UNIVERSIDAD NACIONAL AUTONOMA
DE MEXICO

FACULTAD DE CONTADURIA Y ADMINISTRACION

CONTROLES EN LA ADMINISTRACION DE CENTROS DE COMPUTO PARA EQUIPO MEDIANO Y GRANDE. (MAINFRAME Y MINICOMPUTADORAS)

SEMINARIO DE INVESTIGACION
I N F O R M A T I C A
QUE EN OPCION AL GRADO DE
LICENCIADO EN INFORMATICA
P R E S E N T A

ERIKA DINEE CAMPOS ARAGON

DIRECTOR DEL SEMINARIO
C. P. Y M. B. A. JOSE ANTONIO ECHENIQUE GARCIA
DIRECTOR DE LA FACULTAD DE
CONTADURIA Y ADMINISTRACION

MEXICO, D. F. 1993

UNAM – Dirección General de Bibliotecas Tesis Digitales Restricciones de uso

DEDICATORIAS:

A MIS PAPÁS :

Por todo el amor, cariño, apoyo y compresión que he recibido durante toda mi vida y como un tributo a su esfuerzo les dedico en primer plano mi trabajo de tesis.
Muchas gracias los quiero mucho.

A MI MAMÁ :
Por ser un ejemplo de trabajo, estudio y compresión.
Gracias por ayudarme con la redacción de mi trabajo.

A MI PAPÁ:
Por su gran labor dedicada siempre al trabajo e investigación.

A MIS HERMANOS FABIOLA Y ALVARO:
A fabi por ayudarme con la ortografía.

A MI ABUELITA CUCA:
Por ser el más claro ejemplo de trabajo, superación y entusiasmo para lograr hacer las cosas que uno se propone. Gracias por tu amor.

A TODOS MIS TÍOS Y TÍAS

A TODOS MIS PRIMOS Y PRIMAS.

EN ESPECIAL PARA GERARDO:
Con todo mi amor.
Gracias por tu apoyo, comprensión y amor que me has brindado en todo momento.
Por tu colaboración para el presente trabajo.

AGRADECIMIENTOS

A MI DIRECTOR DE TESIS:

Al C.P. y M.B.A. JOSÉ ANTONIO ECHENIQUE GARCÍA
Director de la Facultad de Contaduría y Administración.

Por sus aportaciones, confianza , apoyo e interés para la realización del presente trabajo le doy las gracias con el mayor respeto y afecto.

UN ESPECIAL AGRADECIMIENTO:

A la L.A.E. y M.A. María Teresa Pérez Morales
por el apoyo, tiempo , dirección y esfuerzo incondicional que me brindó para el inicio y culminación del presente trabajo.

Al L.A.I. y M.C. Eduardo López Castro
Por sus valiosos consejos y tiempo dedicados al presente trabajo.

TITULO DE LA PRESENTE TESIS :

CONTROLES EN LA ADMINISTRACIÓN DE CENTROS DE CÓMPUTO PARA EQUIPO MEDIANO Y GRANDE

OBJETIVO:

PLANEAR, ORGANIZAR, DIRIGIR Y CONTROLAR UN CENTRO DE CÓMPUTO PARA EQUIPO MEDIANO Y GRANDE.

PROBLEMA:

FUNCIONAMIENTO INOPORTUNO E INEFICIENTE DE UN CENTRO DE CÓMPUTO.

HIPÓTESIS GENERAL:

SI TENEMOS UNA BUENA PLANEACIÓN, ORGANIZACIÓN, DIRECCIÓN Y CONTROL DEL CENTRO DE CÓMPUTO, NO SE TENDRÁN PROBLEMAS GRAVES.

INDICE.

CAPITULO 1.
GENERALIDADES.

CAPITULO 2.
PROCESO ADMINISTRATIVO APLICADO A UN CENTRO DE CÓMPUTO

CAPITULO 3.
FACTORES CRÍTICOS EN UN CENTRO DE CÓMPUTO

CAPITULO 4.
ORGANIZACIÓN-ADMINISTRACIÓN DEL CENTRO DE CÓMPUTO.

CAPITULO NO. 1

GENERALIDADES

1.1 INTRODUCCIÓN

La introducción y utilización de los controles en los centros de cómputo en una organización es una tarea complicada. Esto ocurre en sí porque en México hasta hace apenas poco tiempo se empezaron a introducir las ideas de calidad, en las cuales va implícita lógicamente el concepto de control.

Para llevar a cabo esta tarea se requiere de una gran capacidad de análisis y un considerable conocimiento técnico.

La introducción de controles en el centro de cómputo de la organización implica, además un gran desafío para la capacidad de la administración de la organización, ya que es la que debe planear, organizar, dirigir y controlar la integración adecuada de los mismos para la consecución de sus objetivos.

Ahora si hablamos de los controles para la administración de centros de cómputo, estaremos hablando de los controles que se deben tomar en cuenta para un correcto funcionamiento del centro de cómputo, tomando como base todas las técnicas del proceso administrativo como herramientas para lograr nuestras metas.

CAPÍTULO UNO

Se dan los antecedentes, así como una visión personal acerca de los resultados de una encuesta que se levantó por la empresa GEA a petición del "Grupo de Economistas Asociados del CONACYT", sobre el grado tecnológico que se vive actualmente en el país. Se da el alcance y limitaciones del presente trabajo, así como la definición , elementos y función de un centro de cómputo.

CAPÍTULO DOS

Se explica en forma general el concepto de administración, se plantean los controles utilizados en las diferentes etapas del proceso administrativo enfocado al centro de cómputo de una organización.

CAPÍTULO TRES

Se explican los factores críticos de un centro de cómputo, como son : la seguridad, el control, los riesgos y se explican las tres infraestructuras de un centro de cómputo (física, ambiental y lógica) que hay que cuidar.

CAPÍTULO CUATRO.

Se muestran un ejemplo de los puestos deseables en un centro de cómputo, así como el ambiente de procesamiento de la información, la segregación de funciones, técnicas para separar funciones, políticas con el personal, personal de los centros de cómputo, selección de equipo y aplicaciones, documentación en los centros de cómputo y todos los problemas más frecuentes en los mismos.

1.2. ANTECENDENTES

Durante los 70's el centro de cómputo contaba con una gran computadora centralizada. Aún existian reglas de procesamiento desarrolladas y controladas de manera centralizada.

Hoy en dia, las organizaciones tienen varias opciones disponibles en el procesamiento de la información y con varias alternativas al alcance.

Los usuarios comenzaron a tener contacto directo con las computadoras via terminales hace muchos años. El procesamiento y la información ahora, están siendo distribuidos hacia workstations, terminales, minicomputadoras y equipo de automatización de oficina. El procesamiento de la información se requiere para ayudar cada vez a más gente. El centro de cómputo de hoy es diferente al de ayer, y será muy diferente del de mañana.

Lo único que se ha mantenido constante a través del tiempo es el servicio.

El centro de cómputo con controles adecuados y con un excelente servicio, será aquél que sobrevivirá a través del tiempo.

La llave para dar servicio, es el crear un ambiente en el cual la gente pueda identificar la calidad de nuestro esfuerzo y trabajo dentro de la organización en el centro de cómputo .

Ahora se ve al centro de cómputo como la vida misma de la organización, como el centro de ganancia de la misma y no como un centro de gastos.

En México a pesar de estar a finales del año 2000, carecemos de una buena administración de centros de cómputo, y en muchas ocasiones nos apoyamos en la improvisación.

En México, las pequeñas, medianas y grandes organizaciones, no parecen tener controles suficientes en sus centros de cómputo, tal como lo demuestra la encuesta que elaboró el Grupo de Economistas Asociados del Consejo Nacional de Ciencia y Tecnología (CONACYT), que tuvo como propósito señalar el grado en que las organizaciones mexicanas utilizan los nuevos modelos de producción y el lapso que transcurre antes de adoptarlos, es decir, el grado de rezago técnico. La investigación, como veremos más adelante, nos demuestra que en México las organizaciones se resisten al cambio tecnológico por razones económicas principalmente. Por esto, si no existe tecnologia, cómo van a existir controles para aprovechar esta tecnología adecuadamente, este es el punto principal de la tesis. No hay controles para la administración de centros de cómputo, ya que no existe infraestructura en las organizaciones mexicanas para llevar tecnologia a sus industrias.

Hoy se sabe que los procesos de adquisición tecnológica, tienen costos importantes para las organizaciones. Además los países en desarrollo, cuya brecha tecnológica es amplia, saben de la importancia de preparar "buenos adaptadores" de tecnología, lo que implica que la política educativa y tecnológica deben fomentar la creación de "centros de excelencia" que desarrollen la función de "copia" y "adaptación técnica".

RESULTADOS DE LA ENCUESTA

Para establecer la situación actual en materia de progreso técnico en México, esta encuesta se aplicó en 68 organizaciones dedicadas a diez diferentes ramas industriales con situaciones económicas variables y se mostró que en gran parte de estas organizaciones había: exhibición de rezagos "obvios" en materia de técnica, apertura a la competencia extranjera o una clara protección; técnicamente dependientes del exterior, con elevada capacidad exportadora o con producción de insumos esenciales dirigidos a otras cadenas productivas.

La investigación de campo se realizó en las áreas industriales de : la Ciudad de México, Monterrey, Guadalajara, Puebla, Texcoco, Toluca, León, Vito (Hidalgo), Tlaxcala y Chihuahua.

De acuerdo con los resultados de la encuesta el estudio señaló que, en términos generales, los bajos niveles de productividad física frente a la competencia exterior se atribuyen a una desventaja en materia tecnológica. A continuación se enumeran las razones por las cuáles las empresas mexicanas se encuentran en desventaja en materia tecnológica respecto a empresas extranjeras, a pesar de aprovechar su tecnología del 36.8% al 50%.
Porque las empresas mexicanas piensan que las empresas extranjeras tienen:

1. Mayor Calidad de los insumos.
2. Mayor productividad física.
3. Mayor Productividad de la mano de obra.
4. Mayor control de calidad.
5. Mayor calidad de la maquinaria.
6. Mayor rendimiento de la maquinaria.
7. Mayor calidad del producto.
8. Mejor capacitación del personal.
9. Menor costo de la producción.
10. Otros aspectos.

Todo esto se refleja en la gráfica No. 1.

Los niveles se agudizan al existir un rezago técnico, es decir, cuando el lapso de tiempo que transcurre entre la creación de un nuevo modelo de producción y su adaptación operativa en las organizaciones es demasiado distante.

A pesar de que la industria mexicana tiene un rezago técnico respecto a la competencia internacional, el estudio indicó que el aprovechamiento de su tecnología es muy alto (entre el 36.8 % y el 50 %) por esta razón, la baja productividad física no puede atribuirse a un aprovechamiento deficiente de la tecnología.

Por otra parte, el estudio determinó que ni la edad promedio de la maquinaria ni el lapso del tiempo transcurrido desde el último reequipamiento son indicadores irrefutables de un rezago "técnico".

Es evidente que los cambios sustanciales de las técnicas de producción que aumentan la productividad física, no se presentan con la misma frecuencia en las diferentes ramas; el estudio muestra cómo la variable fundamental "la periodicidad del cambio tecnológico", por ejemplo: En la industria del cemento el cambio tecnológico- la necesidad de un reequipamiento- ocurre cada 20 años, mientras que en la industria productora de máquinas de oficina y de contabilidad la periodicidad es de cada 5 años.

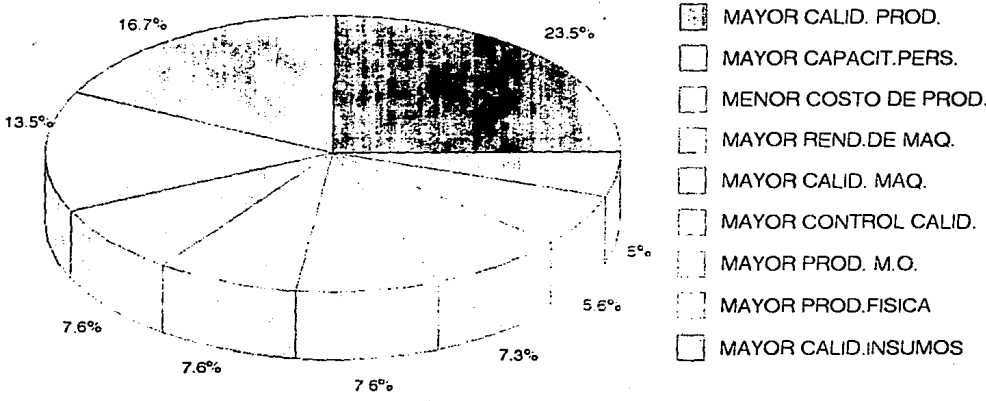
Las organizaciones encuestadas indicaron la existencia de múltiples factores que intervienen en el grado de rezago técnico para las diferentes ramas, pero coincidieron en señalar que el uso de tecnología de punta no es costeable, implica cambios no previstos, y el mercado a quien se dirige no es suficiente, todo esto se muestra en las gráfica 2, en donde en la primera se muestran las razones y en la segunda se encuentran los porcentajes de estas razones, ambas reflejan lo mismo.

Si bien estas razones son de índole económica, las encuestas revelaron factores de tipo institucional -fuentes de información tecnológica, personal técnico bien entrenado y profesionales capacitados- que impiden la modernización técnica en las industrias.

La naturaleza sistemática del progreso técnico y en buena medida, su amplitud, dependen del aparato educacional formal. Por ello, la política tecnológica debe involucrarse en la formulación de programas de formación de profesionales y técnicos que requiere el aparato productivo.

GRAFICA NO. 1

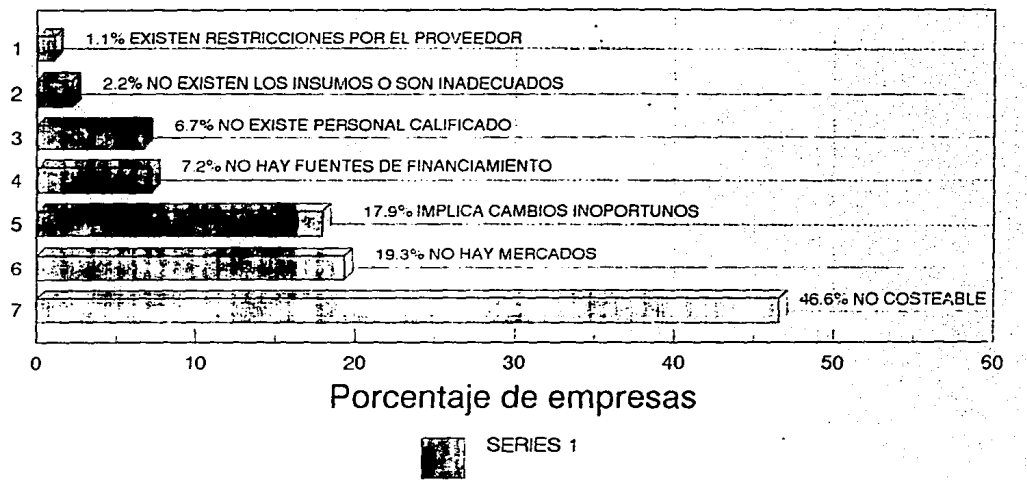
RAZONES POR LAS QUE HAY DESVENTAJAS TECNOLOGICAS



FUENTE: GRUPO DE ECONOMISTAS ASOCIADOS

GRAFICA NO. 2

RAZONES PORQUE NO SE USA TECNOLOGIA DE PUNTA



FUENTE:GRUPO DE ECONOMISTAS ASOCIADOS

NOTA:
El texto anterior es un pequeño resumen de un amplio estudio que la empresa GEA (Grupo de Economistas Asociados) elaboró para el CONACYT. La encuesta se integró al estudio denominado "Velocidad y amplitud de la difusión del progreso técnico en diversos sectores de la economía mexicana" en julio de 1993.

1.3. OBJETIVO.

El objetivo de la presente tesis es el de mostrar los diferentes controles que se deben tomar en cuenta en el momento de concebir un centro de cómputo para equipo mediano y grande. Se intenta con esto resaltar la importancia que tiene el planear, organizar, dirigir y controlar un centro de cómputo, evitando un funcionamiento inoportuno e ineficiente dentro del mismo.

1.4. ALCANCE Y LIMITACIONES.

En la presente tesis nos enfocamos principalmente a los controles en los diversos aspectos que tiene la administración de los centros de cómputo, con el objeto de que exista un procesamiento de la información más eficiente; Todo esto observándolo desde un punto de vista que se apoye en técnicas administrativas.

Se intenta dar a conocer todo lo correspondiente a la planeación, organización, dirección y control de un centro de cómputo para equipo mediano y grande.

Es importante que las personas que nos encontremos en estas áreas de procesamiento de datos, estemos preparadas para llevar a cabo un control efectivo y eficiente, con el cual se logren las metas a corto, mediano y largo plazo que se planteen dentro de la organización.

Se requiere que en este campo se den soluciones que no sólo deben estar cargadas de talento, sino apoyadas en una metodología, que tenga herramientas administrativas, que permitan resolver los problemas en el momento y que además se lleve a cabo un seguimiento de esos errores y que nos aporten EXPERIENCIA.

Los controles son importantes para mantener un área de servicio, como lo es un centro de cómputo para equipo mediano y grande, eficientemente.

Uno de los controles más significativos, es el de mantener contacto con la dirección, para conocer los planes de la organización y elaborar un plan estratégico de sistemas que, en verdad apoyen a la dirección.

'EN CIERTA FORMA, CUALQUIER CRISIS ES UNA FALLA DE LA GERENCIA, DE QUIEN ADMINISTRA'

Edward Bono[1]

Los controles no sólo los deben llevar a cabo el administrador de un centro de cómputo, sino toda la organización, ya que el ascenso en el organigrama, lleva consigo el alejamiento de las fuentes de información; la dependencia de factores ajenos se incrementa; el control se dificulta, las decisiones toman mas tiempo, los resultados tienen que esperar; en otras palabras, el manejo de los centros de cómputo ya no es tan asequible como al principio que se tenían pocos recursos y a medida que el centro de cómputo va creciendo, quien 'administra' el centro quisiera pensar en soluciones mágicas.

[1]Edward Bono 'EDP Administration' pag.15

1.5. DEFINICIÓN DE UN CENTRO DE CÓMPUTO.

"En si un centro de cómputo representa una entidad dentro de la empresa, lo cual tiene como objetivo satisfacer los requerimientos de información de la misma"

"Su función primordial, es apoyar con eficiencia la labor administrativa de la empresa, para hacerla más segura, fluida y simplificada"
"En el centro de cómputo recae la responsabilidad de la centralización, custodia de la mayoría de los datos con los que opera la empresa".

por lo tanto:

"El centro de cómputo es uno de los engranes vitales dentro de la organización, el cual hace que muchos otros se detengan o caminen sistemáticamente"

RICARDO HERNÁNDEZ JIMÉNEZ[2]

¿QUÉ ES UN CENTRO DE CÓMPUTO?

"Un centro de computo es parte responsable del procesamiento de datos, de las transacciones de los negocios día a día"[3]

"Un centro de cómputo es como una gasolinería; todas las gasolinerías venden gasolina; sin embargo, el cliente regresa a una gasolinería, porque esta provee mejor servicio, mejor precio, y alta calidad en el servicio"[4]

WILLIAM E.PERRY

Por lo tanto llegamos a lo sig.:

CENTRO DE CÓMPUTO:

ES EL ÁREA QUE ES RESPONSABLE DE LLEVAR A CABO EL PROCESAMIENTO DE LA INFORMACIÓN DE LAS OPERACIONES QUE REALIZA LA ORGANIZACIÓN, PARA QUE FUNCIONE CORRECTAMENTE, MEDIANTE LAS COMPUTADORAS.

1.6 ELEMENTOS DE UN CENTRO DE CÓMPUTO.

El administrador debe saber los elementos reales y potenciales de trabajo con que cuenta para determinar sus alcances en el desarrollo de las metas.

Los elementos de un centro de cómputo son las partes integrantes del mismo, y éstas son fundamentalmente:
- -Recursos Humanos.
- -Recursos Tecnológicos.
- -Recursos Materiales.
- -Recursos Financieros.

[2]Ricardo Hernández Jiménez "Administración de centros de cómputo" pag. 20.
[3]William E. Perry "EDP Administration and Control" pag. 180.
[4]William E. Perry "EDP Administration and Control, pag. 181.

RECURSOS HUMANOS.
Conjunto de personas que a través de su esfuerzo hacen posible el funcionamiento del centro de cómputo.

RECURSOS MATERIALES.
Bienes tangibles que la organización invierte para ser utilizados por el centro de cómputo, como el hardware y materiales auxiliares.

RECURSOS TECNOLÓGICOS.
Son los conocimientos o bienes tangibles que sirven como herramientas o instrumentos para ayudar a la conducción del centro de cómputo para el cumplimiento de sus objetivos, éstos son, por ejemplo:

-Sistema administrativo
-Software

RECURSOS FINANCIEROS.
Se consideran el dinero con que se cuenta y el dinero que se obtendrá por la vía autónoma o por la vía del préstamo o endeudamiento.

I.7. FUNCIÓN DE UN CENTRO DE CÓMPUTO.

"Su función primordial es apoyar con eficiencia la labor administrativa de la empresa, para hacerla más segura, fluida y simplificada"

"En el centro de cómputo recae la responsabilidad de la centralización custodia y proceso de la mayoría de los datos con los que opera la empresa".

"Prácticamente la mayoría de las actividades del resto de las áreas de la organización toman como base la información que les provee dicho centro"

"La toma de decisiones en los distintos niveles se ve influenciada por la calidad que posea la información y por la capacidad de respuesta del procesamiento de datos."

En gran medida, la eficiencia del centro de cómputo representa el nivel de sistematización alcanzado por la empresa.

"La importancia que adquiere el centro de cómputo dentro de la organización lo compromete fuertemente en las decisiones administrativas y de proyección de la empresa"

RICARDO HERNÁNDEZ[5]

FUNCIÓN DE UN CENTRO DE CÓMPUTO:

"Llevar a cabo un mecanismo que asegure que se están desarrollando los objetivos de una forma efectiva, eficiente y de una forma económica acorde con los planes de la administración (Gerencia) y de acuerdo con los requerimientos de los usuarios"

WILLIAM E.PERRY

[5]Ricardo Hernández Jimenéz "Administración de centros de cómputo" pag.20-21.

POR LO TANTO SU FUNCIÓN ES :

DAR RESULTADOS CON CALIDAD, OPORTUNIDAD, SEGURIDAD Y RENTABILIDAD DEL SERVICIO QUE OFRECE EL CENTRO DE CÓMPUTO DE LA GERENCIA HASTA LOS DEPARTAMENTOS USUARIOS, COMBINANDO EL PROCESO ADMINISTRATIVO CON EL PROCESAMIENTO DE LA INFORMACIÓN.

CAPITULO NO.2

PROCESO ADMINISTRATIVO APLICADO A UN CENTRO DE CÓMPUTO.

2.1. DEFINICIÓN DE ADMINISTRACIÓN GENERAL Y PROCESO ADMINISTRATIVO.

Algunas definiciones sobre administración son :

"La administración es un sistema de funciones coordinadas, que contiene las decisiones adoptadas para lograr con máxima eficiencia los objetivos de un organismo social"

JORGE BARAJAS MEDINA

"La administración es una disciplina, ciencia, arte, técnica que persigue la satisfacción de objetivos organizacionales contando para ello con una estructura que a través del esfuerzo humano coordinado logran los objetivos planeados, utilizando de la mejor manera los recursos : materiales, financieros, técnicos"

JOSÉ LUIS KRAMIS

"La administración es el conjunto sistemático de reglas para lograr la máxima eficiencia en las formas de estructurar y manejar un organismo social"

AGUSTÍN REYES PONCE

"La administración es una ciencia social que persigue la satisfacción de objetivos institucionales por medio de una estructura y a través del esfuerzo humano coordinado"

JOSÉ A. FERNÁNDEZ ARENA

"Una ciencia compuesta de principios, técnicas y prácticas cuya aplicación permite establecer sistemas racionales de esfuerzo cooperativo, a través de los cuales se pueden alcanzar propósitos comunes que individualmente no se pueden lograr en los organismos sociales"

"Conjunto de principios de valor universal en el tiempo y en el espacio".

WILBURG JIMÉNEZ CASTRO:

Definición de organismo, organismo social y organización.

ORGANISMO:

"Conjunto de elementos (órganos) cuya disposición, le dan sinergia, para alcanzar, misiones de vida específica en el ecosistema biológico."

SINERGIA es:

El efecto multiplicador de beneficios, en la unión de dos o más elementos.

Por lo tanto un ORGANISMO SOCIAL es :

"Una entidad social con capacidad jurídica para realizar fines específicos, estables y estructurados formalmente, de tal manera que permita la eficiencia del trabajo grupal en la consecución de sus objetivos."

Sinónimos de organismos son : institución, empresa y organización.
Las ORGANIZACIONES se definen, según Amitai Etzioni, como:

"Unidades sociales deliberadamente construidas o reconstruidas para alcanzar fines específicos."
Richard Hall las define como :

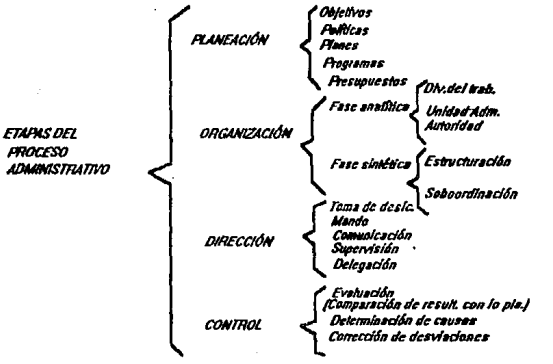
"Colectividades con límites relativamente identificables, con un orden normativo, con escala de autoridad, con sistemas de comunicación; estas colectividades existen sobre una base relativamente continua en un medio...se relaciona con una meta o un conjunto de fines."

"Quien discute alegando sólo la experiencia, no usa la razón (raciocinio) sino sólo la memoria"

Leonardo Da Vinci.

No se puede negar que la experiencia juega un papel muy importante en el éxito administrativo.

PROCESO ADMINISTRATIVO



2.2 PLANEACIÓN DEL CENTRO DE CÓMPUTO.

Implica proyectar en forma consciente la acción futura, por tanto, es un proceso intelectual que requiere tiempo, atención y dedicación suficiente para establecer los resultados que se esperan y la forma en que se pretende lograrlos

Siempre es necesario tener en cuenta el análisis de hechos e información relevante del presente y del pasado, para elegir entre diversas alternativas el curso de acción que represente un alto grado de éxito en la consecución de los fines de una organización.

La planeación es la primera etapa del proceso administrativo por medio de la cual se define un problema, se analizan las experiencias y se establecen planes y programas.

Planear: Es decir por anticipado lo que se va hacer. Para lograr una buena planeación adecuada, debe buscarse una innovación a través de la revisión de la situación actual, encontrando mejores soluciones que puedan provocar cambios en las demás funciones para asegurar el cumplimiento de los objetivos establecidos.

LA PLANEACIÓN EN SÍ.

Es una actividad mental que consiste en relacionar hechos y efectuar suposiciones acerca del futuro, a fin de elaborar un esquema detallado denominado PLAN que indique el curso de acción para lograr los objetivos.

- PLANEACIÓN ESTRATÉGICA (a largo plazo, Gerencia).
  Cubre periodos de cinco años o más.
  Son guías genéricas que habrán de seguirse en la realización de labores

  PLANEACIÓN TÁCTICA (a mediano plazo)(deptos. subordinados de áreas funcionales).
  Cubre periodos a más de un año y menos de cinco años. Se toman los lineamientos de planes estratégicos para desarrollar planes específicos de áreas funcionales.

  PLANEACIÓN OPERATIVA (a corto plazo) (departamentos subordinados de áreas funciónales)
  Cubre periodos menores de un año. Se utilizan para asignación de tareas y trabajos particulares que deben realizar los empleados de unidades operacionales.

PLANEACIÓN A LARGO PLAZO DEL CENTRO DE CÓMPUTO.

Los planes a largo plazo del centro de cómputo, deben ser coherentes con los planes a largo plazo de la alta gerencia y deben considerar las metas organizacionales, los cambios en la organización, los avances tecnológicos y los requisitos gubernamentales.

Se deben revisar los planes a largo plazo del centro de cómputo para verificar su coherencia con los de la alta gerencia, así como su compatibilidad con los cambios organizacionales, los avances tecnológicos y los requisitos legales.

PUNTOS A REVISAR:

1. Revisar la coherencia de los planes del centro de cómputo, con las metas organizacionales y las proyecciones de crecimiento relacionadas.

2. Examinar los documentos fuente utilizados en el desarrollo de los planes y pronósticos a largo plazo y comprobar que las bases de las proyecciones sean razonables.

3. Entrevistar a los principales gerentes del área de sistemas, para conocer su nivel de conocimientos, tanto de las metas del centro de cómputo como las organizacionales.

4. Determinar si los planes del centro de cómputo, han sido distribuidos a otras unidades organizacionales y evaluar el grado de aceptación de éstos.

5. Revisar los organigramas y las descripciones de puestos para determinar si son coherentes, con los planes del centro de cómputo.

6. Actualizarse en los avances tecnológicos y comprobar que éstos, reflejen y/o se consideren adecuadamente en los planes del centro de cómputo.

7. Conocer los principales requisitos legales de la organización y evaluar si los planes del centro de cómputo son coherentes con ellos.

8. En relación con la actualización en el avance tecnológico, se debe confirmar si se han identificado los requerimientos de nuevas habilidades y si se ha estudiado su posible ubicación dentro de la estructura organizacional.

PLANEACIÓN A CORTO PLAZO PARA LA ORGANIZACIÓN Y PARA EL CENTRO DE CÓMPUTO.

