así como, emitir conclusiones y recomendaciones, que coadyuven a la mejora de la operación, para el adecuado cumplimiento de objetivos y metas.

C) Dar puntual seguimiento a la implementación de las recomendaciones preventivas y correctivas, para determinar el grado en que son atendidas.

8.2 Ubicación De La Auditoría Informática En El Proceso Administrativo

El proceso administrativo se divide en varias etapas, para el efecto de nuestro estudio consideráremos cuatro:

A) Planeación
B) Organización
C) Dirección y
D) Control.

La Planeación comprende, la elaboración de los planes, políticas, procedimientos, reglamentos, programas de trabajo y la presupuestación.

La Organización se refiere a la definición de una estructura organizacional funcional, apta y adecuada a los respectivos individuos, definición de un marco jurídico, desarrollo de la reglamentación interior, plantillas de personal autorizadas, catálogo de puestos, desarrollo de sistemas y procedimientos administrativos, etc.

La Dirección se refiere a las actividades o funciones que tienen que realizar la alta gerencia y los niveles medios para que funcione la organización.

El Control es la función encargada de revisar, analizar y evaluar todos los sistemas de control, políticas, y otros documentos con que cuentan la organización y es en esta etapa se ubica la función de auditoría.

[9] Curso de Auditoría FIRA 2003

8.3 Planeación De La Auditoría Informática

Para el cabal entendimiento, se deben definir una planeación a largo plazo para la información y establecer 2 lineamientos:

- Los Lineamientos de Control
- Los Lineamientos de Auditoría

Los lineamientos de control son los que deben de permitirse el acceso a un lugar X sólo al personal autorizado.

Los lineamientos de Auditoría se revisarán los procedimientos relacionados con el acceso a ese lugar X

Para los lineamientos de control, la alta gerencia debe identificar las metas a largo plazo del departamento de sistemas de información y verificar que éstas sean coherentes con las metas organizacionales, Y;

Para los lineamientos de auditoria se deben de revisar los planes a largo a plazo de la gerencia y evaluar la coherencia de las metas a largo plazo del departamento de sistemas de información con las metas organizacionales.

8.4 Revisión De La Auditoría Informática

Con el objeto de dar a la función de control un enfoque moderno, la auditoría deberá orientarse a:

- Fortalecer las acciones preventivas.
- Dar seguimiento a los programas.
- Evaluar el desempeño en todos los niveles de cada área de la dependencia o entidad.
- Promover la creación de un ambiente de autocontrol, autocorrección y autoevaluación.

Estos tres conceptos anteriores deberán formar parte de la estrategia global orientada a la modernización administrativa.

1. Fortalecer las acciones preventivas,
2. Dar seguimiento a los programas, reglamentos, políticas y
3. Evaluar el desempeño en todos los niveles de cada área de la organización
4. Promover la creación de un ambiente de autocontrol, autocorrección y
5. autoevaluación,

8.5 Normas Generales de la Auditoría

Estas normas, aunque de aplicación generalizada para la profesión de contadores públicos, deberán ser observadas por las personas que practiquen auditoría de cualquier tipo, independientemente de su profesión.

Las normas generales de auditoría son once, con sus respectivos pronunciamientos, y se pueden presentan en tres grupos:

- Normas personales.
- Normas sobre la ejecución del trabajo
- Normas sobre el informe de auditoría y seguimiento

Las normas personales comprenden:

Independencia:

asuntos relacionados con su actividad profesional, el auditor debe mantener: Soberanía de juicio, Ser autónomo, y Objetivo, ser independiente desde el punto de vista organizacional y mantener una actitud independiente.

A) Soberanía de juicio.

Durante el desarrollo de su trabajo, el auditor sostendrá en todo tiempo el señorío de su juicio profesional, guiándose exclusiva y libremente por su criterio en la planeación de sus revisiones en la selección y aplicación de procedimientos, técnicas y pruebas de auditoría, en la definición de sus conclusiones y en la elaboración de su informe.

B) Imparcialidad.