En el desarrollo de los planes a corto plazo de la organización, la alta gerencia debe asegurarse de que se asignen los recursos adecuados y de que los planes a corto plazo sean coherentes con los planes a largo plazo de dicho centro de cómputo.

Se deben revisar los planes a corto plazo de la alta gerencia y se debe evaluar la adecuación de los recursos en el centro de cómputo asignados para el corto plazo y largo plazo.

PUNTOS A REVISAR:

1. Revisar los planes a corto plazo de la alta gerencia e identificar los recursos asignados al centro de cómputo para el corto plazo.

2. Evaluar la adecuación de los recursos asignados al centro de cómputo para el corto plazo.

3. Garantizar la coherencia entre los planes a corto plazo y los planes a largo plazo del centro de cómputo.

REVISIÓN DE LA PLANEACIÓN PARA LA ORGANIZACIÓN Y PARA EL CENTRO DE CÓMPUTO.

La alta gerencia debe recibir informes gerenciales, para revisar el avance en el logro de las metas.

Se deben examinar los informes gerenciales para verificar la revisión de la alta gerencia (o del comité de planeación y vigilancia del centro de cómputo) y su coordinación de las actividades del centro de cómputo.

PUNTOS A REVISAR:

1. Determinar la fecha y la naturaleza de la última revisión gerencial de los planes a corto y largo plazo.

2. Investigar en los informes gerenciales, el avance hacia el logro de las metas.

3. Supervisar la frecuencia y la exactitud de los informes de proyectos relacionados con la planeación a largo y a corto plazo.

4. Comparar los gastos reales contra los gastos presupuestados para identificar diferencias importantes.

5. Entrevistar a los usuarios y a la gerencia para determinar si hay áreas específicas en las que no se han alcanzado las metas.

6. Revisar los informes gerenciales y las respuestas específicas relativas a las áreas en que no se han logrado las metas.

7. Evaluar, en ausencia de procedimientos formales de revisión y elaboración de informes , si la alta gerencia ejerce una adecuada comunicación y revisión informales sobre las actividades del centro de cómputo.

PLANEACIÓN DE LA ADMINISTRACIÓN

La función del centro de cómputo, es la de un negocio dentro de otro negocio (de acuerdo con William E.Perry). Desde una empresa mediana a una gran empresa, el presupuesto anual para el funcionemiento del centro de cómputo excede a los costos totales de las pequeñas organizaciones.

Aún en organizaciones pequeñas , el presupuesto para el procesamiento de datos puede ser una parte significativa en los costos totales de operación de la organización. El administrador del centro de cómputo tiene la responsabilidad de llevar a cabo el "negocio" del procesamiento de la información dentro del centro de cómputo.

Una parte importante de la administración de una organización. es la planeación. La función administrativa normalmente tiene la responsabilidad de preparar los planes para el centro de cómputo. El objetivo de este proceso, es explicar como manejar el centro de cómputo como si fuera un negocio, así se podrá proveer de una ganancia en la inversión de la organización.

La planeación del centro de cómputo no puede ser desarrollada independientemente de la planeación de la organización. El procesamiento de datos, a pesar de que sea un negocio dentro de otro negocio, todavía es parte de la organización.

EL PAPEL DEL ADMINISTRADOR DEL CENTRO DE CÓMPUTO EN LA PLANEACIÓN.

El papel de la administración en la planeación depende del rol y la responsabilidad del administrador del centro de cómputo.

Las opciones de la responsabilidad de la planeación para el administrador del centro de cómputo son:

1. DESARROLLAR EL PLAN :	Independientemente el administrador del centro de cómputo crea un plan para el centro de cómputo.
2. CONTRIBUIR AL PLAN:	El administrador del centro de cómputo provee información administrativa para el plan del centro de cómputo .
3. ORGANIZAR EL PLAN :	El administrador del centro de cómputo se asegura de que se esté desarrollando un buen plan.

La opción correcta por la que debe optar el administrador del centro de cómputo es la opción número 3.

ADMINISTRAR EL CENTRO DE CÓMPUTO COMO UN NEGOCIO PLANEADO.

En muchas organizaciones , la administración de la organización sustenta la teoría de que el procesamiento de la información es un servicio a los diversos usuarios de las distintas áreas; sin embargo ésta no es la prerrogativa del centro de cómputo de la organización, sino la operación de la misma organización y no sólo la atención a los usuarios.

Su función no está subordinada a otras unidades de la organización.

ATRIBUTOS DE LA FUNCIÓN BIEN PLANEADA DEL CENTRO DE CÓMPUTO.

El objetivo de la planeación, es el permitir que el personal del centro de cómputo controle su propio destino.

Sin planes, el centro de cómputo puede reaccionar de acuerdo a las necesidades de otros en vez de las propias.

A través de la planeación, el centro de cómputo se encuentra en una posición de liderazgo. Por ejemplo en un ambiente que no ha sido planeado, el procesamiento de la información puede tener dificultades en determinar qué trabajo aceptar y qué trabajo no aceptar. En un ambiente que ha sido planeado esta postura no tiene ningún problema en absoluto.

Las organizaciones que dependen enteramente del centro de cómputo para su funcionamiento, deben balancear los requerimientos de los usuarios contra los requerimientos del procesamiento de la información que resulta de las operaciones de la organización.

LA PLANEACIÓN ADMINISTRATIVA Y OTROS ASUNTOS QUE NADIE TOMA EN CUENTA.

La planeación es una tarea en la cual todo mundo se encuentra en ella, sin embargo a nadie parece importarle mucho. Muchas personas desarrollan la planeación como si fuera una cosa tan común como dar vuelta a la hoja del calendario. Los pasos son desarrollados, pero pocas personas parecen entender donde nace la necesidad de planear, quién utiliza el plan y qué se está midiendo.

Existen tres aspectos que se deben tener en cuenta para la planeación, de acuerdo con William E. Perry :

PLANEADO E IGNORADO: El plan es desarrollado y aprobado, pero después de su aprobación a nadie parece importarle, y el trabajo sigue como siempre.

ADMINISTRACIÓN POR OBJETIVOS:
El plan incluye algunos objetivos especificos para las gentes involucradas y conforme el plan va siendo desarrollado, la gente va tomando sus tiempos, conforme al mismo e involucrando todas sus habilidades para lograr cumplir con los objetivos dentro del plan.

ADMINISTRACIÓN PONIENDO EN EVIDENCIA A LA PERSONAS:
El plan es usado sólo para castigar a la gente mostrándole cuanto ha fallado y qué es lo que se espera de ellos.

EL PROCESO DE LA PLANEACIÓN ADMINISTRATIVA

El desarrollo de un plan administrativo es un proyecto administrativo. Éste contempla todos los atributos de cualquier otro proyecto en el centro de cómputo. El tipo de plan desarrollado dependerá del tiempo, atención, y recursos dedicados al proceso de la planeación.

Los que planean deben reconocer que hay un ciclo de eventos que ocurren en la planeación administrativa

El ciclo comienza con:

1. LA RECOLECCIÓN DE INFORMACIÓN:
Durante este paso, aquellos individuos y grupos que utilizan y requieren servicios del centro de cómputo son contactados para preparar el flujo de trabajo futuro.

2. DE LA INFORMACIÓN RECOPILADA SE CREA UN PLAN:
Se crea un plan para la función del centro de cómputo. Note que en este paso se puede crear un plan a corto o largo plazo.

3. UNA VEZ APROBADO EL PLAN:
El plan debe ser puesto en marcha para llevar a cabo las tareas delimitadas en el plan. Sin embargo, durante un año, los eventos cambian, así que el plan debe estar sujeto a continuas modificaciones y análisis. Los planes que no son actualizados caen rápidamente en desuso , así como todo el proceso de planeación.

Una parte importante del ciclo de planeación es el análisis del trabajo ya terminado contra con lo que se planeó. Este análisis debe evaluar lo siguiente :

1. Porcentaje del plan finalizado.
2. Frecuencia y extensión de los nuevos requerimientos.
3. ¿Es correcta la información incluida dentro del plan.?
4. Valor del plan para la función del centro de cómputo
5. Debilidades en el proceso de planeación administrativa.

PASOS PARA LA PLANEACIÓN ADMINISTRATIVA.

La administración del centro de cómputo tiene la responsabilidad de desarrollar , implementar y controlar el proceso de planeación. No es responsabilidad, de la administración de la organización , determinar cuál debe ser el plan, o juzgar sobre los méritos que han sido propuestos. Sin embargo, esto no significa que el

personal de la administración. no pueda cuestionar o asistir a otras áreas en la planeación, como lo es el centro de cómputo.

El objetivo de la planeación es la utilización efectiva de los recursos del centro de cómputo. Esto incluye, primero , la identificación de la tarea que va a llevarse a cabo; en segundo, la jerarquización de aquellas tareas en concordancia con el plan general de la organización; y en tercero, los recursos deben estar en concordancia con los objetivos desde el punto de vista "costo-eficiencia".

Los objetivos de la administración y del control del plan son dos :

1. Minimizar los recursos gastados en la planeación.
2. Administrar y controlar el proceso diseñado para producir el mejor plan posible.

Para cubrir estas responsabilidades , la administración del centro de cómputo debe jugar un papel activo en el proceso total de la planeación del centro de cómputo.
La administración efectiva y el control de la planeación es un proceso continuo. No sólo debe estar involucrada la administración en la creación del plan, sino también debe estar involucrada en el monitoreo de la implementación del plan y en el registro del estatus de los resultados.

A través del análisis y la evaluación del proceso, se sabrá si se pueden hacer mejoras.

La administración y el control del proceso de planeación es realizado a través de los siguientes ocho pasos en el cuadro No. 1.

CUADRO 1.

FASE	NÚMERO	PASOS
Requerimientos	1	Prevención de la planeación
Requerimientos	2	Definición de restricciones
Requerimientos	3	Estimación de tareas
Diseño	4	Jerarquización de las tareas
Diseño	5	Calendarización del trabajo que va a realizarse
Implementación	6	Prueba del plan
Pruebas	7	Aprobación y modificación
Operación y mantenimiento	8	

Nota : Esta tabla esta basada en la tabla de "Administrative Planning Steps"[6]

PROPÓSITOS DE LOS PASOS ANTERIORES:

1. PLANEACIÓN PREVENTIVA: Alertar al staff de los requerimientos de planeación y construir el entusiasmo por el proceso (nota: Ésta puede ser iniciada por la organización o gerencia general).

[6]Edward E. Perry "EDP Administration and control" pag. 84

2. RECOLECCIÓN DE LA INFORMACIÓN: Recolectar con entradas para los planes:

1. Planes corporativos.
2. Planes del Procesamiento de datos a largo plazo.
3. Planes de procesamiento de datos de requerimientos continuos.
4. Requerimientos de los nuevos usuarios.
5. Requerimientos de los nuevos procesos de datos.

3. DEFINICIÓN DE RESTRICCIONES: Determinación de la magnitud y los límites de los planes.

4. ESTIMACIÓN DE LAS TAREAS: Identificar los recursos requeridos para llevar a cabo cada una de las tareas.

5. PRIORIZACIÓN DE LAS TAREAS(JERARQUIZACIÓN): Determinar la secuencia de cada tarea.

6. CALENDARIZACIÓN DEL TRABAJO QUE VA A REALIZARSE: Crear un plan para llevar a cabo aquellas tareas que pueden ser realizadas con los recursos propuestos.

7. PRUEBA DEL PLAN: Evaluar el plan para :

1. Que sea razonable.
2. Sea acorde con los planes de la organización.
3. Que no haya duplicidad.

8. APROBACIÓN Y MODIFICACIÓN : Ajustar el plan basado en las limitaciones de la administración.

2.3 ORGANIZACIÓN DEL CENTRO DE CÓMPUTO.

La definición de organización que más se ajusta a nuestras necesidades en este tema es la siguiente:

DEFINICIÓN.

" Es la estructuración técnica de las relaciones que deben existir: funciones, niveles de autoridad, actividades y responsabilidades de los miembros de la organización. Parte de los principios de división del trabajo, especialización, de la autoridad, responsabilidad y de la unidad de mando. Al organizarse un grupo u organización, debe definirse qué secciones, departamentos, gerencias, divisiones, etc., deben reportar a la máxima autoridad. Por eso esta parte del proceso, otros autores la denominan departamentalización. Sisk dice que realmente lo que hace una empresa es reorganizarse constantemente, una organización total sólo se da cuando la organización inicia sus operaciones y posiblemente surja de una idea amorfa, que empieza con una organización poco definida."[7]

DEFINICIÓN.

Podemos decir que con base en los objetivos fijados en la planeación, la organización se encarga de dividir el trabajo, agrupar actividades, establecer jerarquías, designar las tareas de autoridad y responsabilidad de los integrantes, coordinar a los grupos en sentido vertical y horizontal, por medio de las relaciones de autoridad y comunicación.

[7]Secretaría del Trabajo y previsión Social "Hacia la calidad total y el mejoramiento continuo" pag.15

PRINCIPIOS PARA LA ORGANIZACIÓN DE CENTROS DE CÓMPUTO.

Ciertas verdades inalienables en la práctica de la administración deben ser tomadas en cuenta.

La localización organizacional de la administración del centro de cómputo debe ser situada según la filosofía gerencial acerca de cuál es su función. Las habilidades y los antecedentes del centro de cómputo puede variar significativamente. Sin embargo, una violación de los principios básicos de la administración afectará adversamente el éxito de la función.

La contaduría está basada en procedimientos contables generalmente aceptados. La ingeniería trabaja con la fuerza de los materiales, y la fuerza que pueden soportar estos materiales de acuerdo con el tipo de construcción. Las ciencias están basadas en las leyes de la naturaleza. Los principios de la administración del centro de cómputo han sido codificadas por Edward Perry para ayudar a los administradores a determinar si las políticas y los procedimientos van a funcionar. Por ejemplo un ingeniero, a través de principios ingenieriles, pueden determinar qué es necesario para sostener un puente o un edificio alto. Similarmente los principios de Perry son ese cuerpo de conocimientos comparados con las prácticas administrativas y los procedimientos, para que puedan ser medidos y determinar si sirven o no sirven.

Los 10 principios de la administración del centro de cómputo son los factores de éxito para la administración.

PRINCIPIO No. 1 ESTABLECER OBJETIVOS.

Si la administración no tiene objetivos, la misión de la función del centro de cómputo no será clara a aquéllos encargados de desarrollarla. Los objetivos de la administración son: el desarrollo de procedimientos de reporte que razonablemente reflejan el estatus actual de los proyectos, son necesarios para utilizar la función efectivamente y para medir el desarrollo de la función.

PRINCIPIO NO.2 ASIGNAR RESPONSABILIDADES.

La gente sólo lo hace bien si creen que es suyo. La administración efectiva utiliza políticas y procedimientos que han sido realizados por el personal del centro de cómputo.

Si las políticas y los procedimientos son de ellos, a ellos les va a gustar, las van a seguir y se van a esforzar. Si las políticas administrativas y los procedimientos son dictados, es probable que no funcione.

PRINCIPIO NO.3 DEFINIR LA TERMINACIÓN DE LAS TAREAS.

Las entregas para cada tarea desarrollada por el administrador del centro de cómputo, deben ser definidas. Las tareas que se entregan rápidamente son pérdidas de tiempo y puede que no den resultados satisfactorios.

La gente debe ser capaz de saber que tienen la responsabilidad de terminar una tarea. Sin embargo, si existe alguna necesidad por algún trabajo urgente, ésta deberá ser la excepción y no la regla.

PRINCIPIO NO.4 DESARROLLAR LOS PLANES.

Una vez que los objetivos y las especificaciones han sido determinadas, debe desarrollarse un plan para llevar a cabo los objetivos de la administración.

La planeación es necesaria para asegurar que los objetivos sean terminados con un mínimo de recursos. Los planes son esenciales para un desarrollo efectivo de la función.

PRINCIPIO NO.5 LIMITAR ALTERNATIVAS.

Esta regla, es aplicable para evaluar cursos alternativos de la acción de la administración. En cualquier proceso de decisión administrativa, las alternativas deben ser rápidamente limitadas, y sólo esas opciones deben ser investigadas.

PRINCIPIO NO. 6 ASIGNACIÓN DE RESPONSABILIDADES.

Una persona debe ser responsable y confiable para cada una de las tareas administrativas. A cada persona en específico le pertenece y es responsable por al menos una función.

PRINCIPIO NO.7 RESPECTO AL LIDERAZGO.

La administración de la organización (gerencia) debe respetar el liderazgo de la administración del centro de cómputo en su forma de llevar a cabo la organización de éste, debido a que la misma gerencia delegó al administrador del centro de cómputo la autoridad y responsabilidad.

Retar la autoridad de ciertas personas, no producirá el tipo de resultados administrativos necesarios para mejorar la productividad de la función del centro de cómputo .

Las presiones indirectas son más efectivas en la ejecución de procedimientos administrativos que la confrontación directa entre administradores y los gerentes.

PRINCIPIO NO 8 OBTENCIÓN DE HERRAMIENTAS.

Desafortunadamente, son demasiados los administradores de centros de cómputo que desarrollan su función con lápiz y papel.

En la administración, como en cualquier otra función, se deben utilizar herramientas para la calendarización de procesos , actividades, tareas etc.., es bueno buscar paquetes que se amolden a nuestras necesidades y que nos sirvan como apoyo para la administración del centro de cómputo, para facilitar su labor.

PRINCIPIO NO.9 CRITICAR EL PRODUCTO, NO A LA PERSONA.

En el curso de la función de la administración, suelen surgir problemas dentro del centro de cómputo, ésta, será responsabilidad de la administración del centro de cómputo

Si el problema es sobre el producto o el proceso, la situación tiene solución rápidamente, por otro lado, si la crítica, es directamente hecha al individuo, se presenta una postura defensiva por parte del individuo que es atacado y creerá que es necesario defender su posición. Esto ocasionará un importante retraso en la solución del problema .

PRINCIPIO NO. 10 DESCARTAR LO OBSOLETO.

Los avances tecnológicos en hardware deben adoptarse y se debe tratar en lo posible de desechar lo obsoleto.

2.4 DIRECCIÓN DEL CENTRO DE CÓMPUTO.

La función de dirección implica conducir esfuerzos de las personas para ejecutar los planes y lograr los objetivos de la organización.

La dirección es la parte central de la administración, puesto que por su conducto se logran los resultados que finalmente servirán para evaluar al administrador; poco efecto tendrán técnicas complicadas de planeación, organización y control, si la labor de la dirección es deficiente.

DIRECCIÓN ADMINISTRATIVA.

El administrador del centro de cómputo tiene dos grandes retos cuando visualiza la operación del mismo como un centro de ganancia.

Éstas son:

1. Obtener la tecnología cambiante que provee el costo más bajo posible.
2. Determinar el nivel de servicio que va a proporcionar a los clientes.

El papel del administrador del centro de cómputo tiene una responsabilidad muy grande, ésta es la de estar a la vanguardia siempre que sea posible, ya que tan pronto como el administrador pueda seleccionar y adoptar tecnología, un vendedor anuncia algo nuevo. La nueva tecnología aparece más barata y mas rápida.

Sin embargo, parece no importar lo que haga el administrador del centro de cómputo para estar con la tecnología de punta, ya que siempre emerge tecnología nueva.

El administrador debe también decidir el nivel de servicio que se les ofrecerá a los usuarios.

Si un programa o aplicación no funciona en el centro de cómputo o los reportes no son entregados à tiempo o la capacidad de la computadora no está disponible, el centro de cómputo debe aceptar parte o toda la responsabilidad. El concepto de centro de ganancia se aplica para saber como prevenir y evitar esos problemas, para que no vuelvan a ocurrir. Sería fabuloso decir que la administración del centro de cómputo no tiene la culpa de esta situación, pero el usuario nunca lo creerá.

El negocio de administrar un centro de cómputo es ilustrado en la fig. 1.

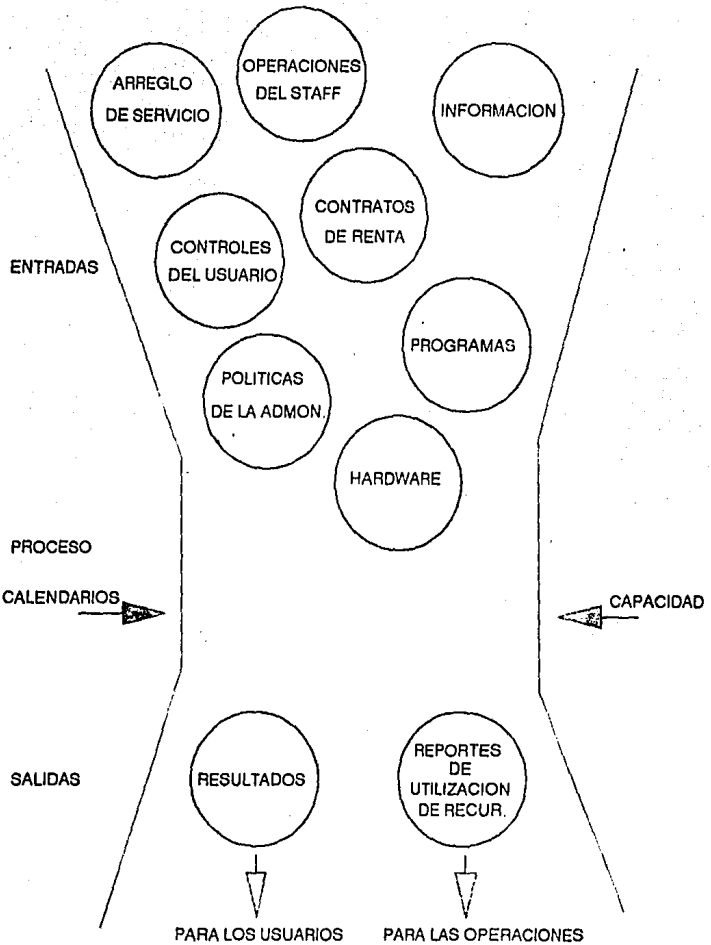
Ésta muestra el amplio rango de entradas que debemos manejar.

El administrador del centro de cómputo debe dirigir los acuerdos de servicios, acuerdos de renta, hardware y software operando.

El centro de cómputo tiene contratos tanto formales como informales con los usuarios para desarrollar trabajo en concordancia con las políticas de la administración del centro de cómputo.

El trabajo que se entrega por parte de los usuarios al centro de cómputo se mide y se registra con programas, así la cantidad de programas entregados de acuerdo a un calendario establecido, determinará en cierta forma la eficiencia de éste.

Los resultados del procesamiento son monitoreados. Éstos van al administrador del centro de cómputo para evaluar el trabajo del centro de cómputo .



EL NEGOCIO DE LAS OPERACIONES DE LA COMPUTADORA

FIG. 1

Desde el punto de vista de los negocios, cualquier grupo de negocios pueden ser descritos en términos de las entradas que éllos reciben, el proceso que ellos desarrollan y los productos que éllos dan a sus clientes.

Sin embargo, es el análisis o el recurso de la utilización de los reportes que diferencian el centro de ganancia del centro de costos. El centro de costos puede enviar los resultados del procesamiento y el costo al usuario.

El centro de ganancia está midiendo su costo-efectividad y reduciendo costos cuando éstos no muestran un apropiado regreso de la inversión.

EL TRIÁNGULO DEL ÉXITO DE LAS OPERACIONES DEL CENTRO DE CÓMPUTO.

Hemos definido obstáculos que hay que vencer en la operación del centro de cómputo como las siguientes:

1. El centro de cómputo ofrece una comodidad para vender, por ejemplo recursos de la computadora (incluyendo a la gente).

2. Usuarios de este servicio requieren de equipo alternativo para una mejor realización de sus funciones, por ejemplo centros de servicio, redes de teléfono, microcomputadoras, etc.

3. Los bajos costos de ahora son mayores a los costos de mañana cuando el siguiente vendedor ofrece una nueva tecnología.

El éxito del triángulo de las operaciones del centro de cómputo se ilustran en la fig. 2. El triángulo establece que los administradores deben balancear los siguientes tres criterios operacionales para que se pueda llegar al éxito.

1. CALIDAD EN EL TRABAJO.
Entregando a los usuarios los resultados correctos.

2. ADECUAR NIVEL DE SERVICIO.
Ofreciendo a los clientes a tiempo otro tipo de servicios alternativos.

3. PROCESAMIENTO COSTO-EFECTIVIDAD.
Cargando a los clientes un precio que puedan pagar.

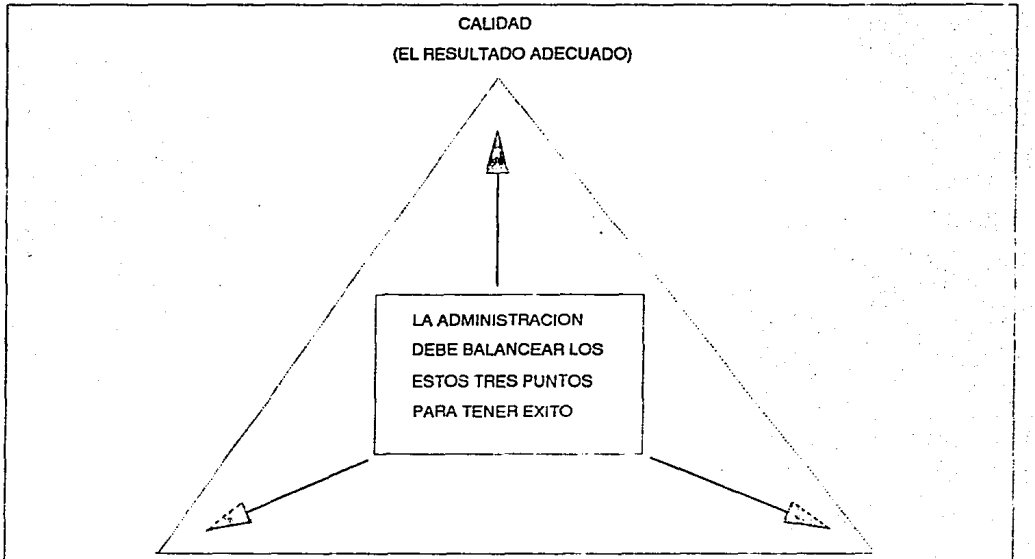
La mezcla de estos tres puntos para cada cliente puede ser diferente.

El centro de cómputo exitoso no es una operación de un precio. Como las estaciones de gasolina, debemos ofrecer gasolina regular nova y gasolina magna sin, es decir debemos ofrecer diferentes tipos de servicio para los diferentes tipos de clientes.

Un usuario de un centro de cómputo requiere un reporte mensual resumido para propósitos de análisis y no está particularmente molesto si esta 1 ó 2 días tarde. Por otro lado, otro usuario necesita una respuesta instantánea para cerrar una venta con un cliente. Una respuesta tardía puede significar una venta perdida para ese usuario.

CONSTRUYENDO BUENAS RELACIONES CON LOS USUARIOS.

Los usuarios son los clientes del centro de cómputo . Éstos se encuentran en todas las áreas mayores o las grandes áreas dentro de la organización como en: la gerencia, administración senior, administración



EL TRIANGULO DEL EXITO DE LAS OPERACIONES DEL CENTRO DE COMPUTO

FIG. 2

operacional, la sección de desarrollo de sistemas etc. Bajo el concepto de negocios, es importante que la administración de este centro de cómputo encuentre la forma de dar el mejor servicio para que los usuarios o clientes continúen regresando para darles servicio.

Cualquier persona inteligente pasaría su tiempo conociendo a sus clientes.

En muchas organizaciones el centro de cómputo es un monopolio y aunque a los clientes o usuarios no les guste ir a resolver sus problemas no tienen ninguna alternativa.

La única pregunta lógica es preguntar si el centro de cómputo puede pagar un servicio amable y amistoso hacia los usuarios que son los clientes del centro de cómputo y si se puede ¿ se debería dar esta clase de servicio?. La respuesta a esta pregunta es "SI". El administrador del centro de cómputo debe tomar su tiempo para aprender lo siguiente acerca de los clientes o usuarios:

1. CONOCIMIENTO SOBRE EL FLUJO DE TRABAJO FUTURO:
Es esencial para el centro de cómputo que el personal conozca el trabajo futuro.
Entre más conozca el flujo de trabajo, el tipo, mezcla y la cantidad, mejor preparado estará junto con los requerimientos que lo satisfagan.

2. QUEJAS Y SUGERENCIAS:
Si el cliente o el usuario de un centro de cómputo no está contento, o tiene sugerencias para un mejoramiento, es mucho mejor que ponga al tanto al administrador del centro de cómputo y no al administrador de la organización.
Por esto se debe elaborar un mecanismo de quejas y sugerencias para que sean pasadas al administrador del centro de cómputo .

3. TURNAR EL FLUJO DEL TRABAJO :
A veces puede ser necesario por el administrador del centro de cómputo acelerar o retrasar trabajos. Si el administrador tiene una relación cercana de trabajo con los usuarios o clientes, este problema puede ser discutido libremente y en muchos casos los usuarios de los servicios del centro de cómputo estarán de acuerdo en turnar los trabajos.

4. EL NEGOCIO O FUNCIÓN DE LOS USUARIOS O CLIENTES:
Si el administrador sabe el negocio o la función del usuario, el administrador puede ser capaz de proveer mejores servicios. Es difícil hacer sugerencias sobre un área para la cual no es conocida. Para que el cliente tenga una relación más cercana con el centro de cómputo el administrador debe conocer y entender las necesidades y el negocio del cliente.

En sistemas, parece razonable operar bajo la política de cualquier negocio "Si no queda satisfecho, le regresamos su dinero".

Existen muchas formas en las cuales el administrador de un centro puede construir buenas relaciones con el cliente, incluyendo:

-LLEVAR AL USUARIO A COMER:
Periódicamente, es recomendable para el administrador del centro de cómputo , conocer mejor a sus clientes sobre un ambiente amigable. En el almuerzo o la comida es una manera amistosa de hacerlo y no será una cosa irrazonable para el administrador del centro de cómputo, pagar el almuerzo del presupuesto del centro de cómputo .