El auditor está obligado a abstenerse de intervenir, con ese carácter, en los casos en que existan hechos, situaciones o relaciones que impidan su independencia, vulnerando la absoluta imparcialidad de criterio.

En caso de que, aún existiendo alguna limitación, el auditor se viere obligado a practicar la auditoría, hará constar expresamente en su informe la situación en que se encuentra.

C) Objetividad.

En el desarrollo de su trabajo, el auditor se apoyará en hechos y evidencias que lo lleven al convencimiento razonable de la realidad o veracidad de los actos, documentos o situaciones examinados, que le permitan conformar una base firme para la emisión de sus juicios y opiniones.

Las normas sobre la ejecución del trabajo comprenden:

Planeación.

Previamente a la ejecución del trabajo de auditoría, el auditor deberá realizar una investigación para definir sus objetivos, alcances, procedimientos, recursos, tiempos y oportunidad de los mismos precisándolos en su programa de trabajo.

Examen y evaluación de los sistemas de control.
El auditor público deberá efectuar un adecuado examen del control operativo y contable establecido en área sujeta a revisión.

Supervisión del trabajo de auditoría.
El personal debe ser cuidadosamente supervisado.

Obtención de la evidencia.
El auditor deberá realizar, con la amplitud que estime necesaria, las pruebas adecuadas para obtener evidencia de calidad que fundamente, objetiva y razonablemente, sus conclusiones y recomendaciones.

Papeles de trabajo.
La evidencia se deberá documentar en papeles de trabajo.

Tratamiento de irregularidades.
El auditor deberá prestar especial atención a aquellas transacciones o situaciones que denoten indicios de irregularidades, haciéndolas del conocimiento de las autoridades competentes (Comité de Informática o Gerencia General)

Normas Sobre el Informe de Auditoría y su Seguimiento.

El informe de auditoría.
Al término de cada intervención, el auditor presentará a la autoridad competente, por escrito y con su firma, un informe acerca de la auditoría practicada.

Seguimiento de las recomendaciones.

El auditor hará el seguimiento de las acciones correctivas adoptadas como resultado de las observaciones y recomendaciones contenidas en el informe de *auditoría*.

El cumplir con estas normas, en su esencia y en su filosofía, permite tener un parámetro y un medio de comparación de la manera en que se desarrolla la actuación del auditor. Su observancia es de carácter obligatorio para los órganos internos de control.

El apego a estas normas y pronunciamientos, permitirán dar uniformidad a las tareas de control y auditoría, además de establecer los niveles de calidad que deben cumplirse en su desarrollo.

POLÍTICAS Y REGLAMENTOS GENERALES DE UN CENTRO DE CÓMPUTO

IX. POLITICAS Y REGLAMENTOS GENERALES DEL CENTRO DE CÓMPUTO.

Del objeto

1. Estos criterios establecen los ordenamientos y lineamientos para el acceso y uso de los sistemas instalados en la Red de Cómputo, La estrategia informática de la Red de Cómputo estará orientada hacia los siguientes puntos:

    - Plataforma de sistemas abiertos.
    - Esquema de operación bajo el concepto cliente-servidor.
    - Estandarización en equipos, paquetes y estructuras de datos.
    - Intercomunicación entre las distintas áreas y sus equipos a fin de integrar bases de datos.
    - Intercambio de experiencias y capacitación.

2. Para efectos de estos criterios las áreas que se mencionan serán las mismas que conforman y que por alguna característica están separadas unas de otras.

3. Para el uso de la Red de Cómputo de Información será necesario que se cumplan con los requisitos y los usuarios acaten invariablemente los ordenamientos y lineamientos que inciden en la contratación y el uso de los bienes y servicios informáticos establecidos en estos criterios.