-MUESTRE INTERÉS EN EL NEGOCIO O ASUNTOS DEL USUARIO:
Cuando se anuncia sobre algún evento en el área del usuario, una llamada telefónica para felicitarlo es una forma de mostrar atención.

-HACER VISITAS FORMALES ANUALMENTE.
La gente del centro de cómputo, debe discutir anualmente con todos los usuarios posibles, para establecer el estatus del servicio del centro de cómputo, para un mejoramiento potencial. Esto también es una buena oportunidad para discutir futuros flujos de trabajos.

-INTERCAMBIO DE PERSONAL:
Es una buena práctica dejar a los empleados de un área trabajar en: otras áreas por períodos cortos de tiempo, o transferir el personal entre áreas para mejorar el entendimiento entre un área y otra.

Los puntos discutidos anteriormente, reflejan algunas ideas para mejorar las relaciones entre el centro de cómputo y la base de los clientes o usuarios

PRÁCTICAS DE MEJORAMIENTO DE SERVICIO.

El servicio no puede ser definido como una entrega sobre tiempo. Se deberá dar a los usuarios los resultados apropiados en el tiempo que ellos requieren. El problema del centro de cómputo es el de realizar un nivel de servicio con calidad, este no es problema del usuario.

IDENTIFICACIÓN DEL FLUJO DE TRABAJO QUE VA A REALIZARSE.

El centro de cómputo debe tratar de estimar el trabajo que debe realizarse por mes, por semana, por día y por hora.

El trabajo esperado puede ser obtenido de las siguientes dos fuentes:

1. Historia actual del trabajo que se hace.
2. De los cambios esperados en el trabajo que va a realizarse.

Una de los mejores formas de prever el trabajo futuro y prepararnos para ello, es llevar un registro detallado sobre el trabajo que va a realizarse sobre periodos extendidos de tiempo.

Es importante para identificar la fuente y el tipo de trabajo que se va a realizar, lo siguiente:

1. Qué usuario o cliente submitió el trabajo.
2. Generación de nuevos procesos.
3. Reinicios por fallas de los procesos.
4. Mantenimiento de los sistemas.
5. Área de negocios (o aplicación)

MONITOREANDO EL TRABAJO QUE SE REALIZA.

El centro de cómputo no puede garantizar que el trabajo se entregará o terminará de acuerdo al calendario ya que algunos trabajos pueden llegar tarde y otros temprano. A esto se suma que pueden surgir trabajos no esperados, problemas con la computadora, fallas con el sistema etc. Todo puede afectar significativamente el trabajo, pues pueden ocurrir en cualquier momento y de forma inesperada.

El centro de cómputo debe monitorear continuamente, el trabajo para asegurarse que está siendo procesado a tiempo y adecuadamente, para que si surge alguna situación inesperada se actúe rápidamente y no se retrasen los trabajos.

Es sólo por medio del monitoreo continuo, que el centro de cómputo puede ofrecer el nivel de servicio requerido.

CUARTO DE TRABAJO PARA LA GENTE DE PRODUCCIÓN.

Aqui se discuten los problemas del centro de cómputo y se define la estrategia a tomar en ciertas circunstancias.

En este lugar se obtiene el reporte de estatus sobre los resultados del procesamiento del dia anterior, el flujo de trabajo para ese dia, cualquier obstáculo para el trabajo de hoy, el estatus de los proyectos actuales en el centro de cómputo.

Cada administrador en la reunión debe proveer con reportes de estatus y pizarrones o el equivalente para poder listar los problemas para la acción.

Si ocurren problemas durante el día, el equipo es otra vez llamado a junta en el cuarto de trabajo para tomar la acción.

ESCRITORIO DE AYUDA.

El centro de cómputo sirve a una amplia variedad de usuarios. Los usuarios experimentan periodos de ansiedad cuando su trabajo está retrasado o aparece incorrecto. Muchos usuarios llevan buenas relaciones con los programadores, pero puede no que no tengan la misma buena relación con el administrador del centro de cómputo. Por esta razón nace el escritorio de ayuda.

El escritorio de ayuda es un concepto que pone a una persona para cualquier aclaración sobre algún problema.

Los tipos de problema que pueden ser dirigidos para el escritorio de ayuda son:

1. Petición para el estatus de un job.
2. Pregunta de porqué parte del trabajo está retrasado.
3. Pregunta de porqué parte del trabajo está perdido.
4. Necesidad de volver a correr un job.
5. Necesidad para clarificar un procedimiento operativo en el centro de cómputo.
6. Descontento con un procedimiento del centro de cómputo.

MANTENER LOS SUMINISTROS CERCA DE PRODUCCIÓN.

Las operaciones de la computadora pueden ser retrasadas porque no hay disponibilidad de los suministros. Los suministros en el centro de cómputo incluyen los archivos de producción, archivos scratch, papel de impresora y otros suministros requeridos para propósitos de la producción. Si estos abastecimientos están almacenados lejos del área de producción, se ocasionarán retrasos en la producción.

PRÁCTICAS DE MEJORAMIENTO DE LA CALIDAD.

Si el administrador del centro de cómputo cree que 15 minutos de retraso es un tiempo razonable y el usuario no lo cree asi, se tiene un problema de calidad.

ESTÁNDARES DE CALIDAD.

Los estándares son la medida por la cual la calidad es obtenida. Los estándares predefinen qué es esperado y luego lo que ocurre debe ser medido para saber si los estándares ayudaron a mejorar lo esperado.

Entre los estándares de calidad que necesitan ser establecidos dentro del centro de cómputo, están:

1. Niveles aceptables de desarrollo de aplicaciones.
2. Criterio de que los programas de aplicación deben ser correctos antes de que entren al ambiente de producción y sean ejecutados.
3. Se requiere documentación de las operaciones.
4. Nivel aceptable de operador-error.
5. Números esperados de jobs para ser finalizados a tiempo.
6. Porcentaje esperado de la capacidad de procesamiento que será utilizado.
7. Nivel aceptable de quejas del usuario o cliente.

Es normalmente más económico tener un proceso de control de calidad, en donde se revise todo con más detenimiento, que tener que resolver los problemas cuando surjan.

INSPECTORES DE LOS PRODUCTOS.

Los productos entregados a los usuarios del centro de cómputo deben ser inspeccionados, para saber si los productos de los procesos que entrega el centro de cómputo están completos y satisfacen las necesidades de los usuarios.

Los inspectores deberán revisar lo siguiente:

1. Que las salidas estén impresas en el tipo de papel correcto.
2. Que las salidas estén impresas en el formato correcto.
3. Que los nuevos cambios hayan sido incorporados.
4. Que los reportes estén completos.
5. Que los mensajes sean dirigidos a la terminal/locación correcta.
6. Que el dispositivo de salida no falle por un mal funcionamiento de la impresora.
7. Que los documentos negociables sean todos contabilizados.
8. Que los procedimientos de seguridad sean apropiadamente utilizados.

RECIBIENDO EN EL PUERTO CENTRAL.

En la mayoría de las organizaciones, todos los productos recibidos de fuentes exteriores se reciben a través de un puerto de recibimiento central. Esto sirve para dos propósitos:

1. Asegurar que todos los productos ordenados fueron recibidos.
2. Dar una oportunidad para rechazar un producto que no se quiere o un producto de pobre calidad.

Cuando la función de recepción es formalizada, las sorpresas son minimizadas. El puerto registra formalmente todo lo que se recibe, el estado en el que llegue y luego entrega al centro de cómputo la nota de recibido.

Los centros de cómputo reciben dos tipos de productos.

1. Físico, como el hardware, dispositivos de la computadora, muebles, papel etc.
2. Lógico, como los sistemas de software operativo, archivos en cintas, documentación etc.

Los procedimientos generales de recepción en el puerto son:

1. Obtener notificación de cosas que se esperan recibir.
2. Aceptar todos los recibos de parte del centro de cómputo .
3. Rechazar todos los productos que no han sido ordenados.
4. Notar cualquier deficiencia en la condición de los productos recibidos, incluyendo el software.

EQUIPO DE EMERGENCIA.

Un equipo de emergencias, es un grupo especializado, organizado para el propósito de lidiar con los problemas.

En el centro de cómputo se debe armar un equipo de emergencia, si algún problema fuerte llega a ocurrir; el equipo de emergencia es despachado inmediatamente para resolver el problema.

El equipo de emergencia está normalmente integrado por personal altamente calificado. Este personal debe tener conocimiento, sobre las aplicaciones así como del software operativo. Muchas organizaciones ponen al equipo de emergencia en horarios de, 12 horas tres días a la semana.

Esto ha probado ser útil, si este equipo es formado por gente voluntaria.

RELACIONES PÚBLICAS.

Las relaciones públicas son esfuerzos formales para mejorar la imagen de las operaciones de la computadora. Es creado para asegurar que las funciones que están siendo desarrolladas por el centro de cómputo, son vistas positivamente por los usuarios.

Se plantean a los usuarios, de acuerdo a las actividades que se desarrollan en el centro de cómputo, las siguientes preguntas:

1	¿Se tiene una imagen positiva del centro de cómputo por parte de los clientes o usuarios?.
2.	¿Los empleados del centro de cómputo actúan de una manera que trae credibilidad al centro de cómputo ?.
3	¿Hay cosas que el centro de cómputo puede hacer para mejorar su imagen dentro de la organización?
4.	¿Los productos producidos por el grupo del centro de cómputo tienen calidad y cubren una imagen profesional?

Es probable que hoy en día, algunas actividades del centro de cómputo resulten de imagen negativa. A menos que a alguien en el centro de cómputo se preocupe por mejorar la imagen, ésta siempre será negativa.

GRUPO USUARIO.

Muchos usuarios tienen muy poco entendimiento de los procedimientos y problemas con los que se tienen que lidiar en el centro de cómputo. Por otro lado, en muchos centros de cómputo no entienden las necesidades específicas y los requerimientos de los usuarios.

Formar un comité de usuarios provee un vehículo para este tipo de discusiones. Generalmente, el comité es informal, no tienen autoridad o poder, pero se convierte en vocero de los usuarios.

Así como las ideas pueden ser inaceptables para los usuarios individuales, pueden ser implementadas a través del diálogo. Una vez que los grupos de usuarios entienden el valor y el impacto de un error suyo en producción, lo aceptan o rechazan. Sin embargo, si el concepto es impuesto no lo aceptarán aunque entiendan el valor.

COMUNICADO INFORMATIVO DEL CENTRO DE CÓMPUTO PARA LOS USUARIOS.

Es importante crear y mantener un medio de comunicación entre el centro de cómputo y los usuarios, con el propósito de que los usuarios noten que hay un interés por parte del centro de cómputo en notificarles e informales sobre las cosas que están pasando en el centro de cómputo . Algunos puntos que pueden ser incluidos en un comunicado informativo son los siguientes:

1. Nuevo equipo en orden.
2. Nuevo equipo que está siendo instalado.
3. Capacidad y velocidad del equipo.
4. Calendarización de la información.
5. Información objetiva sobre la cantidad y el tipo de material.
6. Información explicando las habilidades del centro de cómputo para conocer sus estándares de calidad. (por ejemplo, el hardware está operando a un 80% del tiempo etc..)

2.5 CONTROL DEL CENTRO DE CÓMPUTO.

DEFINICIÓN DE CONTROL

"Consiste en el establecimiento de sistemas que permitan medir resultados actuales y pasados en relación con los esperados, con el fin de saber si se ha obtenido: lo que se esperaba, corregir, mejorar y formular planes".[8]

OTRAS DEFINICIONES DE CONTROL SON:

" El término control es de origen galo, viene del sufijo cont-contra y de rol-lista-, contra la lista, contra lo programado en una lista, Rol significa también cilindro, rodillo, que camina rodando. Payroll significa en inglés nomina o lista de pago".[9]

"La palabra control, desde el punto de vista científico, según la Enciclopedia Británica (cir. "Hombre, ciencia y Tecnología"), se define como : "Proceso realizado mediante estructuras naturales o artificiales, por el cual cantidades variables son inducidas a ajustarse a una regla preestablecida". Léase por regla, estándar."[10]

[8]Agustín Reyes Ponce.
[9]Secretaría del Trabajo y Previsión Social "Hacia la Calidad Total y el Mejoramiento Continuo" pag 77.
[10]Secretaría del Trabajo y Previsión Social "Hacia la Calidad Total y el Mejoramiento Continuo" pag 78.

Para el enfoque clásico, el control es una comparación de lo planeado con lo acontecido y se presenta como la última fase del proceso administrativo. Ello ha creado confusión, pues visto así pierde sentido. Es mejor verlo como una parte del sistema, una parte del sistema, una parte del todo como unidad, ya que es una pieza clave al servicio de la dirección de la organización.

El control es la última etapa del proceso administrativo, pero está estrechamente relacionado con la planeación, a la cual sirve de retroalimentación para futuros planes. Su función consiste en establecer sistemas para medir y corregir las ejecuciones de los integrantes de la organización, con el fin de asegurar que los objetivos fijados se vayan logrando. Por tanto, mientras más claros, completos y ordenados sean los planes, más se facilitará la función del control. Los factores sobre los cuales se pueden controlar todas las actividades son: cantidad, calidad, tiempo y costo. El control se utiliza para:

1. Conocer lo que realmente se está logrando.
2. Evaluar el desempeño de los integrantes.
3. Detectar fallas o errores.
4. Corregir las desviaciones.
5. Modificar los planes.
6. Mejorar la coordinación.
7. Establecer un mejor sistema de comunicación.
8. Predecir problemas y/o soluciones, etc.

MECANISMOS DE CONTROL.

1. La observación personal.
2. Los presupuestos.
3. Las estadísticas.
4. Las auditorías.
5. Informes verbales y/o escritos etc.

PROCESOS DE CONTROL.

1.- Establecimiento de normas o estándares de ejecución.
2.- Medición de lo que se ha hecho.
3.- Comparación de lo hecho con lo establecido e investigación de las diferencias, si las hay.
4.- Corrección de las desviaciones aplicando acciones correctivas.

El establecimiento de estándares consiste en fijar las unidades de medida que sirven como punto de referencia y que están basadas en los objetivos. Los estándares fijados estarán relacionados, con:

1. Niveles de producción.
2. Cuotas de ventas.
3. Índices de productividad.
4. Posición en el mercado.
5. Cargas de trabajo.

MÉTODOS DE PLANEACIÓN Y CONTROL:

1. Gráficas de Gantt.
2. Redes de actividades: PERT (Técnica de revisión y evaluación de programas).
3. Ruta crítica.

Lo que puede variar en una organización son los planes; llámense programas, normas, procedimientos, presupuesto, metas en el procesamiento de la información, consecuentemente se requieren controles que permitan a la unidad de dirección mantener la operación de acuerdo con los límites de lo planeado.

Si la planeación fuera ejecutada sin defectos, por una organización perfectamente estructurada y bajo la dirección omnipotente, jefes y subordinados infalibles y un medio ambiente estático, no habría la necesidad de controlar su ejecución. Todo plan requiere de seguimiento y evaluación, lo que técnicamente se llama también monitoreo.

Para cumplir tal propósito se deben identificar previamente las áreas de ejecución críticas, variable a controlar. Por ejemplo en una empresa manufacturera, el volumen de producción por período, ventas, ingresos y egresos son áreas críticas que requieren control.

Una vez determinada el área crítica a controlar, se pasa a definir el objeto del control, esto es, clarificar la misión del control y en qué contribuye evaluando su costo-beneficio.

Esto definirá los rangos de expectación que permita una selección adecuada de unidades de medición.

Los estándares se deben apoyar, en indicadores que señalen si se cumplen o no con los objetivos y en qué puntos hay desviaciones. Estos estándares, se determinan de acuerdo a la cantidad de programas de mediana complejidad que desarrolla un programador, en un período de tiempo determinado; o bien, en el caso de los analistas de sistemas, se puede observar si han cumplido adecuadamente con los objetivos establecidos en su plan de trabajo, en el tiempo planeado.

Definidos los estándares meta, el organismo requiere de un instrumento de medición y con su consecuente sistema de información que alimente oportunamente a la unidad de decisión o dirección y al sistema de registro histórico.

Con todos estos elementos se procede a la ejecución y medición.

El control y sus partes, deben ser objeto de evaluación para saber si cumple su función, ya que se debe informar inmediatamente de la ocurrencia de desviaciones, a la administración del centro de cómputo para que se lleve a cabo una acción correctiva oportuna.

El control para mantener las variables dentro de lo deseado requiere de:

1. Detección del área crítica a controlar.
2. Objetivo del control a establecer.
3. Unidades de medición/parámetros/estándares
4. Instrumentos o medios de medición y sistemas de información y registro.
5. Normas de acción correctiva.
6. Ejecución y medición.
7. Toma de la acción correctiva correspondiente.
8. Evaluación.

El control es un elemento de todo sistema cuyo propósito es mantener las variables en los términos deseados.

Cuantificar la calidad de un producto, requiere de medidas que permitan saber si se cumple o no con los requisitos preestablecidos y así saber si se tiene calidad.

Por calidad entendemos el cumplimiento de todos los requisitos.

RASGOS QUE INDICAN UN BUEN CONTROL

Los controles, para su utilización óptima, deben poseer ciertas características:

MEDIDAS APROPIADAS

Frecuentemente se confunde lo que se desea medir y por tanto, se usan medidas inadecuadas, por ejemplo, evaluar el aprendizaje mediante la asistencia o la simpatía. En las organizaciones, también se evalúa el desempeño a través de factores como la presentación o el número de alabanzas al jefe, o el desarrollo del personal por el número de cursos de capacitación aunque no se haya aprendido nada, perdiéndose la objetividad y haciendo de la evaluación un aspecto más cualitativo y subjetivo que cuantitativo y objetivo.

OPORTUNIDAD

.La información proporcionada por el control, deja de tener valor y utilidad si no llega al nivel donde se toman las decisiones a tiempo. Por ejemplo, la contabilidad y los estados financieros son herramientas fundamentales en la toma de decisiones diarias; sin embargo, los contadores en las pequeñas y medianas organizaciones proporcionan generalmente, tal información hasta el fin de un periodo fiscal, haciendo de este valioso instrumento de control, un documento sin valor.

QUÉ ES LA CALIDAD

" El diccionario Espasa-Calpe nos dice que calidad significa:" conjunto de cualidades que constituyen la manera de ser de una persona o cosa..".[11]

"También significa, de acuerdo con el diccionario citado:"..nobleza y lustre de sangre" o "cálido" en el sentido de delicado, de bello, que cautiva, que costo trabajo hacerlo "[12].

En lenguaje popular, la calidad se ha asociado con: lujo, precio alto, marca exclusiva, estatus que proporciona el poseer o usar un producto, atributos "cálidos" del producto (por ejemplo, un perfume delicado o un vino costoso), artículo importado (aún si es "chatarra").
Administrativamente, calidad significa: cumplimiento de estándares para satisfacer al cliente o al usuario.

Estándar :significa normal, uniforme a lo que debe ser; es un punto de comparación.

Técnicamente, calidad es el cumplimiento de ciertas normas establecidas que debe cubrir el producto para cumplir su objetivo.

CALIDAD ES ESTAR DENTRO DEL CONTROL.

Existen actualmente varias escuelas de calidad total:

[11]Secretaría del Trabajo y Previsión Social. "Hacia la Calidad Total y el Mejoramiento Continuo" pag.43
[12]Secretaría del Trabajo y Previsión Social "Hacia la Calidad Total y el Mejoramiento Continuo" pag.43

*Escuela Norteamericana:

EDWARD DEMMING Y SUS 14 PRINCIPIOS.

1. Congruencia con la misión.
2. Adoptar la filosofía de la calidad como cultura organizacional.
3. Redefinir el propósito de la inspección.
4. Fin de la práctica de adjudicar las compras y adquisiciones sólo sobre la base del precio.
5. Mejorar constantemente y para siempre el sistema de producción y de servicio.
6. Instituir el entrenamiento (para el desarrollo de habilidades).
7. Enseñar e instituir el liderazgo.(de jefe de hombres a jefe de equipos).
8. Expulsar el temor. Crear confianza. Crear un clima para la innovación.
9. Optimizar los esfuerzos de los equipos, grupos y áreas de staff también, hacia las metas y propósitos de la organización.
10. Eliminar las exhortaciones a la fuerza de trabajo una vez implantada la cultura de la calidad.
11. Eliminar las cuotas numéricas de producción. En su lugar, aprender e instituir métodos para la mejora.
12. Remover las barreras que roban a la gente el orgullo de su trabajo.(Cada contribución es importante por pequeña que ésta sea).
13. Fomentar la educación y el automejoramiento de cada uno.
14. Actuar para lograr el cambio.(Sin burocratizar el sistema).

JURAN Y SUS PRINCIPIOS.

1. Crear conciencia de la necesidad y oportunidad de mejoramiento.
2. Determinar metas de mejoramiento.
3. Organizarse para lograr estas metas (comités, equipos, reuniones).
4. Proporcionar entrenamiento.
5. Desarrollar proyectos para resolver problemas.
6. Reportar los problemas.
7. Dar reconocimiento.
8. Comunicar los resultados.
9. Mantener los registros.
10. Mantener la mejora dentro de los sistemas y procesos de la compañía.

*Escuela Japonesa.

KOBAYASHI.ADMINISTRACIÓN CREATIVA.

Gracias a Shigeru Kobayashi, la Sony Corporation fué una de las primeras organizaciones japonesas que se dieron cuenta de la necesidad del concepto de equipos de trabajo, para romper con las estructuras y principios de autoridad taylorianos, sistemas típicos en aquel tiempo en el Japón y que habían sido copiados del modelo estadounidense.

ISHIKAWA CREADOR DEL CONCEPTO DE CALIDAD TOTAL

1. El Diagrama Causa-Efecto(Espina de Pescado).
2. El principio y Diagramas de Pareto(Economista y sociólogo italiano, autor del principio que lleva su nombre " el 80% de las causas origina el 20% de los efectos, mientras que el 20% de las causas origina el 80% de los efectos").
3. El uso de listas de verificación.
4. El gráfico de proceso.
5. El análisis de correlación.
6. El gráfico de control.
7. Histogramas.

CONTROL DE LA ADMINISTRACIÓN.

Control de la administración, es la totalidad de métodos, procedimientos, y herramientas utilizadas para asegurar que los procedimientos administrativos se desarrollen en concordancia con la administración. Un buen control hace una buena administración del centro de cómputo .

LOS PASOS PARA CONSTRUIR LA CALIDAD ADMINISTRATIVA

La calidad no puede ser mejorada hasta que sea medida. El gerente administrativo debe tener información confiable sobre la calidad de la administración para poder mejorarla.

El administrador tiene tres opciones básicas disponibles para medir y mejorar la calidad del centro de cómputo, estas son:

1. La autoevaluación y el mejoramiento.
2. Tareas que forzan el asesoramiento y la recomendación.
3. Círculos de la calidad administrativa.

CAPITULO NO.3

FACTORES CRÍTICOS DE UN CENTRO DE CÓMPUTO.

3.1 SEGURIDAD.

ADMINISTRACIÓN EFECTIVA DE LA SEGURIDAD DE LA COMPUTADORA

Los piratas de la computadora han causado desastres, accesando a los sistemas de las organizaciones.

Los ejecutivos de las organizaciones han expresado su preocupación, en relación a la facilidad de acceso vía telefónica a las redes de los sistemas de la organización; Todo esto realizado por grupos de gentes que se dedican a accesar a estas redes, ya sea por hobbie o por un sinnúmero de razones, utilizando computadoras personales y modems de bajo costo.

En estos días se requiere que los administradores de las corporaciones se aseguren que sus sistemas de cómputo tengan una seguridad adecuada para proteger a sus sistemas de información de accesos no autorizados, modificaciones y/o destrucciones.

EL PAPEL DEL ADMINISTRADOR DE LA SEGURIDAD

El adecuado control del riesgo, requiere de la planeación y la integración en la función de la administración dentro de la jerarquía de la organización. Esto requiere de un staff y de financiamiento para administrar como una función de control, para unir la organización y la administración, así como monitorear la efectividad de varias implementaciones de seguridad. La responsabilidad de la administración de la seguridad es la siguiente:

1. Seguridad en el centro de cómputo, en la comunicación de la red y de las terminales.
2. Comunicación con los usuarios.
3. Producción y empeño en los estándares de seguridad y de los procedimientos.
4. Protección de la información.
5. Análisis de riesgo y monitoreo.
6. Implementación y administración del equipo de control de acceso y del software, así como el control y encriptación.
7. Planeación de Contingencias y atención al contrato de la aseguradora para el equipo.

El administrador de la seguridad debe dar a conocer a las diferentes áreas funcionales, cuándo se llevará a cabo la planeación y la implementación de la seguridad, y ser responsable de monitorear e integrar las mismas.

Debe ser capaz de comunicarse a todos los niveles, para entender los requerimientos de la seguridad de la organización y recomendar e implementar las salvaguardas necesarias en áreas estratégicas.

PLANEACIÓN DE LA SEGURIDAD (ADMINISTRADOR DE LA SEGURIDAD).

El administrador de la seguridad debe estar informado de todos los planes de la organización, así como de las estrategias futuras en el área de computación y comunicaciones, incluyendo propuestas para el nuevo centro de cómputo, encriptación de líneas de comunicación, y la adquisición de computadoras personales en diferentes áreas de la organización.

El administrador de la seguridad debe estar enterado de cualquier iniciación de nuevos proyectos y de la introducción de nuevos sistemas; ya que él mismo puede aplicar sus conocimientos y experiencia para darse cuenta que a éstos, están asociados nuevos riesgos y que son necesarios ciertos controles que pudieron haber escapado de las personas que realizan la planeación de la organización.

La proposición de una nueva legislación dentro de la organización, puede requerir controles más exigentes sobre el fuego, la estructura de nuevos edificios, la confidencialidad en los negocios delicados e importantes y en otros problemas ambientales. El administrador de la seguridad debe revisar y accesar a la vulnerabilidad de la organización, en razón de proponer cambios o una nueva legislación.
Debe recomendar un curso de acción para la instalación de prevención de riesgos y detección de salvaguardas.

El administrador de la seguridad también debe evaluar el costo-beneficio de alternativas en áreas de acceso al control, administración de passwords y encriptamiento de datos, protección contra el fuego, provisiones de respaldos y los procedimientos de respaldo. El presupuesto necesario para la seguridad debe estar justificado de acuerdo al costo-beneficio en razón de las debilidades de la organización.

IMPLEMENTACIÓN DE LA SEGURIDAD (ADMINISTRADOR DE LA SEGURIDAD).

El administrador de la seguridad debe saber hablar con los gerentes acerca de la aplicación de los controles, para que éstos sensibilicen a sus empleados y se lleven a cabo estos controles en su curso normal de trabajo y se adhieran a los estándares de seguridad.

Se deben realizar en conjunto :

1. El análisis de los riesgos.
2. Los planes de contingencias.

Se deben tomar en cuenta para lo anterior:

1. Alternativas de respaldo.
2. Utilización de servicios externos.
3. Búsqueda de espacio para el equipo
4. Planes de acción para manejar situaciones de emergencia, deben ser reproducidos y probados exhaustivamente.

Un programa de implementación de la seguridad debe ser puesto en marcha y debe estar acordado por todas las partes concernientes:

1. Fechas-objetivo
2. Compromisos de recursos

Deben ser perfectamente bien especificados y firmados por varias fases, por ejemplo:

1. Para la instalación del software de acceso de control
2. Para realizar todos los respaldos necesarios
3. Para conocer todos planes de contingencia disponibles para el centro de cómputo.

El administrador de la seguridad debe asegurarse que exista y funcione correctamente un mecanismo para el registro de accidentes, fallas del sistema y reclamaciones, así como de accesos no autorizados al sistema. Las pérdidas importantes de información también deben ser registradas, así como los factores que contribuyan a ayudar a advertir de un incidente serio.

MONITOREO DE LA SEGURIDAD

La administración de la seguridad es responsable de monitorear día a día los eventos acorde con los estándares y las políticas de seguridad.

El administrador de la seguridad debe estar seguro que el mecanismo de registro de contingencias efectivamente sea utilizado de acuerdo a los objetivos para lo que fué creado, y que se encuentre disponible, para que el staff que se encargue de registrar :

1. Accidentes y fallas del sistema
2. Reclamaciones y quejas acerca del sistema.
3. Accesos no autorizados al sistema

Las pérdidas importantes también deben ser registradas, explicando dónde y cómo sucedieron, así como los factores que contribuyen a prevenir un incidente serio.

El mecanismo de evaluación del registro del accidente o falla , debe asegurar que la información registrada es significativa, exacta y completa.

Las entradas deben proveer detalles suficientes para un análisis subsecuente.

Se deben realizar :

1 Revisiones periódicas de incidentes registrados
2. Reportes de excepción

Los cuales deben ir idealmente acompañados por comentarios constructivos sobre:

1. La experiencia del usuario
2. Actitud y respuesta al procedimiento de control
3. Software o dispositivos
4. Detalles de cualquier problema
5. Beneficios positivos emergiendo desde la aplicación de aquellos controles

Entonces se pueden realizar recomendaciones para mejorar la eficiencia de un control futuro.

INTEGRACIÓN DE LA SEGURIDAD
El administrador de la seguridad no es un administrador en el sentido estricto de la palabra.

FUNCIÓN ADMINISTRACIÓN EN GENERAL:
La función del administrador de línea es el de controlar

FUNCIÓN DE LA ADMINISTRACIÓN DE LA SEGURIDAD
Es la de comunicar, monitorear y reportar.

Con sus pequeñas excepciones, la mecánica actual del esfuerzo de la seguridad de la organización, esta probablemente planeada e implementada fuera de la jurisdicción del administrador de la seguridad.

El administrador de la seguridad debe asegurarse que la administración de la organización esté al tanto de sus acciones. Si es necesario, los administradores de la organización deben ser persuadidos para que estén de acuerdo con los controles y procedimientos que se estén llevando a cabo.

Estos controles y procedimientos que lleve a cabo el administrador de la seguridad, deben cumplir con los preceptos de la organización, para que haya un control más efectivo, y así puedan ser mejor aprovechados en sus áreas.

En algunas ocasiones puede ser que al administrador de la seguridad se le requiera ocasionalmente para:

1. Instalar salvaguardas y procedimientos de control. Esto aplica en particular en la preparación de guías de seguridad para las computadoras personales en las diferentes áreas de la organización, o para cumplir con los requerimientos de la protección de datos. En estos casos el administrador de la seguridad debe integrarse con los usuarios directamente.
2. Debe revisar que los controles recomendados y las salvaguardas sean apropiadas y efectivas. Se debe dar a conocer a los usuarios las recomendaciones de seguridad teniendo en cuenta que tendrán que seguir con sus recomendaciones día a día.
3. El administrador de la seguridad tendrá que tener persuasión y habilidades de venta para que los controles que se hayan integrado no sean ignorados por los jefes de las áreas. La administración debe darse cuenta de las razones reales detrás de la implementación de esos controles, y de los efectos indeseables. Si no se le ha prestado suficiente importancia a los controles, se debe proceder a reportar a la alta gerencia para presentar el caso.

ESTÁNDARES DE SEGURIDAD, PROCEDIMIENTOS Y REVISIÓN

Se deben preparar por parte de la administración de la seguridad en conjunto con la administración de la organización:

1. Seminarios de prevención y seguridad

Todo esto, para sensibilizar a la organización y al personal acerca de las posibles consecuencias de pérdidas potenciales y de la necesidad de seguir los estándares y los procedimientos.

El éxito de la implementación de los estándares recae enteramente sobre la buena voluntad y el entendimiento de los jefes de las áreas. Éstos deben estar convencidos que esos estándares son introducidos por el bien del personal y de sus áreas.

La revisión de la seguridad debe ser llevada a cabo periódicamente para determinar posibles problemas en asuntos de seguridad y como una anticipación a las inspecciones de rutina.

REPORTES A LA ADMINISTRACIÓN

Para poder desarrollar su papel efectivamente, el administrador de la seguridad debe tener contacto directo con la alta gerencia de la organización.

Esto significa reportar directamente a un ejecutivo de la gerencia. Este ejecutivo es el designado para ser responsable por :

1. Todos los asuntos de seguridad de la organización en las áreas clave
2. Es el que establece las políticas de seguridad para la organización
3. Delega su autoridad al administrador de la seguridad, quien se encarga día a día de la implementación y el monitoreo de las políticas de seguridad, para que sean cumplidas.
4. Cualquier problema que exista entre el administrador de la seguridad y el administrador de la organización, debe ser resuelto por el ejecutivo quien es responsable por la seguridad y el bienestar de la organización.

ADMINISTRACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN

La buena seguridad de la información no es solamente el resultado de un efectivo cumplimiento de los procedimientos día a día dentro del centro de cómputo. La importancia de la seguridad debe ser entendida a través de la organización y debe ser reflejada en planes estratégicos y procedimientos de rutina.

El pasado o la historia de la organización debe ser revisada para identificar cualquier fuente potencial en incremento del riesgo en la seguridad.
La actitud de un cliente hacia el procesamiento de datos y la presencia de una estrategia de la computadora, integrada con el plan de la organización, tendrá un efecto significativo sobre la seguridad de la información.

La estructura de la organización nos ayuda a evaluar las prácticas de seguridad y procedimientos, y el papel de las personas responsables para hacerlos funcionar bien. Debe haber alguien responsable de la seguridad. La definición del trabajo de esa persona, debe ser revisada para asegurarse que es entendible y completa, además los resultados de su trabajo deben ser examinados para la efectividad.

Las políticas del personal son importantes para asegurar que todo el staff está prevenido de sus responsabilidades y que esas precauciones son tomadas, para proteger la organización de dependencia excesiva sobre importantes individuos. Las políticas y los procedimientos seguidos, cuando una persona es reclutada o se va de la organización, debe siempre incluir una prevención de los riesgos de la seguridad de estas acciones. Las preferencias deben ser siempre tomadas para nuevos reclutas. La gente que se va de la organización debe ser movida a un papel no muy importante o se le debe pedir que se vaya inmediatamente después de renunciar.

El staff de auditoría interna debe incluir gente suficientemente entrenada y con experiencia para revisar la instalación o un sistema a detalle. El alcance de su trabajo debe ser lo suficientemente amplio para incluir todas las áreas de riesgo potencial, y ellas deben ser de suficiente influencia para que sus recomendaciones sean aceptadas e implementadas. En la actividad final, nosotros debemos examinar el alcance y los acuerdos de mantenimiento deben ser regularmente revisados y vueltos a revisar para asegurar que todo el equipo de cómputo y el equipo está cubierto por la aseguradora. La administración debe asegurarse que el trabajo de mantenimiento es actualmente desarrollado conforme con estos acuerdos por gente calificada.

PROGRAMA DE INFORMACIÓN DE LA SEGURIDAD

Las grandes organizaciones, han siempre sido muy conscientes de la necesidad de una seguridad efectiva de nuestros activos financieros y nuestra información sobre los empleados y los clientes.

Habiendo identificado la necesidad de una guía y en un esfuerzo por estandarizar, se debe crear un "Manual de Información de Políticas y Estándares".

CLASIFICACIÓN

Nuestra clasificación de políticas establece, que la información debe ser protegida a un grado apropiado de acuerdo a su vulnerabilidad e importancia para la organización. Así se presentan cuatro clasificaciones de seguridad, una de las cuales aparece sobre todos los registros internos y correspondencia.

PÚBLICO

Esta información está dedicada a la distribución fuera de la organización, ya sea a un grupo seleccionado de individuos, o al público en general.

USO INTERNO

Esta información está dirigida al personal dentro de la organización, sin embargo su uso, no está permitido a gente externa a la misma.
Si una persona no autorizada hace uso, reproducción o destrucción del mismo, no tendrá un impacto significativo, sobre nosotros, nuestros clientes o nuestros empleados

CONFIDENCIAL

Esta información es para uso interno en la organización, y su utilización no autorizada o su destrucción puede traernos un impacto adverso

ALTAMENTE RESTRINGIDO

Esta información es para el uso dentro de la organización. Su utilización sin permiso o su destrucción puede causar un daño significativo que puede traernos problemas a nosotros, a nuestros clientes o a nuestros empleados

ESTANDARES DE AMBIENTE EN EL CENTRO DE COMPUTO

Las acciones dictadas por estos estandares son para minimizar la información que ha sido accidentalmente o intencionalmente accesada, modificada, perdida o retrasada dentro del ambiente del centro de cómputo

Esto incluye acceso al departamento de sistemas, donde se utilizan procesadores de palabras y computadoras personales

MEDIDAS DE SEGURIDAD QUE SE TIENEN QUE CONSIDERAR CON EL PERSONAL DEL CENTRO DE CÓMPUTO.

Algunos de los procedimientos más elementales para mantener secretos industriales, incluye la relación de la organizacion con sus empleados. Los empleados deben estar advertidos que cierta información es confidencial Sumado a esto, deben haber procedimientos para mantener la información en secreto. Estos procedimientos pueden ser el de seccionar los departamentos donde los secretos pueden darse a conocer y luego hacer que el área se salga de los limites.

Dibujos, diseños, diagramas, fórmulas, especificaciones o reportes de computadora puede traer una leyenda restrictiva. Esta debe establecer que la información es secreta y no puede ser reproducida, del todo o en parte, o en cualquier otra forma, sin una autorización escrita.

Las leyendas restrictivas "Prohibido reproducción" no evitarán un robo, pero hará trabajo de reproducirlas más difícil y recordará al empleado descuidado que sea más precavido. También si ninguna precaución es tomada, es muy difícil tener un fundamento legal para salvaguardar sus tratados secretos.

Si la mayoria de la información confidencial de las organizaciones es dada a conocer por la prensa, en las relaciones públicas o en papeles presentados en convenciones industriales, el derecho a un trato secreto estará perdido Esto es similar a la situación de publicar algo sin su copyright.

Otros procedimientos aparte de clasificar secretos y controlar las impresiones de la organización, incluye la revisión de los empleados prospectos.

Frecuentemente se pasa por alto el pasado más elemental de los prospectos a empleados, aún cuando el candidato está siendo considerado para una posición importante. En ocasiones no se investiga a los prospectos, por el costo que esto implica o por la inexperiencia del personal de recursos humanos.

Los aspirantes con antecedentes penales no son necesariamente un riesgo de malos empleados, pero es importante tenerlo en cuenta de acuerdo al nivel de responsabilidad del puesto solicitado.

Al personal de nuevo ingreso, deberá firmar un documento-compromiso en el c al se le informa que tendrá acceso a información confidencial y que no está autorizado a divulgarla.

La organización debe ser cuidadosa, para no estar envuelta en un pleito legal. Si la organización contrata a personal de la competencia, se arriesga a que dicho personal desarrolle un producto o un software similar al que estaba desarrollando en su trabajo anterior puede provocar un pleito legal.

Un problema más realista es un empleado que se va y toma un nuevo trabajo. EL empleado que se va puede firmar un documento diciendo que no tiene ninguna propiedad de la organización, tales como archivos, programas, diagramas, reportes de investigación o cualquier otro tipo de propiedad de la organización. Esto no ofrece protección legal, pero recuerda al empleado que tiene una obligación con la organización. Ya que es raro que un empleado permanezca más de 1 ó 2 años en el mismo trabajo, debido a que el mercado profesional del área de sistemas es muy amplia.

Los empleados que no se sienten satisfechos, son un blanco perfecto para hacer tratos secretos fuera de la organización. Los espías industriales saben que si pueden encontrar a alguien que le pagan poco en puesto importante o con una deuda muy grande, entre otras...está es una obvia posibilidad para el soborno y el chantaje. Esto usualmente empieza cuando alguien inocentemente le pregunta por alguna información y si se la consigue le pagará bien. Una vez que el empleado lo ha hecho puede ser chantajeado la segunda vez si es necesario.

LISTA DE PUNTOS PARA SALVAGUARDAR INFORMACIÓN CONFIDENCIAL

1. Busque un individuo responsable para supervisar y dirigir medidas de seguridad.

2. Informe a sus empleados que cierta información es confidencial y que se espera mantengan su confidencialidad.

3. Conduzca una campaña educacional y enfatice el peligro al trabajo, a las ganancias y a la seguridad, por perder secretos.

4. Proporcione sólo la suficiente información confidencial, a cada empleado, para que funcione eficientemente.

5. Establezca procedimientos para que cualquier información que se genere en la organización, no se divulgue fuera de la misma.

6. Clasifique y etiquete todos los documentos confidenciales.

7. Esté prevenido de las posibilidades de los dispositivos modernos como: micrófonos escondidos y espías industriales profesionales.

8. Establezca procedimientos propios para destruir el papel usado, así no caerá en manos ajenas.

11. Establezca un inventario del equipo de la organización.

PREVENCIÓN DE FRAUDES POR PARTE DEL PERSONAL.

La estratégia para prevenir que un fraude ocurra, es adoptar medidas para hacer mas difícil el abuso, para poder reducir la frecuencia de ocurrencia o minimizar este tipo de acciones con los siguientes puntos:

1. Segregación de actividades.

El control más efectivo es el reducir la habilidad de un individuo para ejercer el control en más de una área funcional. Por ejemplo, para cambiar un cheque, éste deberá ser firmado independientemente por diferentes individuos, en diferentes áreas, para poder ser autorizado su cobro, esto ayudará a descubrir un fraude.

2. Control de las Entradas y salidas.

La mayoría de los fraudes por computadora involucran la explotación de "lagunas" que se tienen en los controles de entradas y salidas.

La función de los controles de acceso debe ser apropiada, para prevenir que extraños o intrusos quieran entrar en ciertas terminales, cuando nadie las está usando por alguna razón (el personal salió a comer, olvidaron apagarla, se fueron a una junta etc.).

Se debe de dar atención a la administración y control del uso de passwords. Los usuarios de las terminales deben estar conscientes de la importancia de custodiar sus passwords o la identidad de sus códigos, así como de no dejar su terminal prendida y en sesión.

3. Control de cambios.

Se deben tener procedimientos de autorización apropiados cuando el analista y los programadores hagan cambios al sistema vivo y a la información. Se deben probar exhaustivamente los cambios que se intentan hacer en producción para que éstos sean aprobados, antes que la versión viva o actual sea reemplazada.

4. Estructura "Walk-Through".

Es un sistema diseñado para conocer los detalles del sistema por más de un individuo. Es para que los auditores puedan conocer el diseño del sistema y hacer pruebas, para detectar deficiencias en los procedimientos de control e identificar debilidades en las áreas clave en el sistema.

5. Buena Documentación.

La documentación del programa y del sistema deben estar dentro de los estándares de la organización para que una persona independiente pueda mantener el sistema. Si en la organización solamente el diseñador del sistema conoce y mantienen al sistema, la organización confía grandemente en la integridad y lealtad de esa persona.

6. Rotación del trabajo.

Debe haber una rotación de deberes apropiada en la organización para asegurar que una persona no se encajone en una función en particular. El aburrimiento y la frustración pueden causar que un individuo pueda tratar de probar la debilidad del sistema, como un reto técnico y luego explotar su conocimiento en ganancias particulares.

7. Haga acuerdos/realización difícil

Muy a menudo es difícil diferenciar entre el abuso deliberado y un error genuino. Donde sea posible, la organización debe poner en claro las instrucciones al staff acerca de lo que esta prohibido.

Por ejemplo, los documentos marcados como secretos no deben ser sacados de las instalaciones, o bien, los programadores no deben entrar al cuarto del equipo de telecomunicaciones.

8. Buenos procedimientos del personal.

Los empleados deben estar regularmente evaluados y valorados, para motivarlos en el trabajo y en el desarrollo de su carrera con una remuneración y premios de méritos adecuados para alentar la productividad.

Los empleados despedidos por una mala conducta o incompetencia deben ser escoltados fuera de las instalaciones cuando se les de la noticia. Se les debe negar el acceso a las instalaciones de la computadora o a las terminales remotas. Los passwords y los códigos de seguridad deben ser cambiados inmediatamente antes de que el despido tenga efecto.

9. Seguro contra el abuso cometido contra la computadora.

Conviene que la administración contrate un seguro de cobertura amplia contra el abuso, daño o pérdida de información, así como daño al equipo por acciones de personas ajenas a la organización, como garantía para aminorar cualquier pérdida futura o fraude.

3.2 CLASIFICACIÓN DE LOS CONTROLES

Control : "Es todo aquello que tiende a causar la reducción de los riesgos. Introduciendo controles, los riesgos y su frecuencia de ocurrencia se minimiza nunca se elimina".[13]

La utilización de las computadoras no cambia ninguno de los conceptos básicos de los controles.

Aún cuando no ha habido ningún cambio fundamental en la naturaleza de los controles, existen cambios radicales en el aspecto externo de los controles que se implantan en los sistemas informáticos , éstos se reflejan en los siguientes puntos:

1. Reducción del uso de los controles manuales.
2. Las fuentes de información han cambiado y son con frecuencia independientes de los usuarios de la información.
3. Las pistas de las transacciones son susceptibles de perderse, debido a que ya no existe una correspondencia directa entre los datos de entrada y los de salida.
4. Puede haber un cambio en los controles a los empleados y supervisores de la computadora y los analistas de sistemas.
5. Los controles deben ser mas explícitos, debido a que se han reducido o eliminado muchos
de los aspectos de procesamiento de información que antes se permitían al juicio humano.
6. La calidad de la documentación es más crítica debido a que muchos de los registros que anteriormente podían haber existido en forma impresa se encuentran ahora dentro de los

[13]William C. Mair.

La estructura y la aplicación de los controles deben ser claras para todas las partes interesadas. Existen dos niveles de controles dentro del área de sistemas:

-Lógicos
-Técnicos.

La distinción entre ambos niveles radica principalmente en su grado de complejidad.

Los controles pueden clasificarse en diversas formas. Cada una de las clasificaciones nos dice algo distinto respecto a la forma en que los controles cambian en diversas situaciones en el centro de cómputo.

CONTROLES LÓGICOS Y CONTROLES TÉCNICOS

CONTROLES LÓGICOS :

Naturaleza: Funcional
Implantación: Por personas
Por las computadoras sin que su aspecto externo sufra ningún cambio importante.

Ejemplo.- La aprobación del supervisor respecto al trabajo realizado por un operador de la computadora no es muy diferente a la aprobación del supervisor sobre el trabajo de los empleados de contabilidad.

CONTROLES TÉCNICOS :

Son controles nuevos.
Característicos de la tecnología de las computadoras.

Ejemplo.- Los controles de verificación de paridad son incorporados por los fabricantes del equipo de cómputo, para detectar fallas electrónicas en la transmisión o en el registro de los datos codificados en binario. No puede encontrarse una situación semejante en un procesamiento puramente manual.

Ciertos controles normalmente no se considerarían puramente lógicos o técnicos. Mas bien los controles relativos a las funciones de la computadora, se encuentran dentro de una gama de relativa complejidad técnica.

Muchos otros controles podrían ubicarse en áreas intermedias comprendidas entre tales extremos. Esto no implica que no haya nada de ilógico respecto a los controles técnicos considerando el medio técnico que origina su uso.

CONTROLES VERTICALES Y CONTROLES HORIZONTALES

Otra forma de clasificar los controles es, dividirlos entre aquéllos que siguen las líneas verticales de autoridad de un organigrama y aquéllos que siguen los flujos de procesamiento que cruzan dichas líneas.

CONTROLES VERTICALES:

-Son controles de supervisión que son ejercidos en dirección ascendente a lo largo de las líneas verticales del organigrama.

CONTROLES HORIZONTALES :

Son por ejemplo los documentos, los memoranda, los comunicados, los trípticos informativos que se envían entre los departamentos, pueden diagramarse horizontalmente entre niveles iguales de la organización.

La implantación de las computadoras implica en muchas situaciones un giro ascendente del nivel mínimo de supervisión común o del control de la gerencia.

Este giro ascendente afecta la naturaleza de los controles verticales, debido a que quienes tenían una autoridad general sobre los procesos, se encuentran en una posición más alta dentro de la organización y tienen menos tiempo para ejercer una supervisión detallada a partir de la integración de las computadoras a todas las áreas de la organización.

Por otra parte, en virtud de que ciertos departamentos adicionales participan en un proceso en el que antes existía un solo departamento, surge la necesidad de más controles horizontales. Una estructura organizacional que proporcionaba controles adecuados para un sistema manual, normalmente no proporcionará el mismo grado de control para un sistema después de la introducción de las computadoras y de aplicaciones integrales.

Lo anterior no quiere decir que los controles verticales, tales como la supervisión y la segregación de funciones, ya no sean importantes para un centro de cómputo; sin embargo, se reduce su efectividad y el énfasis relativo. Tal énfasis, debe dirigirse mas bien hacia los controles de tipo horizontal, tales como los documentos de envío, las cifras de control etc.

CONTROLES PREVENTIVOS, DETECTIVOS Y CORRECTIVOS

Esta clasificación se refiere a una determinada técnica de control, que evitará que ocurra un incidente, detectará el hecho de que ya haya ocurrido y corregirá sus efectos después de que haya sido detectada.

CONTROLES PREVENTIVOS:

-Reducen la frecuencia con que ocurren las causas de riesgo.
-Actúan como una guía para que las cosas sucedan como deben ser.
-Frecuentemente son pasivos y no implican ninguna actividad física directa.
-A menudo permiten cierto porcentaje de violaciones.

Los controles preventivos se encuentran a menudo tan sutilmente intercalados dentro de un proceso, que las personas involucradas en la operación pueden no estar siquiera conscientes de su existencia.

CONTROLES DETECTIVOS:

-No evitan que ocurran las causas de riesgo.
-Detectan causas del riesgo, después de que han ocurrido.
-Después se toma una decisión respecto de la acción correctiva apropiada y se lleva a cabo dicha acción.

Al detectarse una causa de riesgo se dispara una alarma. El control detectivo puede poner fin al procesamiento posterior o simplemente registrar la ocurrencia. Esta función de "vigilancia" con frecuencia es bastante confiable.

Los controles detectivos alertarán a las personas involucradas en el proceso a fin de que estén conscientes de la existencia de un problema. Tal conocimiento es imprescindible si ha de sugerirse la acción correspondiente para corregir los efectos de la causa detectada.

Control correctivo

Ayuda a la investigación y corrección de las causas de riesgo detectadas.
Una acción correctiva, es necesaria para remediar las causas de riesgo que se detectan.

En ciertas ocasiones puede decidirse que no vale la pena seguir una acción correctiva, pero tal decisión debe tomarse consciente y consistentemente. La alarma que proporciona un control detectivo es inútil si nadie la escucha. Debido a que los controles preventivos son a menudo pasivos (como las instrucciones para llenar una forma), es necesario un control detectivo para determinar si el control preventivo está funcionando. Aún si así fuese, los controles detectivos seguirán siendo necesarios para detectar los riesgos que evaden el control preventivo.

Los controles detectivos sobre los controles correctivos son esenciales debido a que la corrección del error es en sí misma una actividad altamente propensa a errores.

RELACIÓN ENTRE COSTO/BENEFICIO DE LOS CONTROLES

En los sistemas de información, como en cualquier otra parte, cada control tiene un factor de costo. Ningún control debe costar más que los errores potenciales para cuya detección, prevención o corrección se establece. El costo de comprender y corregir los errores no debe pasarse por alto en esta consideración de costo-riesgo. En la medida en que los controles se diseñan inapropiadamente o son excesivos. Debe hacerse una revisión para ver si los errores pueden ser descubiertos con mayor anticipación en el ciclo de procesamiento minimizando:

1. Los puntos de control requeridos.
2. El daño que puede hacerse al archivo.
3. El trabajo de corrección necesario.

Las necesidades de la gerencia y la importancia de cualquier error dado así como la evaluación de los costos y riesgos, son consideraciones efectivas para determinar en donde y en que medida deben aplicarse los controles

Controles preventivos

-Bajo costo.
-No son suficientes por sí solos.
-Se requiere cierta actividad correctiva.

Controles detectivos

-Gastos operativos moderados.

Controles correctivos

-Costosos

El diseño de controles óptimos, por lo tanto, requiere que se hagan una serie de consideraciones. El equilibrio entre los costos y los beneficios, debe encontrarse entre el costo de implantar controles preventivos

adicionales y el de llevar a cabo las actividades de corrección. La eliminación de los controles de detección, es rara vez un medio apropiado para reducir costos. Sin ellos, no pueden medirse ni la efectividad de los controles preventivos ni el riesgo resultante.

Los controles efectivos requieren una combinación de experiencia técnica, tanto en el manejo de negocios como en el área de sistemas. Los hombres de negocios y los técnicos en procesamiento de datos deben combinar en forma efectiva su experiencia para lograr el éxito de las operaciones resultantes.

Una persona cuya experiencia técnica es limitada puede tener dificultades para evaluar sus observaciones y convencer a la gerencia técnica que siga sus recomendaciones.

Hemos determinado que son relativamente pocas las organizaciones que tienen controles internos suficientes para prevenir o detectar confiablemente los actos de fraude y robo por medio de la computadora. Aparentemente, la única razón por la que estos actos no son más frecuentes, es que el personal del área de sistemas por lo general, es honesto.

La información dentro de la máquina desempeña un papel esencial en la organización. Una seria deficiencia en la calidad de esta información o su pérdida completa, pueden causar "amnesia organizacional". Esto ocurre cuando el centro de cómputo de la organización no proporciona información exacta y oportuna respecto a las actividades de la organización. Conforme una organización crece y trata con una sociedad cada vez más compleja, los efectos de la amnesia organizacional se vuelven más preocupantes. Se deben adoptar las medidas necesarias para asegurar que la supervivencia de la organización no se vea amenazada.

PROGRAMA DE CAMBIO DE CONTROL[14]

EL programa de cambio de control, es el proceso estructurado y disciplinado de la administración de cambios a los programas de aplicación de la producción. Esto, involucra cambios requeridos implementados para apoyar las necesidades de los negocios cambiantes de la organización en un ambiente tecnológico y dinámico. Es el proceso de realizar cambios controlados y deliberados a los procedimientos de procesamiento de datos de la organización con resultados conocidos que han sido probados y verificados.

El programa de cambio de controles críticos es para ayudar a asegurar la integridad de las aplicaciones. Donde sea que los cambios sean hechos, la reliabilidad y la integridad de la aplicación queda asegurada.

El programa de cambio de control puede también basarse para determinar o detectar un fraude por computadora o un sabotaje.

En resumen, el programa de cambio de control es diseñado para asegurar que:

1. Que los cambios a los programas sean autorizados.
2. Que todos los cambios autorizados sean hechos.
3. Que los cambios sin autorización sean prevenidos o detectados.
4. Solo la versión autorizada de un programa sea implementado.

[14]Conducido por el IIA´S International Advanced Technology Forum "Audit, control and security of paperless systems" "Trends, Guidelines, Practices and Techniques" Based on the proceeding of 1990. Advanced Technology Forum.

OBJETIVOS DE AUDITORÍA DE UN CAMBIO DE CONTROL[15]

Habiendo presentado la necesidad para un cambio de control y el alcance relevante los sigs. objetivos de auditoria son establecidos para satisfacer estas necesidades:

- Formalizar procedimientos.
- Requisición de recursos de procesamiento de datos.
- Aprobación de requerimientos

Controles correctivos

- Costosos

El diseño de controles óptimos, por lo tanto, requiere que se hagan una serie de consideraciones. El equilibrio entre los costos y los beneficios debe encontrarse entre el costo de implantar controles preventivos adicionales y el de llevar a cabo las actividades de corrección. La eliminación de los controles de detección rara vez es un medio apropiado para reducir costos. Sin ellos, no pueden medirse ni la efectividad de los controles preventivos ni el riesgo resultante.

Los controles efectivos requieren una combinación de experiencia técnica, tanto en negocios como en computación. Los hombres de negocios y los técnicos en procesamiento de datos deben combinar en forma efectiva su experiencia para lograr el éxito de las operaciones resultantes.

Una persona cuya experiencia técnica es limitada puede tener dificultades para evaluar sus observaciones y convencer a la gerencia técnica que siga sus recomendaciones. Al mismo tiempo, sin embargo, muchas actividades de las operaciones de la instalación de procesamiento de información siguen siendo en esencia juicios de negocios, por ejemplo la seguridad física. La evaluación efectiva de estas actividades queda comprendida dentro de las capacidades de una persona que únicamente posee antecedentes técnicos moderados.

La incorporación de distintos niveles de experiencia técnica respecto a los controles en el área de sistemas no impide que un gerente o un auditor con experiencia sólida en negocios y con conocimientos técnicos limitados diseñen, implanten o evalúen en forma efectiva los controles sobre el procesamiento de las aplicaciones en el centro de cómputo.

3.3 RIESGOS

Los controles son necesarios para un propósito. reducir los riesgos. Antes de empezar a evaluar los controles dentro de cualquier contexto, debemos identificar los riesgos que los controles deben prevenir detectar o corregir. La siguiente lista de riesgos incluyen una gran parte de los efectos adversos a los que puede enfrentarse una organización:

1. Contabilidad errónea
2. Pérdida o destrucción de activos
3. Costos excesivos/ingresos deficientes
4. Sanciones legales
5. Fraude y robo
6. Decisiones erróneas de la gerencia
7. Interrupción de la organización
8. Contabilidad inaceptable
9. Desventaja ante la competencia

[15]Conducido por The IIA'S International Advanced Technology Comitee "Audit, control and security of paperlesss systems" based on the proceeding of the 1990 Asvanced Technology Forum. sponsored by The Institute of Internal Auditors Research Foundation.

1. Contabilidad errónea:

Es el registro de transacciones financieras en forma contraria a las políticas contables establecidas. Los errores pueden referirse a la oportunidad en su registro, a su valuación y a su clasificación contable.

2. Contabilidad inaceptable:

Es el establecimiento o la implantación de políticas contables que no son de aceptación general o que son inapropiadas en las circunstancias. Esto también puede conducir a riesgos adicionales, tales como las sanciones legales.

3. Interrupción de las funciones de la organización:

Puede incluir desde la suspensión temporal de las operaciones, hasta el cierre definitivo de la organización. En última instancia, esto también afecta el principio contable de la organización en marcha.

4. Decisiones erróneas de la gerencia:

Son reprobables por sí mismas pero además pueden conducir a otros riesgos. Tales decisiones pueden derivarse de información falsa, falta de información o errores de juicio.

5. Fraude y robo:

La malversación directa de fondos es sólo una forma de fraude. El proporcionar deliberadamente información errónea a la gerencia o a los inversionistas es también un acto fraudulento, aún cuando se haga con el fin de no perder el empleo.

6. Sanciones legales:

Se refieren a cualquiera de las sanciones que pueden provenir de las diversas autoridades que tienen jurisdicción sobre las operaciones de la organización.

7. Pérdida o destrucción de activos:

Se refiere a la pérdida no intencional de activos , efectivo, cuentas por cobrar, o activos de información etc...

8. Desventaja ante la competencia:

Se relaciona con la incapacidad de una organización para sostener eficientemente su posición en el mercado o para responder eficientemente a los retos de la organización.

CAUSAS DE RIESGOS

Los riesgos no surgen simplemente por la falta de controles. Los riesgos son causados.
Los controles actúan para reducir o eliminar estas causas.

Una causa puede generar más de un tipo de riesgo. No existe una simple relación directa. Los diversos riesgos que pueden derivarse de una causa en particular normalmente no se presentarán con el mismo grado de probabilidad.