De la Infraestructura de La Red de Cómputo

4. La infraestructura de la Red de Cómputo está comprendida por el cableado de fibra óptica, el cableado en cobre, los equipos concentradores, antenas de telecomunicaciones y demás equipos de conexión distribuidos en las regionales

5. Los equipos conectados a la Red de Cómputo son parte de la Organización, y el cual forma parte de su infraestructura.

6. Los equipos que forman parte de la infraestructura de la red y que fueron instalados en alguna oficina se encuentran en calidad de resguardo y ésta se hará responsable por el buen uso de los mismos y de avisar al Centro de Cómputo, en caso de fallas o descomposturas.

7. Los concentradores y servidores deberán permanecer encendidos las 24 horas del día durante todo el año y sólo serán apagados en caso de mantenimiento o reemplazo o previo acuerdo con el Centro de Cómputo.

8. Las intervenciones a la Red parte del personal del Centro de Cómputo que ocasionen contratiempos, deberán de realizarse previo acuerdo entre el Centro de Cómputo y el usuario.

9. Las áreas que necesiten desconectar algún(os) equipo(s) de la Red deberán dar aviso por escrito al Centro de Cómputo al menos con un día hábil de anticipación, para tomar las medidas preventivas correspondientes, ya que los equipos instalados a través de la Red de Cómputo no deberán ser manipulados o reubicados sin autorización.

10. Para la adquisición de equipos de computación que se vayan a integrar a la Red, se deberán seleccionar tomando en cuenta calidad, compatibilidad, desarrollo tecnológico, capacidades, deberán de tener una garantía mínima

de un año y se deberá contar con el servicio técnico correspondiente en el país.

Ningún usuario esta autorizado para conectar o desconectar equipo en los puertos de los concentradores que pertenecen a la red. En caso de que exista necesidad de hacerlo, el encargado del área deberá comunicarse al Centro de Cómputo.

Usos y Servicios de la Red de Cómputo

11. Los servicios de la Red de Cómputo están basados en necesidades de administración.

12. Dependiendo del perfil del usuario y sus necesidades la Red de Cómputo ofrecerá los siguientes servicios:

I.-Correo Electrónico. Herramienta de comunicación personal entre usuarios dentro y fuera de la institución. El Centro de Cómputo no se hará responsable del contenido que se transmita.

II.-Acceso Remoto: Es el uso de servicios provistos por operaciones computacionales por medio de las redes locales, regionales, nacionales y mundiales.

III.-Espacio en Disco: El Centro de Cómputo determinará la cantidad de espacio en disco en los servidores de la Red de Cómputo que podrá ser utilizado por los usuarios.

IV.-Uso de programas y archivos de dominio público: Son aquellos programas y/o archivos en la Red de Cómputo que pueden ser copiados y distribuidos libremente.

13. Todos los usuarios que deseen emplear uno o más servicios de la Red de Cómputo, deberán contar con equipo de Cómputo, su registro de usuario y los permisos de las áreas involucradas en el uso de estos servicios.

14. Para hacer uso de la Red de Cómputo deberá contar con una cuenta personal que no podrá compartir ni a hacer mal uso de ella.

15. Cuando el usuario requiera la ampliación de servicios que se le ofrecen, deberá presentar solicitud escrita al Centro de Cómputo.

De la Seguridad de la Red de Cómputo

16. El Centro de Cómputo tiene la obligación de vigilar la seguridad de los sistemas instalados en la Red de Cómputo. Los sistemas operativos y programas comerciales empleados deberán estar registrados y no se deberán copiar o instalar en otros equipos. Para garantizar el uso de los programas operativos y comerciales se deberán de asegurar un número adecuado de licencias, para tener un control mas exhaustivo el órgano de control interno por medio de sus auditorias internas tendrá un control mas especifico en el SW

17. Se mantendrá la privacidad de los usuarios y no se examinará el contenido de los archivos o programas, excepto durante las operaciones normales de mantenimiento como son los respaldos, instalaciones y otros.

18. Las áreas que posean equipo que estén conectados en la Red de Cómputo deberán contar con un plan de contingencias tomando en cuenta las recomendaciones o sugerencias del Centro de Cómputo.