Estas relaciones pueden ilustrarse en forma tabular. En una tabla, las causas de riesgo pueden listarse en la parte superior y los riesgos potenciales resultantes, en forma vertical, en la parte inferior. Después, podríamos asignar valores numéricos a la izquierda de cada riesgo, para indicar el grado de probabilidad de que la causa provoque el riesgo.

Un riesgo:

Es el efecto de una causa (expresado en términos monetarios) multiplicado por la frecuencia probable de su ocurrencia[16]

El fuego en sí no es un riesgo, el riesgo es la destrucción que el fuego puede causar. Un control actúa para reducir una causa de riesgo, en vez de afectar al riesgo directamente. Por lo tanto, aún cuando los controles tienen por objeto reducir los riesgos, lo que en realidad hacen es actuar sobre una causa.

Como ya se mencionó, no existe una simple relación directa entre controles y causas, por consiguiente, varias técnicas de control pueden tener efectos sobre una causa particular, y una causa particular puede ser controlada mediante diversas técnicas.

No es necesario utilizar todos los controles que pudieran ejercerse sobre una causa en particular, sino únicamente aquéllos que sean suficientes para limitar el riesgo en forma efectiva, cuando los auditores encuentran que determinado control no está en uso, normalmente tienden a considerar esto como una deficiencia. Sin embargo, no resultará un riesgo neto si existe otro control que limite la misma causa al grado deseado.

En ocasiones, los auditores se sienten tentados a pedir que en un proceso en particular se establezcan simultáneamente todos los controles potenciales concebibles. Esto no es necesario (y de hecho, es un desperdicio) si los controles que ya se encuentran implantados y son suficientes por si solos. El efecto de un control que está sirviendo en lugar de otro se conoce generalmente como "un control compensatorio".

Estas relaciones se pueden ilustrar de la siguientes manera: las causas de riesgo pueden listarse en la parte superior y los riesgos potenciales resultantes, en la parte inferior. Asignamos valores numéricos a la izquierda de cada riesgo, para indicar el grado de probabilidad de que la causa provocase el riesgo en la tabla 3.1.

También podemos representar esta relación entre controles y causas en una tabla, listando las causas de riesgo en la parte superior, pero colocando los controles al lado izquierdo. Además también podemos utilizar números en las intersecciones para indicar el grado en que el control específico afectará a la causa especifica en la tabla 3.2.

Estas dos tablas pueden combinarse en una "tabla de evaluación de controles", simplemente colocándolas una sobre otra a fin de que las causas de riesgo se encuentren alineadas. De esta manera podemos observar la relación entre los tres elementos: control, causa y riegos, para analizar la calidad del control en la tabla 3.3.

[16]William C.Mair "Control y Auditoria de la computadora"
Instituto Mexicano de Contadores Públicos A.C.
Detroit Michigan 1980.

TABLA 3.1 POSIBLES RIESGOS CAUSADOS POR UN ACCESO NO AUTORIZADO AL CENTRO DE CÓMPUTO.

Grado de probabilidad del riesgo.

MAGNITUD DEL RIESGO	TIPOS DE RIESGOS
3	Acceso no autorizado con consecuencias graves.
-	Pérdida de información.
1	Robo de equipo de cómputo.
-	Daño al equipo de cómputo.
-	Acceso a información no autorizada.
-	Acceso a la consola del operador.
2	Acceso a manuales no autorizados a personas ajenas.
3	Pérdida o destrucción de activos del centro de cómputo.
2	Desventaja ante la competencia.

CLAVE DE LA MAGNITUD DEL RIESGO
3 -- Virtualmente Seguro.
2 -- Probable.
1 -- Posible pero improbable.
En blanco -- Muy improbable.

TABLA 3.2 RELACION ENTRE CONTROLES Y CAUSAS DE RIESGO

	CAUSA DE RIESGO
CONTROLES	ACCESO NO AUTORIZADO A LAS INSTALACIONES DEL CENTRO DE CÓMPUTO
Mesa de control de registro de e/s del personal.	1
Personas que entren deben contar con firma autorizada.	3
Puerta de acceso "Piggy Backing".	2
Gáfete de identificación con foto.	1
Al registrarse se deberá llenar una forma en donde especifique la razón del acceso, a que compañía pertenece etc.	1
Vigilancia por circuito cerrado de televisión.	2
Detector de metales .	3
Rayos "x" para portafolios, bolsas, cajas etc.	3
Reportes de eventos inesperados.	2

CLAVE DE LA EFICACIA DE LOS CONTROLES
3 -- Muy confiable.
2 -- Moderadamente confiable.
1 -- Útil Pero no confiable.
En blanco -- No tiene ningún uso importante.

TABLA FIGURA 3.3 TABLA DE EVALUACIÓN DE CONTROLES

	CAUSAS DE RIESGO	
CONTROLES	Acceso no autorizado al centro de cómputo.	
Mesa de control y registro a la entrada.	1	CLAVE DE LA EFICACIA
Persona debe contar con firma autorizada.	3	DE LOS CONTROLES
Puerta de acceso "Piggy Backing".	2	3 -- Muy confiable.
Gáfete de identificación.	1	2 -- Moderadamente confiable.
Debe llenar forma en donde se especifique la razón para el acceso , la compañía que representa etc.	1	1 -- Útil pero no confiable. En blanco -- No tiene ningún uso importante.
Vigilancia por circuito cerrado de televisión.	2	
Detector de metales	3	
Rayos "X" para portafolios, bolsa, cajas etc.	3	
Reportes de eventos no esperados.	2	
		RIESGOS
	3	Acceso no autorizado con consecuencias graves.
	-	Pérdida de información.
	1	Robo al equipo.
	-	Daño al equipo.
	-	Acceso a información no autorizada.
	-	Acceso a la consola del operador.
	2	Acceso a manuales no autorizados a personas ajenas.
	3	Pérdida o destrucción de activos.
	2	Desventaja ante la competencia.

ANÁLISIS DE LOS CONTROLES

Una vez que hemos elaborado una tabla de evaluación de controles, podemos evaluar la calidad del control. Como primer paso, asumimos que todas las causas de riesgo se encuentran presentes.

siempre funciona en forma perfecta, no hay razón para tener controles. Desafortunadamente, muchos sistemas en el área de sistemas se han diseñado sobre esta falsa premisa.

Los controles que se ha determinado que no son efectivos o bien que no existen, se eliminan de la tabla de evaluación, al igual que los efectos asociados con las causas del riesgo y después, se revisa cada causa de riesgo para determinar los controles que existen sobre ella. Esta revisión incluye la consideración de qué tan confiable se espera que sea cada control en la situación específica.

Posteriormente puede hacerse otro juicio respecto a los riesgos probables. Una vez analizados los controles de esta manera, podemos concluir si es probable que ocurra la causa particular y, de ser así, los riesgos resultantes.

Estas tablas y el análisis son un ejemplo basado en las tablas de análisis de controles de William C. Mair.

EFECTOS DE LA COMPUTADORA SOBRE LAS CAUSAS DE RIESGO

La introducción de la computadora en el procesamiento de la información de la organización desde un principio no afectó directamente a los riesgos que pueden presentarse, sino que, cambia los tipos de causas de riesgo, así como su frecuencia.

ÁREAS CLAVES DE RIESGO

La seguridad absoluta es algo casi imposible. No importa que tan bien se encuentren las medidas protectoras, siempre habrá algún daño sobre la computadora o sobre la información.

El objetivo de cualquier revisión de seguridad, es el de minimizar las debilidades que la organización enfrenta. Existe un gran número de técnicas para reafirmar la seguridad, no todas serán de utilidad o aplicables a una organización en particular. Es necesario seleccionar aquélla que sea la mejor opción.

El nivel de gasto sobre una protección requiere ser analizado, si el efecto de pérdida o daño será extremadamente caro para la organización, es absolutamente válido gastar una buena suma de dinero en la prevención de alguna contingencia. Sin embargo, si la información se pierde o es incorrecta y los efectos no son tan desastrosos, no es conveniente tomar precauciones muy elaboradas.

La vulnerabilidad hacia ciertos eventos pueden ser definidos como el costo en que una organización puede incurrir si el evento llega a ocurrir.

Un programa de seguridad debe ser diseñado para proteger una instalación de grandes desfalcos y de eventos pequeños como son: errores del operador, que pueden ocurrir muchas veces durante la semana. Consecuentemente, el programa de seguridad debe utilizar 4 métodos para reducir las debilidades anteriores:

1. Minimizar la probabilidad de que ocurra un abuso. Una parte importante de cualquier programa de seguridad física es reducir la manipulación y las malversaciones.

2. Identificar que un problema ha ocurrido. La seguridad de la instalación y los controles alrededor de los sistemas deben darnos detalles acerca de los personas no autorizados que han tratado de accesar a las instalaciones o a los sistemas. Estos detalles deben ser registrados y revisados regularmente.

3. Minimizar el daño de un evento. Una vez que un incendio ha empezado o un archivo ha sido accesado sin autorización los controles y los procedimientos que están funcionando deben ser suficientes para detectar el evento y restringir los efectos a una área pequeña.

4. Diseñar un método para recobrar información que ha sido dañada. Es importante para la continuidad de la organización que el rescate de la información sea rápido y efectivo, aún si se requiere el reemplazo del equipo o la reconstrucción de un archivo.

Dentro de cualquier instalación y en cualquier organización, habrá un conjunto en común de riesgos o áreas problema que siempre deben ser identificadas.

A continuación vamos a numerar ciertos preguntas que reflejan puntos fundamentales que deben ser entendidos y utilizados por el administrador Senior (o Gerente) y por el administrador del centro de cómputo.

1.¿Existen procedimientos rigurosos para controlar el movimiento de un programa o modificaciones a un programa?
2.¿Existe un plan de emergencia completo, documentado y probado?

3. ¿Existen controles adecuados sobre el acceso al cuarto de la computadora y al equipo asociado, así como las áreas alternas?

4. ¿La computadora lleva un registro automático del uso y la intervención del operador?
¿Esta intervención es revisada por la administración?

5. ¿El acceso a la computadora vía terminales está restringido por la necesidad de una identificación positiva por parte del usuario?

6. ¿Existe seguridad adecuada para proteger la documentación en contra de una utilización o manipulación no-autorizada?

7.¿Existen copias de respaldo del software del sistema, aplicación o información, que se toman regularmente y son almacenadas en un offsite?

8. ¿Las responsabilidades del departamento de usuarios y el staff del centro de cómputo están repartidas equitativamente?

9. ¿Existe un control adecuado sobre la adquisición y el uso de equipo de microcomputadoras, así como los paquetes de software que se utilicen?

10. ¿Existe un departamento de auditoría interna independiente y técnicamente competente?

ASESORAMIENTO EXTERNO PARA LA PROTECCIÓN EN CONTRA DE LOS RIESGOS

Los asesores externos asisten en la determinación de protecciones adicionales, esta forma de asesoramiento, asegura que las decisiones sobre los riesgos sean tomadas en el nivel correcto dentro de la organización y remueve los peligros inherentes de decisiones impulsivas, hechas por la gente equivocada.

Se deben también circular boletines y sumarios en tamaño de bolsillo, que sirvan como guías de seguridad y protección contra el riesgo. Para complementar esto, se necesita realizar muchas sesiones de entrenamiento de la gente del centro de cómputo en un esfuerzo de concientización.

IMPLEMENTACION

"La motivación de la gente de sistemas hacia una aceptación y cooperación voluntaria para realizar correctamente las protecciones en contra del riesgo, fue vista como el mejor método para garantizar el éxito."[17]

Todos los administradores de la seguridad encuentran difícil imponer medidas de seguridad, a menos que exista un entendimiento genuino por todos de la necesidad de implementarlas. Con esta mentalidad, se identifican algunas áreas débiles potenciales y a los empleados de todos los niveles se les dan ejemplos reales para que puedan relacionar y entender .

Ha habido un notable incremento en el número de peticiones para asistencia y consejo, recibida de los administradores, quienes están genuinamente interesados en construir controles dentro de los sistemas como un diseño previo y no posterior.

CONCLUSIONES

La primer tarea es realizar una campaña de apoyo a la gerencia; teniendo esto, el resto es razonablemente realizable. Sin embargo, sin este apoyo todos los esfuerzos serán truncados.

El administrador de la seguridad se convertirá legalmente en responsable por cualquier abuso, inexactitud o pérdida de información, y no solamente será una responsabilidad moral hacia sus clientes y su personal.

RESULTADO DE FALLAS EN LA SEGURIDAD

Cualquier abuso en los procedimientos y controles de seguridad de la organización puede tener un efecto serio en la misma. Si cualquier evento ocurre y es perpetrado por un empleado, éste puede tener un efecto limitado y tendrá vigencia en un período corto. La existencia, el método usado, el daño causado y la pérdida incurrida probablemente será conocida por solo un número pequeño de personas.

Las repercusiones pueden ser más obvias si el individuo es transferido o renuncia y son introducidos nuevos procedimientos.

Sin embargo, si el evento tiene repercusiones fuera de la organización o es perpetrado por alguien de afuera, o es suficientemente grande para afectar la función normal de la organización, la publicidad puede incrementarse.

La imagen de la organización se empañará, con una pérdida potencial en las finanzas.

La publicidad alrededor de cualquier incidente es el único método por el cual los detalles se vuelven ampliamente conocidos.

En México no existe la obligación legal de reportar cualquier evento, relacionado con este tipo de ultrajes y éstos no son registrados.

Esto trae como resultado, la dificultad para cuantificar el nivel de crimen en los centros de cómputo y hace imposible la identificación de las áreas débiles en común.

[17]Keith Hearden "A Handbook of Computer".

EL RIESGO EN SÍ

Claramente, algunos riesgos están fuera del control de la organización, a la cual afectarán. Consecuentemente, el problema se convierte en algo muy complejo.

Históricamente, la mayoria de las organizaciones han tenido una planeación de contingencias como actividad operacional discreta. Sin embargo, así como la industria se mueve en ambientes operacionales que proveen la habilidad de producir alimentos y servicios a bajo costo, esta actividad operacional discreta de planeación de contingencia, ha crecido en controles internos.

INFORMACIÓN A LA ADMINISTRACIÓN

Se le debe de informar a la administración de las exposiciones a los riesgos de gran importancia. La administración debe estimar estas debilidades, para preocuparse acerca de cómo recuperar lo que se ha dañado. La organización utiliza las técnicas relacionadas con la auditoria para medir las prácticas y procedimientos de la organización.

Los siguientes puntos pueden ser usados para alertar a la organización en caso de situaciones de riesgo de acuerdo con los estudios de Michael A. Murphy[18]:

1.- Considerar el efecto de un gran cambio de personal en el centro de cómputo.
No es bueno cambiar o reducir el grupo de gente del centro de cómputo, porque los nuevos en el staff pueden no tener el mismo entendimiento y habilidades.

2.- Evaluar la importancia de manejar un gran volumen de transacciones y cambiar la velocidad de su procesamiento.
Es importante tener cuidado pues también se necesita tener en los datos efectividad y exactitud.
Esto indicará el grado de necesidad para una recuperación de información.

3.- Evitar juicios que sugieren minimizar el riesgo a través de una percepción debajo del nivel de complejidad tecnológica.
Esta percepción puede ser errónea a través de tales condiciones como un entendimiento técnico incompleto, un alto nivel de dependencia del intersistema o a causa de la alta complejidad de la plataforma del equipo técnico.

4.- Asegurarse qué evaluaciones analíticas, incluyen cambios significativos en el sistema para implantar más complejidad y un alto grado de sofisticación en la tecnología.

5.- Ponga especial atención a los ambientes de mainframe con requerimientos de procesamiento remoto.
Los gastos o costos significativos de teléfono y telecomunicaciones connotan una alta dependencia sobre un procesador centralizado y redes complejas.

6.- Asegúrese que la protección del contrato del seguro incluya cobertura amplia de cargos y costos extra, así como interrupción en la organización y cubra el procesamiento de datos.

7.- Considere puntos contractuales y legales. Requiriendo otros métodos para proveer la habilidad para recuperar rápidamente estos arreglos de riesgo.

8.- Cuestione sobre problemas anteriores similares. ¿Cómo hizo la organización en circunstancia similar? ¿Salió bien?.

---

[18]Michael A. Murphy , Xenia Leyparkey " A Handbook of EDP Auditing"
Coopers & Lybrand
Edit. Warner, Gorgham & Lamont
Second Edition, 1989.

9.- Considere otras áreas. ¿Estas áreas carecen de experiencia para desarrollar e implementar una capacidad para recobrar información?.
Ciertamente una discusión abierta de progreso y problemas puede ser útil.

CÓMO ASISTIR A UNA RECUPERACIÓN DE LA ORGANIZACIÓN

Una planeación del rescate de la organización depende de la gente. Porque la gente está sujeta a la presión, especialmente durante una emergencia, no siempre actúan como debieran. El plan de contingencia se enfoca en acciones que deben tomarse, recursos que deben ser usados, y procedimientos que deben ser desarrollados antes, durante y después de la emergencia.

3.4.1 .INFRAESTRUCTURA FÍSICA.

Se refiere a los controles de acceso físico que son diseñados por la organización para proteger los datos, el equipo y al personal, en áreas restringidas.

Las debilidades físicas de la organización son:

1.-LUGARES DE ENTRADA AL CENTRO DE CÓMPUTO.
Las siguientes trayectorias deben ser evaluadas para una seguridad adecuada:

- Todas las puertas de entradas.
- Ventanas de vidrio y paredes.
- Sistemas de ventilación.
- Paredes falsas.

2.-DEBILIDADES DE TIPO FÍSICO.

Los imponderables que existen por la entrada de personas no autorizadas al centro de cómputo son:

- Daño al equipo y a la propiedad,
  Vandalismo al equipo y a la propiedad,
- Robo del equipo y a los documentos,
- Reproducción o revisión de información importante,
- Divulgación pública de información delicada e importante,
- Extorsión

3.- LOS INTRUSOS PROBABLES AL CENTRO DE CÓMPUTO SON :

- Empleados que tienen acceso autorizado, que no están bien informados y que cometen alguna falta por desconocimiento.

- Entrada no autorizada por empleados que están :

  1. Disgustados.
  2. En huelga.
  3. Personal no disciplinado.
  4. Adictos al juego o alguna substancia tóxica.
  5. Problemas financieros o emocionales.
  6. Notificados de su renuncia.

- Empleados de planta.

- Gente de afuera interesada o bien informada, como son los competidores, ladrones, crimen organizado y piratas.

- Una persona carente de conocimientos informáticos que desconoce que ha realizado una operación no-autorizada.

La seguridad debe pensar en todo tipo de intrusos.

Desde el punto de vista del control, lo que se debe proteger es lo siguiente:

- Área de programación.
- Cuarto de la computadora grande y del equipo.
- Consolas del operador.
- Libreria de cintas.
- Cuarto de almacenamiento.
- Almacenamiento remoto de los archivos de respaldo.
- Cuarto de control de las Entradas/Salidas.
- Gabinete de comunicaciones.
- Equipo de telecomunicaciones.
- Fuentes de energía.
- Impresoras fijas o remotas.
- Redes locales.

No se deben descuidar las locaciones remotas, las instalaciones rentadas y los recursos compartidos.

CONTROLES FÍSICOS

Los controles físicos deben limitar el acceso a aquellos individuos autorizados por la administración o la Gerencia.

Esta autorización debe ser explícita, señalando la descripción del trabajo, la cual va a justificar la necesidad de consultar documentos y reportes importantes.

A continuación vamos a mencionar la mayoría de los controles físicos que se llevan a cabo actualmente en las grandes organizaciones :

-LOCALIZACIÓN

Existen varias cosas que el administrador puede hacer antes de que el centro de cómputo sea establecido.

Una de la primeras precauciones es que el centro de cómputo debe estar en un edificio separado y construido por materiales no-combustibles.

Si es utilizada más de una computadora grande o mediana, es deseable que se encuentren en cuartos separados para limitar cualquier desastre.

Se deben construir gabinetes de equipo electrónico resistentes al fuego, así como la construcción de paredes, columnas,muelles,vigas,trabes,armaduras, pisos y techos de material inherentemente no combustible como son : el acero, metal, aluminio, ladrillo, concreto, vidrio, cerámica, yeso, asbesto etc. Todos estos materiales

deben ser tratados para tener cualidades retardantes de fuego. Los materiales utilizados para acabados de interior, barreras de vapor o tratamientos acústicos deben conocer el criterio de no-combustibilidad.

Es importante saber donde localizar el centro de cómputo. Si el centro de cómputo se encuentra en un gran edificio, con todos sus requerimientos completos contra el fuego y en orden, pero las partes adyacentes a él, son altamente combustibles, no habrá servido de nada.

Al igual si la localización del centro de cómputo se encuentra al final de la pista de los aviones que la utilizan para despegar, o al lado de un río, es una invitación al desastre.

Si el centro de cómputo por sí mismo no puede ser localizado en un edificio por separado, (y usualmente no es posible), luego por lo menos debe estar separado del resto de las premisas por un paredes y pisos resistentes al fuego y no combustibles. En esto la resistencia debe de ser por lo menos de 2 horas. Si el centro de cómputo está localizado en una fábrica o en un edificio de almacén, se recomiendan 4 horas de resistencia. Si no es posible tener un sistema de resistencia contra el fuego, es recomendable conseguir un sistema de dispersador de agua.

La sala de cómputo debe estar ubicada en un área de máxima protección a la exposición de riesgos tales como incendios, inundación, terremoto, vibraciones, suciedad y humedad excesivas.

Considere si es remoto, fija, o en un estado industrial, cerca de un área pobre, en un lugar delictivo, o muy solo, o con un canal, río, vías del tren, de acceso fácil para un intruso. Investigar el perfil de crimen, preguntando a los que trabajan o viven por esa área y a la policía local.

- PROTECCIÓN POR FUERA.

Busque por los límites, bardas, agua, vías del tren, carreteras y cualquier otra forma de barrera natural. Entonces considere las debilidades. La protección más común es el de las bardas alrededor.

Una barda de dos metros y medio de altura con una malla de fierro hasta arriba de la barda, es considerablemente bueno y sirve como un factor de retraso para el intruso.

- REFLECTORES Y LUZ EN LUGARES ESTRATÉGICOS.

Esto es una excelente obstáculo para los intrusos. A ningún intruso le gusta tener una gran sombra en algunas lugares y en otros tener muy poca luz. Puede ser utilizado para iluminar edificios, áreas entre edificios y con cierto tipo de suelo para dejar huellas de tierra entre ciertas barreras en el perímetro; Entre los edificios se puede utilizar durante las horas de oscuridad. Un sistema de interrupción de switches, que se active cuando un intruso pase. Un sistema de alarma auditiva puede ser incorporado.

-ACCESO

Es recomendable que al planificar una sala de cómputo se tomen en consideración la entrada y salida de maquinas y equipo (entrega inicial, entrega de ampliaciones, cambios de máquinas, mudanzas etc..)

La zona de descarga de los equipos, así como accesos y pasillos que conduzcan a la sala de cómputo deben ser capaces de soportar la carga de los equipos a ser instalados.

Ventanas, puertas y/o corredores a ser utilizados entre la zona de descarga y la sala deben estar dimensionados para acomodar equipo embalado, más el espacio para herramientas de transportación.

-DIMENSIONES

Las dimensiones mínimas de la sala están determinadas por la cantidad de componentes del sistema, el espacio mínimo requerido por cada unidad para su mantenimiento, área de operación, etc.

El layout del sistema y las expansiones futuras, deben también ser consideradas al planificar el tamaño de la sala; paredes y paneles removibles pueden ser utilizados para facilitar ampliaciones futuras.

Unidades modulares de aire acondicionado y servicio eléctrico prevendrían el crecimiento potencial del sistema.

En adición a la sala de cómputo se debe proveer espacio para lo siguiente:

1. Almacenamiento de cintas y/o cintas magnéticas.
2. Formularios y papel para impresora.
3. Mesas de trabajo y muebles.
4. Área y mobiliario para mantenimiento.
5. Equipo de teleproceso.
6. Área de programación.
7. Consolas del operador.
8. Cuarto de control de entradas y salidas
9. Micro computadoras.
10. Fuentes de poder.

-ILUMINACIÓN

1. El interior de nuestra premisa debe ser iluminada durante la noche.

2. El lugar deberá estar bien iluminado y fácilmente visible desde afuera.

3. Todos los puntos de acceso de afuera, especialmente de la parte posterior y del las puertas deben estar bien iluminadas.

-VENTANAS

1. Todas las ventanas, aparte de aquéllas que sirven para incendios, deben ser aseguradas. Puertas de acero, barras o mallas en las puertas, para que no pueda ser removido nada de ahí; Si no se controla las cerraduras de adentro.

2. Las ventanas de hierro que sirven para los escapes de incendio, deben ser equipadas con una llave de control desde cerraduras por dentro.

3. Las ventanas de afuera con bisagras deben tener clavijas de bisagras no removibles.

-LLAVES

Como una práctica generalizada:

1. Las llaves deben ser dadas sólo por el personal responsable y por sólo cierto número de persona tanto como sea posible y razonable.

2. Cambie la llave cilindro, en caso de que una persona que haya sido encargada de la llave haya renunciado, lo hayan relevado o cuando la llave se haya perdido.

3. No utilice un sistema de cerradura, el cual es "master keyed" a menos que sea absolutamente necesario.

4. No deje las llaves tiradas por donde quiera durante el día; cuando alguna persona sin autorización puede tomarlos y hacer una copia de esta.

5. Utilice una llave de cilindro, que generalmente su duplicación será mas difícil.

- CERRADURAS DE PUERTAS "BOLTING".

Estas cerraduras requieren la tradicional llave de metal para entrar. La llave debe ser estampada con una leyenda que diga "NO DUPLICARSE".

Este sistema utiliza un letrero de numérica o un combinación para poder entrar. La combinación debe ser cambiada en intervalos regulares o cuando un empleado con acceso sea transferido, corrido o sujeto a una llamada de atención por una acción indisciplinada. Esto reduce el riesgo de que una combinación sea conocida por gente sin autorización.

- CERRADURA DE PUERTA ELECTRÓNICA.

Este sistema utiliza una tarjeta de plástico magnético como llave, la inserta dentro de un sensor lector para poder entrar. Un código especial internamente almacenando en esta tarjeta, es leída por el dispositivo sensor que entonces activa el mecanismo de cerradura. Este sistema tiene las siguientes ventajas sobre las cerraduras "bolting" y las cerraduras de combinación :

1. A través del código interno especial, las tarjetas pueden ser asignadas a un individuo bien identificado.

2. A través de un código interno especial, y por los dispositivos sensores, el acceso puede ser restringido basados sólo en los individuos que necesiten realmente entrar. Las restricciones pueden ser asignadas a ciertas puertas en particular o a ciertas horas en particular del día.

3. Es difícil duplicar.

4. La entrada de la tarjeta puede ser fácilmente desactivada, en el momento en que el empleado se haya ido, o su tarjeta haya sido perdida o robada.

5. Alarmas silenciosas o audibles pueden ser activadas automáticamente si una entrada ilegal trata de accesar. "emisión, controlar, y recuperación " la tarjeta llave es un proceso administrativo que debe ser cuidadosamente controlado. La llave tarjeta es un punto importante para recuperar cuando un empleado se va de la firma.

- CERRADURA DE PUERTA BIOMÉTRICA.

Estas cerraduras son activadas por una serie de dispositivos individuales como son, la voz, la retina, las huellas digitales o la firma. Este sistema está siendo usado en instancias cuando ciertas facilidades son extremadamente sensibles y se deben proteger, así como en la milicia.

- PUERTAS "DEADMAN".

Las puertas Deadmen, tipicamente encontradas en entradas a lugares sensitivos como son la sala de maquina, cuarto del computador y las estaciones de documentación, consisten en dos puertas. Para que la segunda puerta pueda operar, la primera puerta de entrada debe estar cerrada y con seguro con solamente una persona permitida en el área. Esto reduce el riesgo de que una persona no-autorizada siga a una persona autorizada a través de una entrada de seguridad.

- PUERTAS, MATERIAL DE LAS PUERTAS, CERRADURAS DE LAS PUERTAS.

1. Puertas con corazón sólido son preferibles, que puertas de panel o puertas de vidrio.

2. Puertas delgadas de panel o puertas con corazón hueco deben ser delineadas con hojas de metal.

3. Puertas de panel de vidrio deben ser cubiertas con barras de metal o con fuertes mallas de red sobre el interior de la puerta.

4. Si hay una puerta con vidrio, la cerradura de la puerta del interior debe requerir una llave y no simplemente un pasador. En el argot de los cerrajeros debe cerrarse con llave por dentro.

5. La bisagra del exterior de la puerta debe tener bisagras no removibles.

6. Si la puerta es suficientemente fuerte para las bisagras o es débil, se debe poner una cerradura donde la seguridad no dependa de la estructura de las bisagras para montarlo.

7. La cerradura de la puerta debe tener un cerradura fuerte y debe ser usado en conjunción con una llave de cilindro resistente.

8. Si se utiliza una cerradura de llave, debe ser de un picaporte de calidad resistente.
Todos los números de identificación deben ser borrados de las llaves antes de que se use.

9. Las puertas del techo que salvaguardan la de energia eléctrica y luces eléctricas deben estar cerradas. Deben tener un picaporte de cilindro resistente.

10. Las puertas del elevador que abren directamente en oficinas o áreas sin seguridad deben ser equipadas con una llave de cerradura de control.

11. Donde sea necesario, deben ser utilizadas esas "barras de pánico" que se utilizan en las salidas de emergencia, la cual active una alarma, que indique cuando la puerta es abierta durante las horas de trabajo.

-PUERTAS DE METAL

1. Acorde con los diferentes tipos de puerta deben ser equipados hasta arriba y hasta abajo con pistas corredizas y deben ser cerradas con la cerradura el cual es un picaporte resistente y que resistirá el uso de la fuerza. Las cerraduras deben de tener números identificación, hay que borrarlos antes de usarlos.

2. Las bisagras de afuera o por fuera deben tener unas clavijas de las bisagras no removibles.

-HACTCHWAYS (ESCOTILLÓN O PUERTA DE TRAMPA)

1. Los hatchways deben ser seguros desde el interior con un cerrojo de barril y cerrados con candado.

-TRAVESAÑOS

1. Los travesaños deben ser cubiertos con barras de metal o con malla los cuales no puedan ser removidos.

2. Los travesaños deben ser seguros desde el interior con llave de cerradura que controle la ventana.

- CERRADURAS A LA TERMINAL DE LA COMPUTADORA.

Las cerraduras de la terminal pueden ser para:
1) Cerrar el dispositivo al escritorio.
2) Prevenir al computador de ser prendida.

-ALARMAS Y CERRADURAS

En nuestros días tenemos una gran variedad de alarmas disponibles. Éstas incluyen alarmas fotoeléctricas que reportan cualquier intromisión en el haz de luz, detectores de movimiento que detectan cualquier movimiento, ya sea por sonido o por rayos de luz dentro del área protegida, y alarmas a la premisa que se activan cuando una puerta o una ventana es abierta después que la alarma ha sido activada por la noche. Otros dispositivos mas complicados incluyen sistemas de detección de vibración. Un consultor experto puede recomendar un tipo especial de sistema de seguridad.

Las alarmas pueden ser instaladas para notificar a la policía, al propietario o un guardia de seguridad sobre cualquier intromisión o fuego. Las alarmas que producen un sonido como de sirena; simplemente asustan a los intrusos cuando ya se fueron y son comúnmente ignorados por casi todos.
Una de las más viejas y baratas de protección es la vieja y simple cerradura. Las cerraduras, como cualquier otro dispositivo de protección, son buenos sólo si se utilizan adecuadamente.

Si las cerraduras de seguridad que son caras, son instaladas pero nunca cerradas, son de muy poca utilidad o si muchas copias de las llaves están disponibles, muy poca protección se ha ganado. La mejor situación de la cerradura incluye buena resistencia del picaporte, que permite para las llaves tener todo bajo absoluto control. Esto significa tener llaves que no puedan ser duplicadas en la tienda de la esquina.
Las llaves y las cerraduras son conseguidas de una compañía de cerraduras con la garantía que la llave que nos den no está disponible como una llave estándar comercial. Como una precaución todas las llaves deberán contener una leyenda "No duplicar".

Este tipo de compañías también ofrecen un plan de seguridad para la organización. Esta consiste, en que si una sección de la planta es utilizada durante los fines de semana, como son el centro de la computadora, el resto de la planta puede ser cerrado para prevenir que los empleados anden por el resto de la planta durante la noche o los fines de semana.

Un nuevo tipo de cerradura el cual puede ser abierto sólo por una tarjeta de identificación ahora está disponible. estas cerraduras son construidas, así un registro es guardado de quien abre cada puerta y las cerraduras pueden ser instaladas, así sólo ciertas tarjetas de identificación pueden abrir solo las puertas necesarias para su función.

- SISTEMA DE ALARMA.

Un sistema de alarma debe ser unido a una serie de puntos de entrada inactivos, detectores de movimiento en áreas de seguridad, y el flujo de entrada- o salida- sólo las puertas. El personal de seguridad debe estar disponible para oír la alarma cuando se active.

- DISPOSITIVOS DE ALARMA.

Contactos infrarrojos, microondas, ultrasónicos, tapetes de presión, o detectores de vidrios rotos; Hay que tener cuidado con la duplicación de recomendaciones.

Cuando un sistema de alarma ha sido elegido, prefiera un señal silenciosa a una compañía de alarmas y esta puede ser complementada por sirenas o campanas, éstas pueden sonar después de haber activado la alarma silenciosa. El objetivo es el de traer al intruso afuera antes de que se quiera sacarlo y le haga daño o interfiera con el equipo.

Asegúrese de un adecuado sistema de encargados de llaves como soporte en caso de emergencia, informando a la policía local y a la compañía de alarmas de los hombres, direcciones y números de teléfono de al menos tres de los encargados de las llaves, que sean elegidos, si es posible, porque ellos tienen transporte y pueden estar en las premisas dentro de unos 20 minutos.

Existen muchos tipos de alarmas:

1. Un sistema de alarma central, la cual trae una respuesta directa de la policía y/o la alarma de la compañía, son las mejores. La instalación es costosa y trae consigo una renta mensual.

2. Las alarmas electrónicas son disponibles con telefono o una grabadora donde se deje el mensaje a cualquiera que usted designe.

3. Las alarmas locales suenan una campana en las premisas. Los vecinos avisaran a la policía cuando la alarma sea activada.

4. Una alarma no debe ser diseñada para ser desactivada desde afuera de las premisas. Utilice una alarma que emplee un mecanismo de retardo de tiempo y que la desactivación sea por una llave desde adentro.

-VIDEO CÁMARAS Y CIRCUITO CERRADO DE TELEVISIÓN (CCTVCLOSE CIRCUIT TELEVISION)

Las video cámaras deben estar localizadas en puntos estratégicos y monitoreados por guardias de seguridad. Cámaras sofisticadas de video pueden ser activadas en el momento de ver un movimiento.

El grabado de video debe ser retenido para un posible futuro que necesitemos un playback, regresarla y ver que paso a una determinada hora.

El C.C.T es un suplemento ideal, pues tendremos en donde sea un guardia y una facilidad de patrullaje. Tiene valor en la búsqueda de áreas especificas e importantes de cualquier lugar del edificio o fuera de los edificios. Es importante poder observar sucesos grabados con anterioridad, y contar con cámaras infrarrojo, para que se pueda ver también de noche. Tenga en mente, que para que sea completamente efectiva, el C.C.T. deben ser observadas sobre una de tiempo-real y recursos del staff deben ser considerados.

Existen muchos tipos del CCTV. Algunos van sólo con una alarma que es activada, otras están prendidas todo el tiempo y aún otras son sólo cámaras que no funcionan para bloquear o inhibir a un intruso potencial. Algunas cámaras son monitoreadas por una estación de guardia central en un gran cuarto, mientras otras como en los bancos simplemente están filmando y las cuales pueden regresar la cinta, ya sea como una rutina básica o en cada sospecha. A veces existen una objeción del empleado para la instalación de cámaras, asi que ese factor también debe ser considerado.

- REGISTRO DE BITÁCORA.

1. Bitácora Manual

Todos los visitantes deben ser registrados en una bitácora de visitantes indicando su nombre, la compañía que representan, la razón de la visita y a la persona que vienen a ver. Un típico registro de bitácora es tener en el frente un escritorio de recepción y a la entrada del cuarto del computador. Antes de entrar, los visitantes deben también dar algún método para la verificación de su identificación, por ejemplo, una licencia de manejo, una tarjeta de negocios, su tarjeta de identificación del vendedor.

2. Bitácora Electrónico

Este es un mecanismo de sistema de seguridad electrónico y biométrico. Todos los accesos pueden ser registrados. Una serie de atentados sin éxito, también pueden ser bien registrados.

- ACCESO DE VISITANTES ESCOLTADO/CONTROLADO.

Todos los visitantes deben ser escoltados por un empleado responsable. Dentro de los visitantes se incluyen amigos, gente de mantenimiento que repara, vendedores de computadoras, consultores (a menos que sean a un término largo, o en el caso de un invitado especial), personal de mantenimiento de limpieza (recordar la gente que le da mantenimiento a las flores y plantas), y los auditores externos.

-VISITANTES CON GÁFETE

Una gafete a la vista tiene muchos otros usos, uno es el de ser distinguido por ser visitante. El visitante es uno de los más comunes intrusos en cualquier centro de cómputo. Aún así la mayoría de las instalaciones del computador tiene como señal en la puerta "Sólo personal autorizado" , esta es regla generalmente ignorada porque es casi imposible decir quién esta autorizado.

Uno de los caminos más fáciles para llevar a cabo esta regla es el de ordenar que todos los visitantes deben ser escoltados y todos los empleados deben tener un gafete de identificación.

El personal puede llamar la atención a cualquiera que no tenga su gafete apropiado o a cualquiera con un gáfete de visitante y que no esté escoltado.

Tours guiados es bueno para las relaciones públicas, pero esto también ofrece una excelente oportunidad para que un intruso obtenga un mapa de la planta.

- UN SÓLO PUNTO DE ENTRADA, MONITOREANDO POR MEDIO DE UNA RECEPCIÓN.

Todas las personas que deseen entrar , lo harán a través de un punto de entrada controlado. Demasiados puntos de entrada incrementa el riesgo de una entrada no autorizada, así que se deberá limitar el número de puntos de entrada a uno o dos ; También eliminar las cerraduras innecesarias o inutilizadas de ciertos puntos de entradas.

- ACCESO DURANTE LAS HORAS DE TRABAJO.

Gente sin autorización debe mantenerse alejada del equipo del computador y sus áreas asociadas, porque:

1. Pueden hacer sin saber o maliciosamente un daño al equipo o a los diferentes dispositivos.

2. Pueden ver información confidencial.

3. Pueden interferir con el funcionamiento de la computadora.

4. Distraen a los operadores.

5. Pueden introducir contaminación dentro del centro de cómputo.

6. Estas personas no están al tanto de los estándares requerido por las personas dentro del cuarto del computador.

La autorización debe ser restringida solo a aquella gente que necesite tener acceso, lo cual significa que solo la gente opera y mantiene el equipo.

Debe ser necesario restringir el acceso, no solo al cuarto del computador, al almacenamiento de media y el cuarto de los periféricos, también al cuarto de preparación de datos o información, a los almacenamientos temporales, área del que lleva a cabo el control, a los cuartos de descanso de los operadores, al área de programación y a las áreas de las terminales de los usuarios.

-IDENTIFICACIÓN CON FOTO PARA TODO EL PERSONAL

Debería de traer todo el personal gafetes de identificación.
Los gafetes de identificación de los visitantes debe ser de diferente color del gafete de los empleados para una rápida identificación. Identificaciones con foto sofisticadas, pueden ser también utilizadas como tarjetas electrónicas llave. Emisión, confiabilidad y la recuperación de las identificaciones es un proceso administrativo que debe ser cuidadosamente controlado.

- REPORTE/DOCUMENTACIÓN DE SEGURIDAD DE LA DISTRIBUCIÓN DE GAFETES.

Reporte/Documentación de la distribución de gafetes, por ejemplo, los gafetes por correo, debe ser cubierta y cerrada o deberá ser dejada sin atender.

- NO SE DEBE COLOCAR LETREROS QUE INDIQUEN LA LOCALIZACIÓN DE LUGARES SENSITIVOS O IMPORTANTES.

Los lugares como los cuartos del computador no debe ser visible o identificable desde afuera, por ejemplo, no ventanas o señales de dirección indicando donde se encuentra el cuarto del computador. El edificio o el departamento de Directorio debe ser discretamente identificado sólo en la localización general de la información del lugar donde se encuentra el procesamiento de datos.

- EL PERSONAL DE MANTENIMIENTO.

Personal contratado para servicios especiales, como son personal de limpieza y servicio remoto de almacenamiento, debe ser conocido y obligado a registrarse. Esto no mejora la seguridad física pero limita la exposición financiera de la organización.

- LIMPIEZA DE ÁREAS DE CÓMPUTO.

El personal de limpieza son tan familiares como cualquiera, y no les prestamos mucha atención.

Ellos crean una imagen confortable de honestidad y confianza en la mente de la Gerencia o Administración. Algunas veces ellos son encargados con la importante tarea de revisar las alarmas y ponerlas a trabajar. Los riesgos involucrados en emplear al personal de limpieza en estos tareas o en otras tareas más, se reduce poniendo las siguientes recomendaciones en marcha:

1. Trate que el personal de limpieza trabaje durante horas de trabajo normal. Esto será un inconveniente para el personal del staff, pero ha sido encontrado aceptable.
2. Supervisar el trabajo del personal de limpieza, y checar en caso de que se realice otra actividad.

3. Asegúrese que este personal se rote regularmente, y no haya personal de limpieza que traiga su propia ayuda, así como a sus hijos adolescentes o hijas.

4. Dé prioridad, para asegurar que las computadoras sean adecuadamente cerradas, las terminales estén apagadas y no haya oportunidad de un acceso no autorizado a la información del computador.

5. Asegúrese que los manuales, documentos estén guardados bajo llave.

6. De atención apropiada a los papeles gastados, llevándolos a un lugar donde se destruyen este tipo de papel.

- GUARDIAS DE SEGURIDAD.

Los guardias es un dispositivo exitoso, si lo complementamos con video cámaras y cerraduras de puertas. Los guardias se obligan a proteger la organización de una pérdida.

Guardias uniformados pueden proveer prevención y protección. Los guardias profesionales bien entrenados pueden ser contratados por una compañía individual reconocida. La ventaja de que la organización cuente con sus guardias es más barato y hay un control mas rigido. Pero una agencia de guardias privados ofrecen las ventajas de un mejor entrenamiento de guardias, menos personal de quien preocuparse, y también muchos servicios auxiliares, como investigaciones de seguridad, agentes de servicio secreto y adiciones temporales de patrullas durante un período de crisis.

- MICRÓFONOS ESCONDIDOS

Otros tipos más complicados, son los dispositivos que incluyen, un equipo moderno de micrófonos escondidos.. Aun así las leyes prohiben la venta legal de los micrófonos escondidos, excepto para la policía. Los micrófonos escondidos son , aún asi, disponibles gracias a. muchas firmas en los Estados Unidos y en nuestro país México venden diagramas esquemáticos para que la gente que quiera hacer el suyo y de acuerdo con detectives privados, los micrófonos escondidos son a veces anunciados y vendidos como juguetes.

Periódicos, revistas de seguridad y publicaciones de ejecutivos regularmente traen equipo electrónico que despliegan esto en Estados Unidos. Los investigadores del Servicio de Información, una firma de electrónica en Los Ángeles, tiene una cadena de ventas que tienen muchos micrófonos escondidos. La mayoría de estos se anuncian, sin embargo son vendidos solo a la policía.

-MEJOR DESTRUIDO QUE LEÍDO

En las organizaciones modernas se vive en montañas de papel y las computadoras proveen montañas adicionales de papel. Estas montañas se suman al problema de seguridad.

En la mayoría de las grandes ciudades está prohibido quemar el papel inservible o ya usado, así la destrucción del papel es la única protección en contra del mal uso de los archivos confidenciales descartados. Listas de teléfono, archivos de clientes, archivos de nómina, reportes de investigaciones y archivos personales son algunos de los reportes que deben ser destruidos cuando ya no se necesitan.

Parte de cualquier programa de seguridad debe ser la clasificación de documentos confidenciales. Los programas pueden ser escritos, así los reportes confidenciales de la computadora pueden ser etiquetados. Algunas veces esto es hecho, así cada página tiene una etiqueta confidencial y una fecha de destrucción. Etiquetado con una fecha de destrucción, facilita la destrucción de un reporte y reduce costos caros de almacenamiento. Desde que los centros de cómputo son notorios por correr reportes inservibles, una etiqueta puede recordar al centro de cómputo para canalizar un mal reporte para destruirlo, en vez de tirarlo a un basurero, donde un espía industrial o un empleado entrometido pudiera tomarlo.

- SISTEMAS SOFISTICADOS.

Existen muchos sistemas de control de acceso sofisticado disponibles, como son el scan del ojo, y el scan de la huella digital, pero estos son muy caros y no muy comunes.

- LÍNEAS DE TELECOMUNICACIONES.

Los sistemas de ON-LINE involucrán el uso de líneas de telecomunicación, las cuales pueden ser pegados con cinta en el cuarto del computador, dentro de la instalación del computador, en la calle o en un intercambio. No existe una seguridad completa sobre una línea.

El nivel de riesgo puede ser disminuido por la instalación de técnicas de encriptamiento, mezclar los instrumentos del teléfono y más sistemas sofisticados.

En este campo el riesgo más grande es el profesional torpe, por ejemplo un Ingeniero que tenga acceso legítimo a todas las telecomunicaciones de la empresa. La supervisión de la administración sobre los Ingenieros es teóricamente buena, sin embargo hay prácticas obvias de problemas de supervisión.

- RESGUARDOS

Cuando se utiliza un resguardo para otro propósito que el de la protección de los registros del fuego, utilice un resguardo tipo "Cajón". Aquellos resguardos son diseñados para proteger cosas valiosas de que las roben.

Si el resguardo es de un tipo movible, quítele las ruedítas y ancle el resguardo al piso.

También, como una práctica en general:

1. No deje una copia escrita de la combinación de las premisas.
2. Cuando a un empleado renuncia o es relevado de su puesto, cambie la combinación.
3. Sobre cerrar el resguardo de vuelta o marque la combinación al menos cuatro veces.
4. Haga depósitos bancarios frecuentemente como sea posible, y trate de no confiar en un resguardo como los anteriores como protección de la noche.

- SEGURIDAD FÍSICA DEL CENTRO DE CÓMPUTO REMOTO

La seguridad física del centro de cómputo remoto debe ser evaluada para asegurar que tenga un acceso apropiado y que cuente con controles ambientales. Estos controles incluyen la habilidad de limitar el acceso sólo a los usuarios autorizados, piso elevado, controles de humedad, controles de temperatura, circuitos especiales. Abastecimiento ininterrumpible de energía eléctrica, dispositivos de detección de agua, detectores de humo y un sistema apropiado de extinguidores. Se debe examinar el equipo para una inspección actualizada y una calibración de etiquetas.

-SEGURIDAD FÍSICA SOBRE EL ALMACÉN DEL CENTRO DE CÓMPUTO REMOTO

El almacén del centro de cómputo remoto, debe tener los mismos controles de seguridad que tiene el centro de cómputo fijo, el acceso al lugar debe estar limitado a aquellos individuos con una necesidad real para el acceso. Como el procesamiento de información del centro de cómputo remoto, la identificación del edificio y sus contenidos no debe ser aparente a un observador casual. También el almacenamiento del centro de cómputo remoto no debe ser sujeto de los mismos desastres naturales que afectan al centro de cómputo original. Así, su localización no debe estar muy cerca del centro de cómputo original.

Como la facilidad del procesamiento de la información, al almacenamiento de la facilidad del OFFSITE debe también poseer el mismo monitoreo constante y el control del SITE original. Esto incluye el monitoreo de la humedad, temperatura y el aire que está alrededor para que logre condiciones óptimas para el almacenamiento magnético.

-PROBANDO LAS SALVAGUARDAS FÍSICAS DEL LUGAR

Muchas de las pruebas de las salvaguardas físicas del lugar pueden ser logradas o conocidas por simple observación de las mismas. Las pruebas deben extenderse a las áreas adyacentes al centro de cómputo para conocer:

1. Localización de todas las consolas del operador.
2. Cuartos de impresión.
3. Cuartos de almacenamiento de la computadora(Esto incluye equipo, papel y cuartos de abastecimiento).
4. Localización de UPS.
5. Localización de todo el equipo de telecomunicaciones identificado sobre un diagrama de redes.
6. Librería de cintas.
7. Lugar de almacenamiento del lugar de respaldo remoto.

Para hacer una prueba más concienzuda, se debe también mirar sobre el techo de paneles y abajo de los pisos falsos en las operaciones del centro, buscar detectores de humo y de agua, limpieza en general y los paneles que estén extendidas hasta abajo del techo real (no sólo al techo falso).

-PISO FALSO

Este tipo de pisos permiten organizar el tendido y protección del cableado del sistema, más la facilidad de reacomodar el sistema.

Los pisos elevados también proveen un excelente método para llevar el aire acondicionado cerca de las unidades del sistema, permitiendo la adición o recolocación de las rejillas de aire cuando son agregadas o recolocadas máquinas en la sala.

Un piso falso debe ser capaz de soportar una carga uniforme de no menos de 1200 kilos por metro cuadrado y una carga concentrada de 1000 kilos por centímetro cuadrado.

La capacidad de soportar unidades adicionales debido al potencial de crecimiento futuro del sistema debe ser considerado.

La distancia entre la superficie del piso del edificio y el piso falso debe tener 45 cm. cuando es usado como cámara plena de aire acondicionado, la altura del plafón, desde el piso falso terminado debe ser de 2.4 metros.

-ACABADO DEL PISO FALSO

Se recomienda que el acabado del piso de la sala de cómputo sea hecho con plástico laminado tipo de piso previene que la base del equipo se ponga en contacto de baja resistencia eléctrica con cualquier superficie metálica del edificio, proporcionando seguridad al personal que trabaja circuitos eléctricamente energizados.

También proporciona una superficie de fácil limpieza con un trapo húmedo o con aspiradora.

Tambien recomienda no usar alfombras de ningún tipo en la sala de cómputo.

Después de la identificación de riesgos sobre el lugar del centro de cómputo , es útil tener una secuencia en orden en el cual se revise una serie de soluciones a la protección del lugar del centro de cómputo.

-ABERTURAS

Las medidas y cantidades de las aberturas necesarias para el pasaje de cables serían suministradas al cliente cuando se cuente con el layout definitivo de ubicación de los equipos.

-REMOCIÓN DE LOS PANELES

Los paneles del piso elevado deben poder ser removidos fácilmente para permitir la instalación del cableado del sistema.

3.4.2. INFRAESTRUCTURA AMBIENTAL

Son aquellos controles que proveen confiabilidad, integridad, protección al centro de cómputo. Estos controles reducen el riesgo de condiciones adversas al negocio por mal funcionamiento, falla, o error por los humanos como son los tratos o convenios naturales hacia la instalación de la computadora. Aspectos clave en la revisión (auditoria) a los controles ambientales incluyen los siguientes:

1. Debilidades o exposiciones ambientales.
2. Controles ambientales.

1.EXPOSICIONES AMBIENTALES

Las exposiciones ambientales son primeramente para los eventos que ocurren naturalmente. Sin embargo, con controles apropiados, la exposición a estos elementos pueden ser reducidos.

-FUEGO

El fuego puede ser empezado dentro o fuera del lugar de procesamiento de la información. Sin embargo, los controles para incendio deben existir a través de la oficina para proveer una adecuada protección.

-TERREMOTO

Deben también ser consideradas en áreas no propensas a los temblores.

-TORNADO

-HURACANES

-TORMENTAS SEVERAS

-INUNDACIÓN

-FALLAS ELÉCTRICAS

-PICOS DE CORRIENTE

-FALLA DEL AIRE ACONDICIONADO

-PÉRDIDA DE ENERGÍA ELÉCTRICA

-FALLA DEL EQUIPO

-DAÑO POR AGUA

Aún con lugares localizados en pisos altos, el daño por agua, es un riesgo, típicamente esto ocurre por una ruptura de pipas de agua.

2. CONTROLES AMBIENTALES

Los controles ambientales reducen el riesgo de una interrupción de la actividad de la organización, alrededor de eventos adversos que la afectan. Estos alrededores incluyen la calidad del aire, la energía eléctrica, condiciones de tierra y atmosféricas.

Algunos ejemplos de controles ambientales son los siguientes:

-DETECTORES DE AGUA

En el cuarto de la computadora, los detectores de agua deben estar localizados debajo del piso falso y cerca de los agujeros del drenaje, aún si el cuarto de cómputo está sobre un piso alto(recuerde las fugas de agua). Cualquier lugar de almacenamiento de equipo sin atender debe tener también detectores de agua. Esta alarma no sólo protege al equipo, sino también al personal de un shock eléctrico. Cuando se activan, los detectores deben producir una alarma audible que puede ser escuchada por el personal de seguridad y el

personal de control. La localización de detectores de agua debe estar marcada en el piso falso del cuarto de cómputo para un fácil acceso.

-EXTINGUIDORES PORTÁTILES

Los extinguidores deben estar en lugares estratégicos por todo el centro de cómputo. Estos deben estar etiquetados para una inspección y luego estar inspeccionados anualmente. Ellos deben también estar identificados para extinguir cualquier clase de incendio.

-ALARMAS DE INCENDIO MANUALES

Alarmas contra incendio manuales, deben estar en lugares estratégicos por todo el centro de cómputo. El resultado deberá ser una alarma audible y debe estar ligada a una estación central de vigilancia que regularmente esta monitoreando.

-DETECTORES DE HUMO

Los detectores de humo deben estar sobre y debajo de los paneles del techo por todo el centro de cómputo, y debajo del piso falso del centro de cómputo. Los detectores deben producir una alarma audible cuando es activada y debe estar conectado a una estación de guardia central que esté regularmente monitoreando (preferentemente el departamento de bomberos). La localización de detectores de humo sobre el techo y debajo del piso falso debe estar marcado sobre el plafón del techo y por encima del piso falso para un fácil acreso.

Los detectores de humo deben complementar, no reemplazar al sistema de supresión del fuego.

-SISTEMA DE SUPRESIÓN DE FUEGO

El sistema de supresión de fuego esta diseñado para activar automáticamente e inmediatamente después de la detección de un calor intenso típicamente generado por el fuego. como detectores de humo, el sistema debe producir una alarma audible. Cuando sea activada y debe ir unida a una estación de guardia central que es regularmente monitoreada. El sistema debe ser ademas inspeccionado y probado anualmente. Los intervalos de prueba deben cumplir con la industria y los estándares y guías de la compañía de seguros.

Idealmente, el sistema debe activar automáticamente, otros mecanismos para localizar el fuego. Esto incluye cerrar puertas contra incendios, notificar al departamento de bomberos, cerrar los conductos de ventilacion, y apagar el equipo eléctrico no esencial. a esto le sumamos, que el sistema debe estar segmentado, así el fuego en centro de cómputo no active el sistema entero

El medio para suprimir el fuego varia, pero usualmente es uno de los siguientes:

-AGUA
Sistemas basados en agua son típicamente referidos a sistemas de dispersadores de agua. Estos sistemas son efectivos pero también no son muy populares porque dañan el equipo y la propiedad. El sistema puede ser almacenada en una pipa de agua, y el agua saldrá sólo cuando el sistema haya sido activado. Un sistema de cargado es más realizable, pero tiene la desventaja de exponer el centro de cómputo, si alguna de las pipas se rompe y provoca una fuga.

-HALON 1301

El sistema de halon, libera gases comprimidos que quitan el oxigeno del aire, y por ende apaga el fuego. El gas halon es muy popular porque no daña el equipo como el agua. Debe haber una alarma audible y una pequeña demora o retraso antes que se riegue el gas, para permitir al personal evacuar el área, y para desconectar el sistema. Sin embargo su efecto adverso es que afecta la capa de ozono, las investigaciones siguen para encontrar un sistema alternativo.

-LOCALIZACIÓN ESTRATÉGICA DEL CUARTO DE CÓMPUTO

Para reducir el riesgo de inundación, el centro de cómputo no debe ser localizado en el sótano. Si se localiza en un edificio de muchos pisos, estudios demuestran que la mejor localización de un centro de cómputo para reducir el riesgo de fuego, humo y daños por agua es el piso 3,4,5, o 6.

-INSPECCIONES REGULARES POR EL DEPARTAMENTO DE BOMBEROS

Para asegurarse que todos los sistemas de detección de fuego, cumplen con los códigos del edificio, el departamento de bomberos deben inspeccionar el sistema y el lugar del centro de cómputo anualmente. También el departamento de bomberos debe notificar de la localización del centro de cómputo así, en caso de un incendio, ellos pueden estar preparados con equipo apropiado para incendios por fallas eléctricas.

-PAREDES A PRUEBA DE FUEGO, PISOS Y TECHOS QUE RODEAN AL CENTRO DE CÓMPUTO

Las paredes alrededor del centro de cómputo deben contener o bloquear al fuego que se disipe. Las paredes alrededor deben tener al menos una resistencia de 2-4 horas contra el fuego.

- ALARMAS CONTRA EL FUEGO

Alarmas automáticas contra el fuego ofrecen la mejor protección en contra del fuego, porque el fuego es detectado aún si no hay nadie en la premisa. Muchas instalaciones de computadoras están abiertas las 24 horas del día, siete días de la semana, la cual suma protección en contra del fuego u otros tipos de desastre.

Detectores de humo son uno de los mejores dispositivos de alarma contra incendios. Este debe ser puesto en todos los cuartos y en particiones cerradas como son: los pisos falsos y los conductos de aire. Idealmente, las alarmas pueden ser conectadas al departamento de bomberos local, todo esto sumado a los servicios de una guardia. Todas las alarmas de fuego deben dar una alarma audible indicando un incendio y si el centro de cómputo no está siempre ocupado la alarma debe transmitir a una localización supervisada constantemente.

Es deseable contar con equipo automático de detección de fuego en el lugar . En E.U. el consejo federal de fuego recomienda el tipo de producto de combustión ionización. También se debe tener consideración con las corrientes de aire y patrones dentro del espacio, áreas debajo del piso falso, espacio dentro del techo falso, los cables y los conductos de aire conectados directamente al equipo.

-EQUIPO PARA COMBATIR EL FUEGO

Se debe tener cuidado con el equipo contra incendios y los extinguidores automáticos.

El agua no siempre es lo mejor para usarse con el equipo técnico. Usualmente el agua es solo el último recurso, pues se utiliza sólo si el fuego esta fuera de control.

El Dióxido de carbono y el Bromoclorodifluorometano (BCF) son dos agentes que pueden ser usados para incendios en el centro de cómputo. Ambos son disponibles para sistemas automáticos y extinguidores portables. Un artículo Británico, sin embargo, previene que el dióxido de carbono tiene desventaja, por ser tóxico. Su uso es cuestionable desde una descarga accidental o un incendio real puede activar el sistema automático. Esto ha pasado y ha habido gente muerta por su uso.(Fire Protection System, W.A. Jacksons).
Un equipo de dispersador automático provee en primera línea de defensa en contra de un incendio en serio. Cada sistema de dispersador automático debe proveer transmisión local y automática activando las alarmas de flujo de agua. Este sistema de preferencia debe ser valuado independientemente de otros sistemas de dispersador. El propósito de este tipo de protección es el de limitar y controlar incidentes mayores con el fuego y previenen una destrucción total de un sistema electrónico. Esto sirve para prevenirnos de un incidente mayor cuyo progreso está más allá de nuestro control o de desarrollarse en un mayor desastre convirtiéndose en una destrucción total de todo el equipo en el área.