De las autoridades en el control de infraestructura de la Red de Cómputo

19. El mando Superior tomando en cuenta la opinión de los funcionarios de primer nivel será el responsable de revisar y aprobar los criterios para el uso de la red de cómputo a propuesta del centro de cómputo.

20. El Centro de Cómputo, por medio del personal de soporte técnico será el responsable del funcionamiento, mantenimiento y actualización de la red de cómputo y para los efectos previstos adquiere las siguientes actividades y obligaciones:

I.-Elaborar, divulgar y actualizar los criterios para el uso de la Red de Cómputo.

II.-Vigilar que se respeten los criterios de la Red de Cómputo en todas las áreas.

III.-Instalar el cableado, equipo y el software necesarios para que las distintas áreas queden integradas a la Red de Cómputo.

IV.-Controlar el uso de los recursos de la red como son equipos, impresoras, repetidores, concentradores, programas y todos aquellos a que se refieran las políticas respectivas.

V.-Registrar y asignar las cuentas de los usuarios que utilicen alguno de los servidores administrados por el Centro de Cómputo.

VI.-Ayudar a los usuarios a resolver problemas que se susciten en el uso de las redes como lo son los aspectos de seguridad, asignación de cuentas y de derechos, acceso a aplicaciones y servicios.

VII.-Mantener el acceso a la Red de Cómputo a todos los usuarios registrados y autorizados.

VIII.-Coordinar la configuración, instalación, manejo y control de sistemas de telecomunicaciones.

IX.-Elaborar los reportes o informes periódicos acerca del uso y la explotación de la red, así como conformar un archivo histórico.

X.-Llevar una relación de los equipos y áreas que se enlazaron a la red y actualizarlos periódicamente.

XI.-Evaluar las nuevas utilerías o sistemas para ser empleados en la red, ya sea para su administración o para su explotación.

XII.-Sugerir, organizar y capacitar a los usuarios sobre el uso de las redes, aplicaciones, servicios disponibles y en el manejo de equipos que los administradores del control de la red consideren necesarios.

XIII.-Salvaguardar la confidencialidad de la información que en las áreas se maneje.

De los Usuarios de la Red de Cómputo

21. Los usuarios de la Red de Cómputo se clasifican como sigue:

I.-Administradores de red.
II.-Personal que labora
III.-Usuarios externos.

22. Todos los usuarios de la Red de Cómputo tienen como obligaciones:

I.-Solicitar su registro y cuenta de usuario de acuerdo al procedimiento establecido en el Centro de Cómputo y guardar una copia del mismo.

II.-Respetar las normas y políticas que fuesen emitidas sobre la red de Cómputo, guardar estrecha relación con el personal de soporte técnico del centro de cómputo y seguir las instrucciones que de estos reciba.

III.-Solicitar la conexión de los equipos que desee conectar a la red institucional.

IV.-Responsabilizarse de todo el correo electrónico que maneje con su cuenta.

V.-Informar al Centro de Cómputo de los problemas que tenga con la red de cómputo a la brevedad posible.

VI.-Informar al personal técnico del Centro de Cómputo sobre las modificaciones que el área necesita: cambio de lugar, configuración, ampliación, renovación y supervisión de equipo.

VII.-Conservar la documentación sobre los programas y manuales de los equipos y software que sean utilizados.

VIII.-Conservar la integridad y buen funcionamiento de los equipos que conforman la infraestructura de la red de cómputo.

IX.-Realizar los respaldos de su información.

X.-Verificar que los archivos, programas y medios magnéticos que emplea para la transportación y almacenamiento de información estén libres de virus informáticos.

XI.-Capacitarse mediante cursos, conferencias y documentación disponibles así como asistir a los cursos sobre el manejo de equipos o paquetes.

XII.-Asistir a las reuniones de información que el Centro de Cómputo convoque.

XIII.-Permitir el acceso al personal de soporte técnico del Centro de Cómputo, a fin de poder realizar las revisiones e instalaciones necesarias.

Del Ancho De Banda

23. El ancho de banda es la capacidad que tiene una conexión para transmitir datos. Cuando se transmite una cantidad excesiva de datos, la conexión se puede llegar a saturar ocasionando un cuello de botella que afecta a todos los usuarios por igual. Para evitar esto, se han definido los siguientes lineamientos:

I.- No se permite la instalación de servicios de Internet de acceso público y masivo, como son los servidores de FTP, IRC y Boletines Electrónicos (BBS), etc. los cuales deberán ser en su caso institucionales, únicos, con restricciones en su acceso e instalados en un servidor administrado por el Centro de Cómputo.

De las Prohibiciones

24. Queda prohibido a los usuarios:

I.-El acceso a archivos y/o datos pertenecientes a otros usuarios sin su previo y expreso consentimiento.

II.-El consumo masivo de recursos cuando ya fueron avisados de cesar tal actividad.

III.-El empleo de recursos y facilidades de la Red de Información con fines comerciales ó lucrativos.

IV.-El intento de la falsificación de mensajes por correo electrónico.

V.-El uso de la Red de Cómputo para intentar acceder sistemas remotos sin autorización.

VI.-El uso de la Red de Cómputo para emplear servicios recreaciones provistos por sistemas remotos o de la instalación y uso de juegos y/o programas recreativos.

VII.-El uso de los equipos pertenecientes a la Red para fines diferentes a los especificados en el momento de su instalación.

VIII.-Todo intento por modificar la cantidad de espacio asignado dentro de la red de cómputo y/o toda forma de alteración de derechos otorgados por el Centro de Cómputo.

IX.-La desencriptación de los passwords de los usuarios o cualquier modificación del material registrado contenido en la Red de Cómputo.

X.-Cualquier intento de acceder a información de la institución financiera cuando no se tenga autorización de hacerlo.

XI.-Cualquier intento de accesar equipo de cómputo o áreas en disco a las que no tenga acceso autorizado.

XII.-La copia de archivos de material registrado contenido en la red de cómputo sin disponer de la licencia correspondiente.

XIII.-Modificar la configuración del hardware y/o software necesario para acceder la Red de Cómputo que el personal del Centro de Cómputo le haya instalado en el equipo.

XIV.-Asignar direcciones IP nuevas sin haber consultado previamente con los administradores de la red.

XV.-Proporcionar información falsa con el fin de tramitar el acceso a la Red de Cómputo.

XVI.- Facilitar, prestar, rentar o vender a otra persona su cuenta personal (login y password).

De las Sanciones

25. Las faltas cometidas por los usuarios al presente reglamento serán evaluadas por el Centro de Cómputo para determinar su gravedad las cuales podrán ser de dos tipos.

    a) Faltas graves.
    b) Faltas leves.

26. Se consideran faltas graves aquellas violaciones a las prohibiciones que después de haber sido reconvenido por parte del Centro de Cómputo reincidieran o que realicen lo siguiente:

    I.-El intento por modificar los privilegios o cuentas asignados a los usuarios en la red de cómputo.

    II.-El acceso a computadoras o áreas en disco a las que no se tenga autorización para hacerlo.

    III.-El intento por "hacer caer" los sistemas de la Red de Cómputo.

    IV.-El mal uso de los equipos que fueron instalados por el Centro de Cómputo.

    V.-Crear conflictos de comunicación en la red, por la mala instalación de software y hardware.

    VI.-La violación a los lineamientos especificados en la sección 32 capítulo I, referente al "ancho de banda".

27. Se consideran faltas leves aquellas en la que los usuarios no sigan las instrucciones que reciban de parte de Administradores de la Red y reciban una primera amonestación escrita por parte del Centro de Cómputo con copia al jefe del área correspondiente.

28. Las sanciones se aplicarán de acuerdo a la gravedad y serán:

I.-Retirar el equipo instalado del área correspondiente en conflicto, el cual será instalado en otra dependencia.

II.-Suspensión de la cuenta y desconexión del equipo hasta resolver la situación.

III.-Revocación temporal o definitiva del acceso a la Red de Cómputo.