Es importante apagar primero la energía eléctrica, antes de activar los dispersadores de agua.

Para minimizar el daño del equipo electrónico con los dispersadores, éstos deben estar en áreas protegidas.

En algunos centros de cómputo los cuales están bajo la supervisión de un operador u otra persona familiar con el equipo, la tardanza normal entre el incendio inicial y el sistema del dispersador, proveerán un tiempo adecuado para que el operador pueda apagar toda la energía, utilizando los switches de apagado de emergencia.

Mientras que el agua puede ser el último método alrededor del equipo eléctrico, todavía es utilizado para extinguir incendios convencionales. Si un empleado angustiado y frenético esparce agua por todos lados, apagando un pequeño incendio puede causar mas daño que el fuego original.

Si el agua es usada en otra parte del edificio o en un piso de arriba para apagar el fuego puede causar un daño extensivo en un centro de cómputo. Por esta razón, las paredes y los pisos deben ser aprueba de agua así como resistentes al fuego. El piso de arriba del centro de cómputo debe estar hecho contra agua y las puertas deben ser protegidas igual.

El piso falso que es común en el centro de cómputo ofrece alguna protección en contra de un daño del agua. Una precaución adicional es que la estructura de los pisos subordinado al piso falso de los cuartos de cómputo debe tener un drenaje positivo. Esto permitirá un rápido desagüe que puede acumular, ya sea por un accidente o por un sistema de dispersador de agua para combatir el fuego. El drenaje ayuda a prevenir una inundación por causas naturales o algo como explosión de mantenimiento de agua. Si el equipo electrónico o las especiales consideraciones se deben tener en cuenta, para proteger el equipo de agua que tiende a correr a la porción más baja del edificio como un resultado de la lucha contra el fuego o por inundación.

-LOCALIZACIÓN Y USO DE LOS EXTINGUIDORES DE FUEGO

El mejor extinguidor , no será disponible a menos que el empleado sepa como usarlo y localizarlo. todos los empleados deben por lo menos leer la etiqueta del extinguidor, y es recomendable que traten de operarlo por lo menos una vez.

Los extinguidores de fuego de dióxido de carbono, debe ser prominentemente localizado; Así que el extinguidor no debe estar lejos, debe estar por lo menos 150 mts de camino y el extinguidor de por lo menos 6.5 kgs.

Son muy importantes los trípticos o folletos de instrucciones de como usar los extinguidores, en caso de emergencia.

-PROTECCIÓN DEL ALMACÉN

Debe haber un cuarto de almacenamiento para cintas, discos y tarjetas de archivos. Estas cosas no deben ser dejados afuera del cuarto de la computadora. El cuarto de almacenamiento debe estar en un cuarto separado. El almacén de suplementos o materiales de oficinas, formas y otro material combustible en el área de la computadora o en el área de almacenamiento debe ser retirada.

Las cintas magnéticas y discos deben ser almacenados en un área no combustible. Materiales no combustibles deben estar almacenados en el vecindario. Para una protección máxima, las cintas y los discos pueden ser almacenados en una bóveda a prueba de fuego, que también sea capaz de mantener una temperatura interna deseable y una humedad relativa por un tiempo razonable. Los estantes de metal deben ser usados para sostener las cintas.

En los contendores de las cintas, se encuentra un grave peligro, ya que éstos son de plástico o polietileno altamente combustible, este riesgo es generalmente pasado por alto.

-PROTECTORES ELÉCTRICOS DE SOBRECARGA

Estos dispositivos eléctricos reducen el riesgo de daño al equipo debido a los picos de corriente. Tales protectores son típicamente construidos dentro de un sistema de abastecimiento de energía ininterrumpido (UPS UNINTERRUPTIBLE POWER SUPPLY SYSTEM).

-SISTEMA ININTERRUMPIDO DE ABASTECIMIENTO DE CORRIENTE(UPS)

Un sistema UPS consiste en un generador, ya sea de batería o de gas, que hace interface entre la energía eléctrica y el dispositivo de entrada de energía eléctrica a la computadora. lo que hace es dar una consistencia a la corriente eléctrica que hace funcionar a la computadora en caso de haber una falla en el abastecimiento de energía eléctrica. El UPS provee de energía eléctrica a la computadora por cierto período de tiempo; Dependiendo de lo sofisticado que sea el UPS, la corriente eléctrica proveniente del UPS puede ser de días o de algunos minutos que permitan respaldar.

-SWITCH DE APAGADO EN CASO DE EMERGENCIAS

Talvez exista en algún momento la necesidad de apagar la computadora y sus dispositivos periféricos en caso de que el cuarto donde se encuentre la computadora se esté incendiando o si hubiera evacuación. Dos switches de emergencia servirían para este propósito, uno dentro del cuarto de máquinas y el otro cerca, pero afuera del cuarto. Deben ser claramente identificados con un letrero, deben ser accesibles e inclusive a salvo de gente que no tiene autorización para utilizarlo. Los switches deben estar bien protegidos de una activación accidental.

-TENER DOS DIFERENTES ESTACIONES DE ABASTECIMIENTO DE ENERGÍA ELÉCTRICA

El cableado de energía eléctrica que alimentan a nuestro centro de cómputo están expuestos al medio ambiente- agua, fuego, excavaciones etc.-. Para reducir el riesgo de falta de energía eléctrica lo que se debe hacer es abastecerse de energía eléctrica no solo de una estación de electricidad sino de dos. Así si falla una por lo menos nos queda la otra estación de electricidad funcionando.

-LOS CABLES DEBEN ESTAR DENTRO DE LOS PANELES Y CANALES ELÉCTRICOS

Incendios por causas de la electricidad son siempre un riesgo. para reducir el riesgo, los cables deben ser puestos en paneles y canales resistentes al fuego. Estos canales y paneles generalmente dan origen al piso falso del cuarto de la computadora no inflamable; Así como los cables debajo del piso.

-REALIZAR PROHIBICIONES EN CONTRA DE FUMAR, TOMAR O COMER ALIMENTOS DENTRO DEL CENTRO DE CÓMPUTO

La comida, el tabaco y los líquidos pueden ocasionar incendios o daño al equipo delicado(especialmente en el caso de líquidos). estas prohibiciones deben estar claramente señaladas a la entrada del centro.

-LOS MATERIALES DE LA OFICINA NO DEBEN SER FLAMABLES

Los basureros, cortinas, escritorios, gabinetes y otros materiales que se encuentren dentro del centro de cómputo deben ser contra incendios de material no flamable.

-PLANES DE EVACUACIÓN DEL CENTRO DEBEN ESTAR PLENAMENTE PROBADOS Y DOCUMENTADOS

Los planes de evacuación son importantes para la seguridad humana, sin embargo este plan no debe descuidar la atención que se le debe al centro de procesamiento de la información.

-SISTEMA DE DISTRIBUCIÓN ELÉCTRICA

Se recomienda que el sistema sea conectado a una única fuente de poder. EL alimentador principal y los conductores de tierra, deberán ser aislados y exclusivos para el sistema. Circuitos ramificados para iluminación, sistemas de aire, etc. no deberán estar conectados a los tableros de potencia utilizados por el sistema.

-TABLEROS DE DISTRIBUCIÓN ELÉCTRICA

La organización debe proveer a la empresa a la cual le compró el equipo de cómputo, de un tablero de distribución, el que deberá contar con un interruptor general, voltímetro, amperímetro, frecuentímetro y un interruptor individual por cada una de las unidades que configuren en el sistema. El tablero debe ubicarse en un lugar accesible y cada interruptor debe estar debidamente rotulado para su fácil localización. Si más de un tablero es usado, ellos deben estar localizados adyacentes uno del otro, con los conductores de tierra y potencia de entrada conectados a la misma fuente. Este tablero debe contener una barra sólida de tierra que no esté conectada a la línea de neutro y aislada de la cubierta de metal. Todos los requerimientos de potencias deben estar basados en cargas del 150%.

-APAGADO DE EMERGENCIA

Seria conveniente proveer un medio de desconectar toda la potencia del sistema y apagar todos los ventiladores del sistema de aire acondicionado sin afectar la iluminación de la Sala de cómputo en caso de emergencia.

Este medio de desconexión deberá estar localizado cerca de cada una de las salidas de la Sala de Cómputo y en lugares fácilmente accesibles al operador.

-TRANSITORIOS Y TOLERANCIAS

Los transitorios en una línea pueden ser causados por el encendido o apagado de máquinas eléctricas, tales como motores, ascensores, equipos de soldádura, sistemas de aire acondicionado, etc. Aún el flujo de corriente de un sistema de iluminación puede producir "picos de ruido" que podrían exceder el nivel de transitorios aceptables para alguna unidad del sistema, por lo cual es altamente recomendable que la entrada de potencia del sistema esté completamente aislada de cualquier carga eléctrica. En zonas grandes, cargas eléctricas industriales o condiciones de entrada de potencia marginales, pueden ser necesarias aislaciones adicionales para prevenir transitorios en el sistema.

El diseño de las unidades de un sistema y sus periféricos permite la tolerancia de la mayoría de los transitorios y variaciones lentas de voltaje y frecuencia que son normalmente encontradas en las líneas de suministro eléctrico;sin embargo hay límites para tales disturbios mas allá de los cuales se incrementa la probabilidad de errores (pérdida o ganancia de información), siendo este inaceptable.

Mayores disturbios incrementarán la probabilidad de interrupción de la operación del sistema por la activación de uno o más de los dispositivos protectores. Estos dispositivos incluyen interruptores de circuito, fusibles sensores de alto y de bajo voltaje y protectores térmicos de sobrecarga. Estos han sido diseñados para limitar los daños que pueden ocasionar en las unidades del sistema los disturbios tanto internos como externos, pero ellos no impiden completamente la posibilidad de un trabajo anormal en los componentes.

Si las variaciones y transitorios de la línea ocasionalmente exceden los niveles aceptables para el sistema, el cliente tienen la opción de proveer un equipo de potencia adicional para evitar estos disturbios o correr el riesgo de frecuentes problemas en el sistema. La selección del equipo de potencia adicional dependería de la naturaleza de los disturbios a ser limitados e irían de un simple filtro de línea a un generador de corriente alterna, a un equipo de corriente ininterrumpida.

-CONEXIÓN A TIERRA

El cliente deberá poner especial énfasis en la provisión de un sistema de tierra efectivo y seguro.

-CONDUCTORES DE TIERRA AL EQUIPO

Los conductores de tierra a todas las máquinas deberán estar aislados y terminados para mostrar un color verde o un color verde continuo con una o mas rayas amarillas, ellos serán instalados como una parte de los cables que vienen del tablero de distribución.

-INSPECCIÓN DE INCENDIOS

La primera precaución es la mas obvia y es generalmente desarrollada gratis por el departamento de bomberos. Pregunte al departamento de bomberos que venga e inspeccione el cuarto de la computadora y el almacén para revisarlo de problemas de fuego. Ojos expertos pueden apuntar algunos inconvenientes individuales y condiciones que ningún artículo de ninguna revista o libro puede encontrar.

Otra fuente de prevención contra incendios, es pedir una inspección al negocio a la firma que vende alarmas contra fuego, extinguidores y materiales de edificio a prueba de fuego. Estas compañías usualmente están

contentas de mandar a un vendedor a checar la seguridad contra el fuego y revise los pequeños detalles y sugiera sus productos para prevenir los incendios.

-SISTEMA DE TEMPERATURA Y

Los equipos de procesamiento de datos, necesitan de un sistema de aire acondicionado diseñado para operación constante, en base a los siguientes parámetros:

1. DISIPACIÓN TÉRMICA(BTU)
2. MOVIMIENTO DE AIRE(CFM)
3. ILUMINACIÓN
4. PÉRDIDAS POR TRANSFERENCIAS DE CALOR
5. VENTILACIÓN E INFILTRACIÓN.
6. PÉRDIDAS DE CALOR DEBIDO AL SISTEMA HUMIDIFICADOR
7. CONDICIONES AMBIENTALES.
8. INSTRUMENTOS REGISTRADORES DE TEMPERATURA Y HUMEDAD.

1. DISIPACIÓN TÉRMICA
La disipación térmica de cada unidad de sistemas es mostrado en Unidades Térmicas Británicas por hora.

2. MOVIMIENTOS DE AIRE
Dicho movimiento es mostrado en pies cúbicos por minuto.

3. ILUMINACIÓN
Los BTU por hora disipados por la iluminación del local deben ser incluidos en los cálculos de carga total de calor. Si la iluminación es seccionada, este cálculo debe ser hecho como si todas las luces estuvieran encendidas al mismo tiempo.
4. PÉRDIDAS POR TRANSFERENCIA DE CALOR

Están afectadas por lo siguiente:

- Pérdidas a través de paredes, piso y techo
- Diferencias en temperatura entre la sala de cómputo y áreas adyacentes.
- Ventanas expuestas a los rayos del sol.

Los cambios de temperatura durante la operación de la computadora deben ser minimizados. La variación cíclica de temperatura sobre el rango completo de operación no debe realizarse en menos de 8 horas.

Los cambios de humedad de un extremo a otro del rango de operación no debe realizarse en menos de 4 horas.

5. VENTILACIÓN E INFILTRACIÓN

El método y tipo de construcción de la Sala de cómputo tiene un efecto definido en el comportamiento de un sistema de aire acondicionado y consecuentemente en la ambientación a ser mantenida en ese lugar.
Esto es particularmente cierto cuando se trata de mantener la humedad relativa del espacio dentro de las tolerancias especificadas.

Si se permite la infiltración de grandes volúmenes de aire frío (por debajo de 15 grados centígrados), o se introducen intencionalmente, el sistema de aire acondicionado debería tener los medios de agregar la humedad adicional al espacio. El comportamiento de un sistema de procesamiento de datos es afectado cuando la humedad se sale de la especificada.

Los requerimientos de ventilación deben ser basados en 15 CFM por persona (ocupación constante), incluyendo cualquier infiltración adicional permitida que pueda ser requerida. Todo aire producido debe introducirse en la computadora pasando primero através de una unidad de filtros.

Se recomienda que la presión de aire en la Sala de Cómputo sea ligeramente superior que la de áreas adyacentes, para reducir así la entrada de polvo y suciedad.

Los grandes ventanales exteriores son la mayor fuente de pérdida o ganancia de calor a no ser que se usen dos cristales separados por el aire.

Luz de sol directa através de ventanas al exterior incrementaran significativamente la carga de calor al sistema de aire acondicionado.

6. PÉRDIDAS DEL CALOR DEBIDO AL SISTEMA HUMIDIFICADOR

La introducción de vapor de agua en un sistema de aire acondicionado remueve el calor del aire. Recíprocamente, el remover excesos de humedad del aire requiere enfriamiento adicional. Las variaciones de temperatura por pérdidas y ganancias debidas al control de humidificación deben ser consideradas al calcular el sistema de aire acondicionado.

7. CONDICIONES AMBIENTALES

Las condiciones ambientales para los sistemas de las computadoras, deben ser mantenidas entre 20 y 24 grados centígrados con una humedad relativa de 45 a 55 porciento, mientras están operando. La temperatura ideal recomendada para la Sala de Cómputo es de 22 grados Centígrados y esta debe ser usada como la base para el diseño del sistema acondicionado.

El criterio de diseño de los controles de acondicionamiento de aire para la sala de cómputo debe ser especificado de la siguiente manera:

1. Temperatura	22 grados C.
2. Variaciones de temp.	+-2 grados C.
3. Humedad relativa	50 %
4. Variaciones de Humedad relativa	+-5%

En el centro de cómputo de Bancomer, donde se encuentra la IBM 3090 se llevan acabo los siguientes estándares en materia de condiciones ambientales:

1. Temperatura	20 grados C.
2. Humedad	55% a 60%.

Aquí no llevan por el momento, un sistema sofisticado de alarma, en caso de que se sucediera una contingencia. Disponen de un tablero en donde :

Foquito amarillo indica 20 grados C.
Foquito verde indica 23 grados C.
Foquito rojo indica 25 grados C.

Este sistema les ha funcionado por mucho tiempo, sin embargo pronto lo van a reemplazar por otro más moderno y confiable.

La humedad relativa de la Sala de Cómputo debe ser mantenida entre 45 y 55%. Para mantener estos requerimientos, la humedad debe ser agregada o quitada al sistema de aire acondicionado. Generalmente, la humedad debe ser agregada ya que al enfriar el aire se remueve la mayoría del vapor de agua por condensación.

8. INSTRUMENTOS REGISTRADORES DE TEMPERATURA Y HUMEDAD

Se recomienda que se instalen instrumentos registradores de temperatura y humedad. Dichos instrumentos son necesarios para proveer un continuo registro de las condiciones ambientales en el área del equipo.

TEMPERATURA	HUMEDAD
En operación:	
68 a 78 grados F(20 a 25 grados C) (máximo 86 grados F(30 grados C) (mínimo 55 grados F(15 grados C)	40 a 60%
No operando:	
(máximo 167 grados F (75 grados C) (mínimo -40 grados F (-40 grados C)	5 a 80%

3.4.3 INFRAESTRUCTURA LÓGICA

La infraestructura lógica se refiere a todos los controles de acceso lógico. En esta área de seguridad se tiene que analizar y evaluar las políticas, estructuras organizacionales, procedimientos operativos, y controles de acceso utilizados para proteger el software de la computadora y los archivos de información de una divulgación no autorizada, manipulación o destrucción.

Se deben realizar tareas como las siguientes para evaluar este tipo de controles:

1. Evaluación de controles sobre las trayectorias de los accesos potenciales dentro del sistema, para fijar suficiencia, eficiencia y efectividad, revisando los rasgos distintivos apropiados de la seguridad del software y hardware; e identificando cualquier deficiencia o redundancia.

2. Probando los controles sobre las trayectorias de acceso para determinar su funcionamiento y efectividad, aplicando técnicas apropiadas de auditoria.

3. Evaluando el ambiente de acceso de control para determinar que el objetivo del control sean logrados, analizando el resultado de las pruebas y otra evidencia de auditoria.

TRAYECTORIAS DE ACCESO LÓGICO

El acceso lógico dentro de una computadora puede ser realizado através de muchas alternativas de seguridad de acceso. Estos métodos de acceso incluyen lo siguiente:

1. Operador de la consola.

Estas terminales de la computadora privilegiadas,.controlan la mayoría de las operaciones y funciones de la computadora. Para proveer seguridad, estas terminales deben estar localizadas en el cuarto de la computadora adecuadamente controlado, así el acceso físico solo puede ser llevado a cabo por operadores de la computadora y el personal de soporte.

2. Terminales ON-LINE

Esta manera de acceso lógico es el más popular con los usuarios. Este requiere típicamente una entrada de un LOGON ID de identificación y un password para poder accesar a la computadora. El acceso ON-LINE puede ser para llevar a cabo una entrada de un transacción, consulta de un archivo, y una actualización de un archivo (añadir, cambiar, borrar). Desde que el acceso es inmediato; la necesidad para iniciar una seguridad lógica sobre este acceso debe ser inmediato también. Estos controles son logrados con la utilización de un software de control de acceso.

3. Procesamiento BATCH

Esta manera de acceso es indirecta desde que el acceso es logrado vía procesamiento de transacciones. Esto generalmente involucra la acumulación de transacciones de entradas y procesarlas en batch solo después de un intervalo de tiempo o después de un cierto número de transacciones que han sido acumuladas. La seguridad es lograda restringiendo quién puede acumular las transacciones(data entry clerks) y quién puede iniciar el proceso batch(operadores de la computadora, o el sistema automático de calendarización de jobs).

4. Puertos remotos (Dial-Up Ports)

El uso de puertos remotos involucran enganchar una terminal remota a una línea de teléfono y logrando el acceso a una computadora marcando un número de teléfono especial, que esta directa o indirectamente conectado a la computadora. A menudo un módem debe ser la interface entre una terminal remota y una línea de teléfono para codificar y decodificar las transmisiones. La seguridad es lograda proveyendo una forma de identificación de un usuario remoto para determinar una autorización al acceso. Esta puede ser "Dial-back line" una línea para la utilización de un LOGON ID y un software de control de acceso involucrando a un operador de computadora para verificar la identidad del que llama y luego proveer la conexión hacia la computadora.

5. Redes de telecomunicación

Las redes de telecomunicación unen un número de terminales a la computadora principal, através de una líneas de redes de telecomunicaciones. Las líneas de telecomunicaciones pueden ser privadas, por ejemplo, dedicadas a un usuario o al público, tal como TELMEX que es el sistema nacional de teléfonos. La seguridad debe ser proveída de la misma manera como es aplicada en las terminales ON-LINE.

BENEFICIOS Y DEBILIDADES DEL ACCESO LÓGICO

Los controles de acceso lógicos adecuados incrementan el potencial de la organización para pérdidas resultantes de exposiciones o debilidades técnicas y de negocios. Estas exposiciones pueden resultar en inconvenientes menores o un completo cierre de las funciones de la organización.

PERPETRADORES DE VIOLACIONES DE ACCESO LÓGICO

Los infractores del acceso lógico son comúnmente la misma gente, que pueden llegar a realizar violaciones a los controles físicos, a pesar de las habilidades requeridas para realizar algo no autorizado a las debilidades lógicas, que son mas técnicas y mas complejas.

- HACKERS

Los hackers típicos están tratando de probar los límites de las restricciones de acceso para probar su habilidad de superar obstáculos. Ellos usualmente no van con la intención de destrucción, pero muy frecuentemente este es el resultado.

- EMPLEADOS (AUTORIZADOS Y NO AUTORIZADOS)

1. Personal del IS

Esta gente tiene el acceso a lo más importante de la información de la computadora desde que son los guardianes de esta información. Además de los controles de acceso lógico, una buena segregación de deberes y la supervisión ayuda a controlar a esta gente.

2. Usuarios finales

Particularmente este prevenido de los empleados que se han ido bajo términos no muy favorables.

- GENTE DE AFUERA INTERESADA Y CAPACITADA

- Competidores
- De países extranjeros
- Del crimen organizado

- EL IGNORANTE ACCIDENTAL

Alguien que sin saberlo comete una violación al acceso

EXPOSICIONES DE ACCESO LÓGICO

Las exposiciones que existen de un acceso no autorizado accidental o intencional a una debilidad del control de acceso lógico incluyen los siguientes:

1.EXPOSICIONES TÉCNICAS

- NO AUTORIZADAS INTENCIONAL O SIN INTENCIÓN IMPLEMENTACION O MODIFICACIÓN DE INFORMACIÓN Y SOFTWARE

Estas exposiciones incluyen un código escondido en el programa y modificaciones directas o indirectas de la información y los programas. Hay muchos nombres para esta clase de exposiciones, incluyendo las siguientes:

1. Modificación de la información.

Esto se refiere al cambio de información dentro de la computadora. Esto es el abuso más común, porque éste requiere un conocimiento técnico limitado y ocurre antes de que la seguridad de la computadora pueda proteger la información.

2. Caballo de Troya.

Esto es el esconder un código maliciosamente en un "programa autorizado" dentro de la computadora. Este código escondido será ejecutado cuando el programa autorizado es ejecutado. Un ejemplo clásico del Caballo de Troya en el programa de cálculo de nómina que toma un centavo de cada cheque y lo acredita a la cuanta del perpetrador.

3. Redondeando abajo.

Esto es el quitar pequeñas cantidades de dinero de un transacción computacional o de una cuenta; y canalizando esta cantidad a la cuenta del perpetrador. El término cuenta abajo o redondeando abajo se refiere a redondear fracciones de un centavo abajo y transfiriendo estas pequeñas fracciones en una cuenta no autorizada. Desde que estas cantidades son tan pequeñas; raramente son notadas.

4. Técnica del salami.

Esta técnica es similar a la técnica del redondeo, pero se refiere a quitar pequeñas cantidades de dinero de una transacción computacional o una cuenta.

5. Virus.

Los virus de la computadora son programas maliciosos los cuales pueden duplicarse y dispersarse de computadora a computadora, a través de compartir diskettes o a través de transferir lógica sobre las líneas de telecomunicaciones. Un virus puede desplegar inofensivos mensajes sobre las terminales de la computadora, o peligrosamente borrar o alterar archivos de cómputo o llenar la memoria de la computadora con basura hacia un punto de la computadora que no podrá funcionar más. Un peligro más, es el virus que puede permanecer "dormido" por algún tiempo hasta que es activado por cierto evento o aún siendo copiado un determinado número de veces. Sin embargo, durante este tiempo el virus se ha esparcido silenciosamente.

6. Bomba Lógica.

Las bombas lógicas son similares a los virus de computadoras, pero no se multiplican.

7. Puertas de trampa.

Las puertas de trampa son salidas o puertas de salida. Un programa autorizado que permite la inserción de una lógica para permitir una revisión de la información durante la mitad del procesamiento. Estos agujeros también permiten la inserción de una lógica no autorizada.

8. Ataque asyncrono.

En un ambiente del multiprocesamiento, la información se mueve a través de una línea de telecomunicaciones asíncronamente (en una dirección o en otra). Como resultado, numerosas transmisiones de información deben esperar por una línea que sea liberada y llevar el flujo en la dirección apropiada antes de ser transmitida.

Esta información que está esperando es susceptible de un acceso no autorizado llamado ataque asincrono. Esto es muy complejo y se necesitará del administrador de la red y la asistencia del analista del software del sistema para evaluar.

9. Fuga de información.

La fuga de información se refiere a la información afuera de la computadora. Esto se refiere a tirar los archivos de los discos ha papel, o ser tan simple como robar los reportes de la computadora y cintas.

10. Intervención del cable.

Esta técnica involucra el escuchar a escondidas sobre información siendo transmitida sobre las líneas de telecomunicación.

11. Piggy backing.

Este proceso puede no ser técnico, consiste en seguir a una persona autorizada a través de una puerta de seguridad; esta técnica sirve para interceptar y posiblemente alterar transmisiones en líneas autorizadas de telecomunicaciones en la computadora.

- PARAR COMPLETAMENTE LA COMPUTADORA(SHOT DOWN THE COMPUTER)

A través de una forma directa (ON-LINE) o indirecta (líneas de teléfono) de conexiones a terminales, un paro de la computadora puede ocurrir . Esto frecuentemente requiere un acceso a la seguridad apropiado, ya que no son envueltos alrededor de logon id's y conexiones de telecomunicaciones dentro de la computadora.

- INTERRUPCIÓN DEL SERVICIO

Las líneas de telecomunicaciones son vulnerables de una interferencia o de un corte.

2. EXPOSICIONES DE LA ORGANIZACIÓN.

La aplicación de crímenes para accesar a la computadora y la información que contiene puede ser dañino para la reputación, la moral y la existencia de una organización.

.Pérdidas de Clientes, enredos de la administración, y acciones legales en contra de la organización puede ser el resultado. Muchos de estos tratos para los negocios incluyen los siguientes:

- PÉRDIDA FINANCIERA

Estas pérdidas pueden ser directas, a través de pérdidas de fondos electrónicos, o indirectas, a través de costos de corrección de exposiciones.

- REPERCUSIONES LEGALES

Hay numerosos derechos por ley de privacidad y derechos humanos; los cuales la organización debe considerar durante el desarrollo de las políticas y procedimientos de seguridad. Estas leyes pueden proteger

la organización, pero pueden también proteger al perpetrador de la prosecución. Sumado a esto, sin tener medidas de seguridad apropiadas puede exponer a la organización a litigios o pleitos legales de sus inversionistas y aseguradores, puede ocurrir una pérdida significativa de una violación a la seguridad. Se debe obtener asistencia legal cuando se revise los puntos asociados con la seguridad de la computadora.

- PÉRDIDA DE LA CREDIBILIDAD O COMPETITIVIDAD DE PUNTA

Muchas organizaciones especialmente firmas de servicio como los bancos, caja de ahorro y préstamos, y firmas de inversión, necesitan buena credibilidad y público confiado para mantenerse en una competitividad de punta o aún para permanecer en el negocio. Una violación a la seguridad puede dañar severamente esta credibilidad, resultando en pérdida de negocio y prestigio.

- EXTORSIÓN/ESPIONAJE INDUSTRIAL

Accesando a información confidencial o a las operaciones de la computadora de impacto adverso, un perpetrador puede extorsionar o exigir un pago o servicios de una organización, tratando de accesar violando la seguridad.

- DIVULGACIÓN DE INFORMACIÓN CONFIDENCIAL, IMPORTANTE Y EMBARAZOSA.

Como se dice arriba, tales eventos pueden dañar la credibilidad de la organización y esto es la conducción del negocio. Acciones legales o regulatorias en contra de la compañía que realizó la divulgación pueden resultar también.

- SABOTAJE

Algunos perpetradores no están buscando una ganancia financiera. Ellos solamente quieren hacer daño. Esto puede ser porque al perpetrador no le gusta la organización o solo quiere un reto para probarse así mismo.

CONTROLES DE ACCESO LÓGICO

Los archivos de la computadora deben ser protegidos de acceso innecesario o acceso no autorizado mediante controles que reducen el riesgo de un mal uso intencional o sin intención, robo, alteración o destrucción. En un ambiente de procesamiento batch, este control puede ser provisto mediante la restricción y monitoreo de las actividades del operador de la computadora. En un sistema ON LINE, las trayectorias de acceso son más complejas y directas, y el nivel de control correspondientemente más complejo. Estos controles de acceso necesitan ser aplicados no sólo a los operadores de la computadora, sino también a los usuarios finales, programadores, administradores de la seguridad, administración y cualquiera que pueda usar la computadora (incluyendo a las personas externas).