CONCLUSIONES Y RECOMENDACIONES

Es un hecho que una dirección de Sistemas es un departamento de servicios, en que los clientes son sus propios empleados y áreas de la empresa, y que son ellos los que ocupan de sus servicios, los cuales, son tan importantes como los que se le ofrecen a los clientes externos; porque aunque erróneamente se crea un departamento de servicios solo ocasiona gastos y no genera ingresos, estos últimos están implicitos en los ahorros que promueve y que logra a través de un adecuado manejo de la información.

Durante la investigación y en el asentamiento del tema que elegí para Tesis puedo concluir que la vida diaria y laboral se alimenta con información, misma que es procesada en grandes cantidades por unidades administrativo – operativas como los centros de cómputo.

En las organizaciones dichos centros varían en tamaños, formas, lineamientos y marcas de acuerdo a la capacidad de infraestructura de las organizaciones. Tuve la vivencia personal de conocer durante esta investigación; desde grandes edificios inteligentes con la tecnología de punta lista para alimentar todo el territorio nacional hasta recintos de 4 x 4 m^2 que procesaban la información de 6 terminales, pero todos los centros de cómputo inciden en la necesidad de seguir normas y procedimientos para la operación efectiva y asegurar en la medida posible las funciones normales del centro de cómputo así como el surgimiento de una necesidad de organización y división de responsabilidades para hacer frente al trabajo diario que exigen los sistemas de información y trabajar de una manera ordenada y responsable.

Finalmente puedo sugerir de manera personal primero una estructura organizacional de un centro de cómputo, ya que hay organizaciones en las que los sistemas son manejados por múltiples personas sin los conocimientos, restricciones y cuidados suficientes como para causar daños incluso irreparables a información de gran utilidad y confidencial, pero si se empieza por definir políticas,

normas, procedimientos y formatos; seguramente se pueden ir alcanzando las metas y objetivos organizacionales para constituir un centro ordenado y apegado a las normas generales que se presentan en este trabajo. Y si se siguen dichas normas sin duda la mayoría de los daños podrán ser reparados, incluso podrán ser evitados.

Como se mencionó en este trabajo acerca de la auditoria informática se establece la necesidad de la revisión de procedimientos, papeles de trabajo y función normal del trabajo diario, avalando elementos de seguridad, lineamientos de adquisición y sobre todo la estricta vigilancia del apego y seguimiento de las normas a las que se hace mención en este trabajo, para no caer en vicios, delitos, actividades anormales y sobre todo en una rutina laboral apegada a malos procedimientos.

Se hace mención también del trabajo del auditor, el cual debe cumplir con un perfil, ciertos requerimientos técnicos pero también con requerimientos informáticos ya que la mayoría de los auditores actuales, tienen el conocimiento contable pero no el computacional, lo que muchas veces provoca el desvío de fincamientos y establecimiento de observaciones que no operan para el centro de cómputo y lleva a un mal ejercicio de la auditoría.

VISITAS

BANCO DE MÉXICO – FIRA (2003), Encargado de la Visita Guiada:

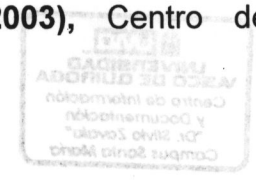
Ing, Martín Salvador Hernández González

RENAULT MORELIA (2003), Centro de Cómputo, Encargado de la Entrevista:

José Ramón Arias Cosme

TESORERIA GENERAL DEL ESTADO (2003), Centro de Cómputo

AUDITORIA SUPERIOR DE MICHOACÁN (2003), Centro de Cómputo. Encargado: Lic. Eric Alfaro Calderón



CURSOS

Curso de Auditoría Pública (2003), Expositor: C.P. Francisco Chávez Ponce

Curso de Comunicación Asertiva (2003), H. Congreso del Estado de Michoacán de Ocampo.

REFERENCIAS WEB

http://www.ignacioguerrero.com/AdmonCC/

http://www.ccu.umich.mx