ARCHIVOS COMPUTACIONALES Y LUGARES PARA PROTEGER MEDIANTE CONTROLES DE ACCESO LÓGICO

1.Información.
2.Software de aplicación
-Prueba
-Producción
3.Utilerías.

4. Líneas de telecomunicación
5. Librerías
6. Password de la librería
7. Archivos en disco temporales
8. Archivos en cinta
9. Sistemas de software
10. Software de control de acceso
11. Procedimiento de librerías
12. Logging de archivos
13. Rasgos del procesamiento de etiquetado.
14. El sistema operador existente
15. Líneas remotas
16. Diccionario/Directorio de información

ALGUNOS EJEMPLOS DE CONTROLES DE ACCESO LÓGICO SON LOS SIGUIENTES:

- LOGON ID'S o IDENTIFICACIÓN Y PASSWORDS PARA LIMITAR EL ACCESO

Estos dos pasos de identificación puede ser usado para restringir el acceso a la información que se encuentra en la computadora, transacciones, programas y software del sistema. La computadora puede mantener una lista interna de LOGON ID'S válidos y una serie de características correspondientes a las reglas de acceso de cada LOGON ID. Estas reglas de acceso identifican a los recursos de la computadora, el usuario de el LOGON ID pueda accesar.

El formato del LOGON ID'S típicamente están estandarizados. Es el password que previene de un uso no autorizado, porque es generalmente asignado por el usuario.

1. El LOGON ID provee una identificación individual. Cada usuario obtiene un LOGON ID único que puede ser identificado por el sistema.

2. El LOGON ID provee una autenticidad individual. La autenticidad es un proceso de dos pasos mediante el cual el sistema de la computadora primero verifica que el usuario tenga un LOGON ID válido y luego forza al usuario a substanciar la validación através de su password.

3. Reglas de acceso especifican quién puede accesar a que. El acceso debe estar sobre una necesidad de saber, en base a la necesidad de hacer y tipos de acceso.

Teniendo acceso a la computadora no significa siempre un acceso irrestringido.

El acceso a la computadora puede ser establecido a muchos diferentes niveles. Mediante la restricción de acceso a los niveles apropiados, un abogado de la seguridad puede ser proveído. Cuandose revisa el acceso a la computadora, se requerirá saber que puede hacerse con el acceso. Estos tipos de restricciones de acceso incluyen las siguientes:

1. Sólo lectura.
2. Sólo consulta.
3. Lectura/escritura.
4. Creación.
5. Actualización.
6. Borrado.
7. Ejecuta.
8. Copiar.

La menos peligrosa es el tipo de acceso no. 2, mientras que la información no esté siendo accesada, no esta sensitiva o confidencial. Esto es porque el usuario no puede alterar o usar el archivo mas ala de la revisión.

- LOGGING ACCESO A LA COMPUTADORA

El acceso a la computadora y violaciones de acceso pueden ser automáticamente registradas por la computadora y reportadas.

La frecuencia con la que el administrador de la seguridad debe revisar los reportes de acceso a la computadora debe estar basado en el grado de importancia de la información que ha sido protegida.

- CUANDOSE REVISE O SE SIGA EL DESARROLLO DEL ACCESO A LA SEGURIDAD, SE DEBE BUSCAR:

1. Patrones que indiquen el abuso de privilegios de acceso o concentración en una aplicación sensitiva

2. Violaciones tales como atentar accesar a los archivos de la computadora, que no estén autorizados y utilización de passwords incorrectos.

- QUÉ HACER CON EL REPORTE DE ATENTADOS DE VIOLACIONES A LA SEGURIDAD.

1. Se debe referir al administrador de la seguridad para investigación.
2. El administrador de la seguridad y administrador responsable deben trabajar juntos para investigar y determinar la severidad de la violación. Generalmente, la mayoría de las violaciones son accidentales.
3. Notificar a la administración. Si el intento de violación es serio, se le debe notificar a la administración, todavía nose notifica a las autoridades.
4. Acciones disciplinarias deben ser un proceso formal que es consistentemente aplicado. Esto puede involucrar lo que es una reprimenda, prueba o una terminación inmediata del contrato. Sin embargo, los procedimientos deben ser legalmente y éticamente sonados para reducir el riesgo de una acción legal en contra de la compañía.
5. Medidas correctivas deben incluir una revisión de las reglas de acceso a la máquina, no solo para el perpetrador sino también para las partes interesadas. Las reglas de un acceso innecesario o inapropiado deben ser eliminados.

- CARACTERÍSTICAS DE LOS PASSWORDS

1. El password debe ser fácil para el usuario, pero difícil para que el perpetrador adivine.

2. La asignación del password inicial debe ser hecho discretamente por el administrador de la seguridad. Cuando el propietario del Log lo tiene por la primera vez, el sistema debe forzar al usuario para cambiar su password periódicamente para mejorar la confiabilidad.
3. "A los tres out estás fuera". Si el password que se ha tecleado es incorrecto, un número predefinido de veces, típicamente tres, el LOGON ID es automáticamente desactivado.

4. Si el LOGON ID ha sido desactivado por un password que se olvidó. El administrador de la seguridad debe ser notificado por el usuario. El administrador de la seguridad debe entonces reactivar el LOGON ID solamente, después de haber verificado la identificación de los usuarios, así como los Bancos verifican la cuenta de una persona y su ID antes de darle información.

5. Los passwords deben ser internamente encriptados. La encriptación es una forma de enconar passwords almacenados en la computadora. Esto reduce el riesgo de que un perpetrador logre el acceso a el password de otra persona, si no lo puedes entender, no lo puedes usar.

6. Los passwords no deben ser desplegados de ninguna forma, en la pantalla de la computadora, o estar escrito en pedazos de papel para ser pegados dentro del escritorio de la persona.

7. Los passwords deben ser cambiados periódicamente. Sobre una base regular, por ejemplo, cada 30 días, el usuario debe cambiar su password. El mejor método es para el sistema de la computadora para forzar el cambio. 8. Reglas de sintaxis del password (Formato)

-Debe ser al menos de cuatro caracteres de longitud. Cualquier cosa mas corta es fácil de adivinar.
- Debe permitirse una combinación de números y letras
- No debe ser particularmente identificabie con el usuario, por ejemplo, el primer apellido, el último apellido, el nombre de la esposa o el esposo, los nombres de las mascotas etc..
- Cuando se cambia, el sistema no debe permitir passwords previos, que puedan ser usados nuevamente.

9. El LOGON ID no deberá ser usado después de un período de tiempo, por ejemplo 60 días, debe ser desactivado para prevenir un posible mal uso. Esto puede ser hecho automáticamente por el sistema o ser manualmente desarrollado por el administrador de la seguridad.

10. El sistema debe ser automáticamente desconectado a la sesión del LOGON, si ninguna actividad ha ocurrido por un período de tiempo, por ejemplo una hora. Esto reduce el riesgo de un mal uso de la sesión de LOGON, dejado sin atender porque el usuario se fue a almorzar, se fue a su casa, se fue a una reunión, etc., pero olvidó apagarlo.

- CONTROL DE ACCESO POR SEGURIDAD BIOMÉTRICA (BIOMETRIC SECURITY CONTROL)

Este control restringe el acceso a la computadora basado en características o rasgos físicos del usuario, tal como huellas digitales o la retina del ojo. Un "lector" es utilizado para interpretar los rasgos biométricos de los individuos antes de permitir el acceso a la computadora. Este es un control de acceso muy efectivo por su dificultad de engañar, pero puede no ser apto para el costo de soporte de hardware y software.

- RESTRICCIONES DEL USO DE LA TERMINAL

1.Seguridad de la terminal.
Estas características de seguridad restringe el número de terminales que pueden accesar a ciertas transacciones basadas en tratamientos físicos y lógicos de la terminal.

2. Cerraduras a la terminal.
Estos rasgos de seguridad previenen de prender, la terminal de la computadora hasta que la llave de la cerradura abra la cerradura mediante la vuelta de la llave o un tarjeta llave.

- PROCEDIMIENTO "DIALBACK"

Cuando una línea "Dial Back" telefónica es usada, el acceso debe ser restringido mediante el mecanismo "dial back". El "dial back" interrumpe la conexión, remota de telecomunicación con la computadora, mediante el "dial back" el que llama para validar la autoridad del usuario. El "dial back" puede ser manual, por ejemplo el operador de la computadora llama de nuevo al usuario, o automático; por ejemplo, la computadora regresa la llamada al usuario utilizando una lista de números telefónicos válidos. Si la llamada de regreso es un número telefónico válido, el acceso está permitido. Como una suma de precaución, los números telefónicos deben ser cambiados periódicamente, no tener el mismo prefijo como los números telefónicos de la oficina, y no serán desplegados sobre los modems o las terminales.

Una vez que una conexión remota es hecha, los controles de acceso lógico deben proveer las mismas restricciones como si el usuario estuviera utilizando una terminal desde dentro de la organización.

Algunos sistemas "dial back" pueden ser engañados, mediante el "call forwading". En estas situaciones el perpetrador primero aplica el "call forwading" a un "call back" autorizado, logrando un acceso no autorizado al teléfono que está conectado al sistema para afectar este cambio. El perpetrador puede entonces lograr el acceso a la computadora desde un número telefónico no autorizado, que va a través de un número autorizado "call back".

- RESTRINGIR Y MONITOREAR EL ACCESO HACIA LAS CARACTERÍSTICAS DE LA COMPUTADORA QUE ELUDE LA SEGURIDAD

Generalmente sólo los programadores del software del sistema deben tener acceso a estas características.

-EL procesamiento de eludir las etiquetas (Bypass label procesing (BLP))

EL BLP hace la lectura de la etiqueta del archivo de la computadora. Desde que la mayoría de las reglas de control de acceso están basados en nombres de archivos (etiquetas). Esto puede eludir acceso a la seguridad.

- SALIDAS DE LOS SISTEMA (SYSTEMS EXITS)

Estas utilidades espaciales del software del sistema permiten al usuario el desarrollar un mantenimiento del sistema complejo. Ellos existen comúnmente afuera del sistema de seguridad de la computadora y no son restringidos o reportados en su uso.

- SISTEMA ESPECIAL LOGON ID'S

Estos LOGON ID'S frecuentemente son provistos por sus proveedores con la computadora. Sus nombres pueden ser determinados fácilmente porque, son los mismos para todos los sistemas de cómputo similares. Las restricciones pueden ser alcanzadas, cambiando los passwords inmediatamente desde la instalación.

- LOGGING LA ACTIVIDAD ON-LINE

Muchos sistemas de computadora pueden automáticamente registrar la actividad de la computadora iniciada a través del logon id o de la terminal de la computadora. Ésta es conocida como una transacción log. Esta información puede ser impresa para proveer información valiosa a la administración/auditoria.

- CONTROL DE CAMBIO DE LA RED

Las redes de telecomunicaciones consisten en terminales, líneas de comunicación, modems, switches y el CPU. Estos puntos deben ser adecuadamente definidos al controlador del hardware de las comunicaciones, así las transmisiones, mensajes de procesamiento, restauración de errores y seguridad en la transmisión puede ser propiamente establecida, de otro modo, las líneas de telecomunicación sin control y la transmisiones pueden ser una trayectoria para una violación a la seguridad.

El administrador de la red es responsable de asegurar que la red está apropiadamente definida. Esto incluye conocer todas las direcciones de las terminales, las uniones de las comunicaciones, y los métodos de transmisión. Desde que las redes son dinámicas y en constante cambio, el administrador de la red, necesita tener primacía suficiente en el tiempo, que la configuración de la red, puede ser redefinida antes que las terminales, líneas etc., sean actualizadas. El software utilizado para desarrollar estos cambios deben ser accesibles solamente para el administrador de la red.

- CLASIFICACIONES DE LA INFORMACIÓN

Los archivos de la computadora, como documentos, tienen diferentes grados de importancia, mediante la asignación de clases o niveles de sensibilidad a estos archivos de computadora, la administración puede establecer guías para el grado de controles de acceso que deben ser asignados

CAPITULO NO.4

ORGANIZACIÓN-ADMINISTRACIÓN DE UN CENTRO DE CÓMPUTO.

4. ORGANIZACIÓN-ADMINISTRACIÓN DE UN CENTRO DE CÓMPUTO.

El objetivo de este punto es el de analizar y evaluar las políticas, administración y estructura organizacional, procedimientos operativos y ambiente de control del centro de cómputo y en general de los departamentos de procesamiento de información de las computadoras.

Los controles que se deben tomar generalmente en cuenta deben ser:

1. Identificación de las áreas funcionales significativas y reportar las responsabilidades de los departamentos de procesamiento de información, sobre las computadoras para lograr un entendimiento del ambiente de procesamiento de información de la organización, a través de la revisión de la documentación relevante, encuestas y observación.

2. La evaluación de la estructura organizacional y procedimientos de los departamentos que utilizan la computadora para estimar su adecuación, mediante la determinación de donde son eficientes y efectivos; y si se incluyen controles apropiados.

3.Probando los controles para determinar el cumplimiento con los estándares apropiados, mediante la aplicación de técnicas de auditoría adecuadas.

4. La estimación del ambiente de control organizacional para determinar que los objetivos del control fueron logrados, mediante el análisis de los resultados de las pruebas y otras evidencias de auditoría.

INTRODUCCIÓN

Los controles de organización y administración incluyen aquéllos controles que proveen protección para el actual o tangible ambiente físico, también como el a la gente de operación del centro de cómputo. Controles de organización y administración proveen una operación efectiva , eficiente y confiable. Los niveles apropiados de responsabilidad deben ser claramente definidos y provistos para una adecuada separación de tareas.

Los controles de la organización y de la administración alrededor del centro de cómputo comprenden lo siguiente:

1.Procesamiento de información
2.Separación de tareas dentro del ambiente de procesamiento de la información.
3.Separación de tareas entre el ambiente de procesamiento de información y otros ambientes organizacionales o funciones.
4.Técnicas para facilitar la adecuada separación de tareas.
5.Controles de compensación.
6.Políticas sólidas del personal y prácticas de administración.
7.Métodos para estimar las operaciones de efectividad y eficiencia.

4.1 AMBIENTE DE PROCESAMIENTO DE INFORMACIÓN (TIPOS DE CENTROS DE CÓMPUTO).

4.1.1 PROCESAMIENTO DE INFORMACIÓN CENTRALIZADO.

Es un ambiente en donde el procesamiento incluye una Mainframe o un Mini para procesar, actualizar y almacenar los datos transmitidos hacia y desde terminales "tontas" (todos los recursos están en un lugar).

Hay tres elementos a considerar que se pueden centralizar o descentralizar:

1.Ubicación del hardware del computadora.
2.Control de procesamiento del computadora.
3.Ubicación de almacenamiento.

El procesamiento centralizado es identificado en forma típica por un procesador central de la computadora y bases de datos que forman una configuración de un procesamiento distribuido. Un ambiente típico puede incluir una Mainframe o Minicomputadora para procesamiento actualizando y almacenando hacia y desde terminales 'tontas'.

Los controles de organización y administración están más enfocados hacia ambientes centralizados que aquéllos que no lo son.

Alternativas para la ubicación y control del hardware:

1.Hardware de computación centralizado con estaciones para entrada remota de trabajos para entrada y salida.
de computación centralizado con acceso a terminales remotas para especificar los trabajos que van a ser corridos.
3.Hardware de computación centralizado con acceso a terminales remotas solamente para entrada y salida.

Alternativas para el almacenamiento y acceso a los datos:

1.Un computadora central tiene todos los archivos y bases de datos.

2.Hay una base de datos central con subarchivos descargados a las computadoras locales para uso local; los cambios en los archivos y los datos de transacciones son enviados a la computadora central para la actualización de la base de datos.

3.Hay una red controlada centralmente de archivos y bases de datos distribuidos. Un archivo o base de datos se asigna a una computadora local y los registros de datos se transfieren a otras computadoras cuando se requiere. Un departamento típico de procesamiento de datos consiste, en un director del centro de cómputo con los sigs. administradores reportándole:

4.Un administrador de desarrollo de sistemas: Responsable por los programadores y analistas, quienes mantienen e implementan nuevos sistemas.

- UN ADMINISTRADOR DE LOS PROGRAMAS DE APLICACIÓN:
  Es responsable por los programadores que mantienen e implementan los sistemas de aplicación.

- ADMINISTRADOR DEL SOPORTE TÉCNICO:
  Es responsable por los programadores del sistema, que mantienen el hardware y el sistema del software.

- EL ADMINISTRADOR DE LA SEGURIDAD:
  Es responsable de proveer seguridad adecuada, para los programas y la información.
- ADMINISTRADOR DE OPERACIONES:
  Es responsable por el personal de las operaciones del computadora, incluyendo al operador de la computadora, al bibliotecario, al que lleva el horario y el control de la información. Estos individuos mantienen a la computadora en funcionamiento (operacional).

4.1.2. PROCESAMIENTO DE INFORMACIÓN DESCENTRALIZADO.

Un procesamiento descentralizado o entrada remota de job (trabajo) permite muchas facilidades para el procesamiento de información local, para enviar y recibir información vía módem. En la actualidad la tecnología avanzada nos ha proveído de redes de telecomunicaciones muy sofisticadas, que se comunican, vía paquete conectadas através de una red, canales microondas, y satélites.

La estructura administrativa y organizacional puede diferir dependiendo del tamaño del staff en cada locación descentralizada.

Los controles sobre el ambiente del computadora serán mas fácil de monitorear en una locación centralizada porque todos los controles importantes que están implantados están concentrados en una locación física.

Alternativas para la ubicación y control del hardware:

1.Hardware de computación descentralizado sin control central sobre las configuraciones y sin comunicaciones.
2.Hardware de computación descentralizado con control central sobre las configuraciones de equipo.
3.Hardware de computación descentralizado con red de comunicaciones para comunicación entre el hardware de diferentes localidades.
4.Hardware de computación descentralizado para procesamiento local de un computadora central para grandes trabajos.
5.Hardware de computación descentralizado con red de comunicaciones controlada por un computadora central que asigna trabajos a los computadoras locales.

Alternativas de almacenamiento y acceso a los datos:

1.Cada computadora descentralizado tiene sus propios archivos y no hay intercambio o control central.
2.Cada computadora distribuido tiene sus propios archivos, pero hay estándares para toda la organización sobre la forma de colocar nombres, las verificaciones de integridad etc..
3.Cada computadora descentralizado tiene archivos, pero los datos se pueden accesar por otros computadoras.

4.1.3. PROCESAMIENTO DE INFORMACIÓN DISTRIBUIDO.

El procesamiento de información puede tomar varias formas:

1.Procesamiento distribuido, con información no distribuida:
La mayoría de los sistemas de procesamiento distribuido, distribuye sus funciones de procesamiento en múltiples "sitios" con un controlador de datos, y que desarrollan solo procesamiento local. En otros ejemplos tenemos, que la base de datos central es copiada en una base periódica, y una copia es transmitida hacia "sitios" remotos.

2.Sistemas de datos dispersos:

Algunos sistemas distribuidos, dispersan la información entre diferentes localidades. Por ejemplo, grandes organizaciones pueden tener en cada locación regional procesos en contra de la misma versión de bases de datos, pero cada locación mantiene su propia información. El único esquema de este tipo de sistema es que la información es compartida entre los diferentes nodos del sistema.

3.Información separada, o sistemas de procesamiento cooperativo:

Algunos sistemas distribuidos tienen separadas y diferentes bases de datos en el nodo con información compartida entre ellos. Este ambiente puede existir en una gran organización donde la división manufactura mantenga, bases de datos deparadas con ciertas funciones de procesamiento y aplicaciones distribuidas entre ellas.

DEFINICIÓN DE SISTEMAS DISTRIBUIDOS

" Sistema físicamente disperso, con sistemas de computadoras autónomas que se encuentran conectadas por medio de redes de comunicación, las cuales permiten un intercambio de información".[19]

Se enfatiza en el concepto de sistemas de computadoras autónomas que actúan en forma cooperativa para resolver algún problema.

En un sistema distribuido se tendrá:

Sistema distribuido = Hardware distribuido
y/o control distribuido
y/o datos distribuidos.

1.- Hardware de Procesamiento.

Un sistema distribuido puede tener dos o mas computadoras, cada una de las cuales contiene su propio procesador y memoria. El aspecto de la distribución física es el factor mas importante en la definición de un sistema distribuido. Para que un conjunto de computadoras puedan trabajar en conjunto, se necesita que estén interconectadas, por algún sistema de redes de comunicación. La distribución física de las computadoras puede reflejarse en la distribución física de las aplicaciones o en la descomposición funcional del sistema.

2.-Control

Los sistemas contienen recursos físicos como son:
procesadores, terminales, dispositivos etc. y recursos lógicos en forma de procesos archivos etc. Por lo anterior se requiere una forma de control para manejar los recursos y coordinar las actividades las cuales se ejecutan en procesadores individuales. La estrategia para administrar los recursos del sistema puede ser centralizada, estratificada o permitiendo la completa autonomía de los procesadores individuales sobre los recursos locales. En la mayoría de los casos se intenta proveer de una transferencia en el sentido de que el sistema de la apariencia de un sistema sencillo y uniforme, independientemente de la distribución física y de la heterogeneidad de los componentes.

[19]EDP ADMINISTRATION

3.-Datos

Uno de los principales recursos que necesitan ser controlados por el sistema y el software de aplicación son los datos. Los datos pueden ser procesados por el sistema distribuido por medio de "replicas" (múltiples copias en diferentes localizaciones) o por medio de "particiones" (los datos se encuentran repartidos en diferentes localizaciones)

La distribución de los datos es también usada para aumentar la tolerancia a las fallas y aumentar la eficiencia del manejo de los datos si estos se encuentran cerca del lugar donde fueron generados y/o usados.

SEGURIDAD EN LOS SISTEMAS DISTRIBUIDOS.

El problema de seguridad de la información dentro de los sistemas distribuidos es muy discutido ya que se piensa que en este tipo de sistemas es aun mas fácil de interceptar, por la gran cantidad de tecnología con la que cuenta.

Por consiguiente se han desarrollado métodos de protección que nos permitan mantener seguridad y que, en un momento dado un usuario o grupo de estos tengan la confianza de que la información que están manejando es estrictamente confidencial.

4.1.4 USUARIO FINAL

El usuario final es el relacionado con la información, ya que tiene el desarrollo y control de sus propias aplicaciones vía micro computadoras y/o redes de área local; En el principio el papel del usuario final fue de alguna manera limitado, por el nivel de conocimientos técnicos requeridos.

Algunas organizaciones proveen entrenamiento y asistencia a través de la creación de un centro de información. Ahora, como resultado de un incremento en el conocimiento, la disponibilidad y portabilidad de las micro computadoras y el software que es fácil de usar, muchos usuarios están en disponibilidad para desarrollarlo, mantenerlo y controlar sus aplicaciones independientemente.

Las microcomputadoras pueden crear la misma preocupación como una mini computadora o una mainframe y consecuentemente, su papel dentro de la organización debe ser formalizado. Un comité de vigilancia o cualquier otra función debe ser asignada para la responsabilidad en general. Una unión formal para el departamento de sistemas debe ser establecido para apoyar a los usuarios. El comité debe tomar decisiones respecto a la centralización y descentralización, como sea apropiado y asignar las responsabilidades para:

1.Justificación de compras
2.Selección, compras, prueba y adquisición de hardware y software.
3.Programación, por ejemplo, nuevos programas y cambios a los existentes.
4.Instalación e implementación de hardware y software.
5.Documentación.
6.Mantenimiento de equipo y suministros.
7.Información y seguridad del programa.
8.Entrenamiento del usuario y soporte técnico.

Estándares, políticas y procedimientos que dirigen las áreas anotadas abajo, incluyendo aspectos legales tanto como la conexión con las leyes de copyright y uso no autorizado de la información, de la organización y los programas.

En organizaciones pequeñas, el auditor de sistemas es más fácil para que encuentre la falta de controles generales adecuados, con el entendido que la confianza no puede ser puesta sobre ellos. También puede estar limitados los controles del usuario y en particular, una falta de controles generales, los controles que limitan al usuario pueden incrementar significativamente el riesgo de un posible mal uso de una divulgación no autorizada de información.

En los ambientes donde las micro computadoras han proliferado, el auditor de sistemas debe asegurar que la administración y los aspectos operacionales han sido estimados por los estándares y las políticas de la organización.

4.1.5 TELECOMUNICACIONES

Las telecomunicaciones relacionadas con la transmisión de la información desde diferentes localizaciones vía electricidad, óptica o por medio de un sonido, como el cable de radio, fibra óptica, microondas, láser y cualquier otro sistema electromagnético. Redes de telecomunicación se han vuelto un componente necesario para la mayoría de las organizaciones de hoy en día. De hecho, muchos han establecido departamentos separados dependiendo en el tamaño y la complejidad de la configuración.

Las telecomunicaciones pueden involucrar la conectividad de las computadoras sobre una base local o global. La responsabilidad para una red de telecomunicaciones es, en muchas organizaciones, parte de el grupo de programación de sistemas. Es importante que el personal contratado ene este departamento sean con individuos técnicamente calificados y responsables. Las funciones de su trabajo deben ser claramente definidas y entendidas.

EL control en el área de telecomunicaciones es importante. El acceso al sistema debe ser controlado con el uso de passwords y tablas autorizadas que son validadas por un software de seguridad. Todos los accesos que traten de entrar deben ser registrados y revisados por la administración con una atención especial dada para el uso de líneas remotas. Sumado a esto, la administración debe desarrollar procedimientos adecuados para registrar y monitorear cualquier cambio hecho a la red. La administración debe proveer evidencias y aprobaciones apropiadas para estos cambios. Inventario e identificación de controles deben de ser mantenidos actuales como todos los activos de la organización. La administración y consideraciones de control operacional deben incluir:

1.-EFECTIVIDAD EN EL COSTO.
Operación y diseño debe ser consistente con su ciclo de vida esperado.

2.-SEGURIDAD FÍSICA.
La seguridad física debe ser suficiente para salvaguardar el equipo, los usuarios y la información.

3.-SEGURIDAD DE LA INFORMACIÓN.
La información crítica debe ser protegida de la pérdida o daño, o de un acceso no autorizado.

4.-ADMINISTRACIÓN DE LA RED.
La administración debe establecer políticas apropiadas, estándares y procedimientos para una operación efectiva, soporte y consideraciones del negocio futuras.

5.-SATISFACCIÓN DEL USUARIO.
La satisfacción del usuario debe ser considerada como una prioridad operacional y sujeto de la responsabilidad de la administración. La satisfacción del usuario puede ser monitoreada por el uso de los acuerdos de nivel de servicio entre el grupo de administración de telecomunicaciones y los usuarios.

4.1.6 REDES

Una red es representada por dos o más computadoras que pueden comunicarse y compartir la información y los recursos de la computadora. Redes de área local (LANS's) son micro computadoras que son unidas con otras micro computadoras para la forma de una red en un área local (dentro de un departamento en particular) que puede comunicarse con una mainframe o mini computadora. Una red conectada diferente en locaciones remota es conocida como una Wide Area Network(WAN).

Es importante para la administración definir una serie de políticas y procedimientos claros gobernando redes para asegurar una seguridad adecuada y control sobre el acceso para estos sistemas compartidos. Cada una de las redes deben conoce una serie de requerimientos funcionales basados en:

1.Las necesidades de los usuarios.
2.Las especificaciones del procesador.
3.Los requerimientos gubernamentales(federales, estados y locales).
4.Requerimientos de la organización (estándares, políticas y procedimientos).

4.1.7 NATURALEZA DEL PROCESAMIENTO

La naturaleza del procesamiento trata con las funciones actuales desarrolladas sobre la línea de la información. En un sistema de computadoras, los diferentes programas de aplicación contienen los pasos requeridos para proveer a los usuarios con el tipo de información que se solicite. Estos pasos usualmente incluyen funciones como: adición, categorización y sumarización, el cual es desarrollado sobre la entrada de información. El procesamiento es la manipulación de la información.

La habilidad del sistema para asistir a la organización en el procesamiento de la información día a día se incrementa como un proceso estándar, son automatizados y unidos juntos dentro del sistema. El sistema operacional, por ejemplo, en la manufacturera, puede incluir el proceso de administración de inventarios y el piso de la tienda proveyendo información estratégica para una planeación del negocio a futuro.

4.1.8 INTEGRACIÓN DE LA MAINFRAME/MICROCOMPUTADORA

La integración de la mainframe/micro computadora es básicamente realizada mediante redes y equipo de la micro computadora .

Estos sistemas permiten diferentes tipos de arquitectura para transferir información entre ellas. El proceso es mas comúnmente referido como un "downloading"(enviar información de una mainframe o mini computadora a una PC) o el "uploading"(mandar información de la PC hacia una mainframe o mini computadora).

Para mantener una era competitiva, muchas organizaciones requieren el acceso a información en un formato que puede ser interpretado mediante la lectura de la mas alta administración para la decisión de hacer propósitos. Este tipo de capacidad de reportar instantáneamente es facilitada mediante el "downloading" de información de una mini o mainframe a una micro computadora.

4.1.9 DESPACHO DE SERVICIOS DE PROCESAMIENTO

Sistemas "third-party" incluyen servicios proveídos por los despachos de servicios y firmas de tiempos compartidos. La distinción formalmente hecha entre los dos tipos de entidades esta desapareciendo lentamente desde que éllos, ahora tienden a ofrecer el mismo tipo de servicios. Los despachos de servicios ofrecen unos grandes sistemas de procesamiento batch, mientras que el sistema de tiempo compartido

proveen acceso a un gran sistema de teleprocesamiento a través de terminales de tipo máquina de escribir. Ambos son caracterizados por una gran computadora mainframe, impresoras de alta velocidad, cinta de gran capacidad y equipo de discos, y capacidad de teleproceso a través de entradas de job remotos, desplegados visuales y otros tipos de terminales.

Un despacho de servicio vende procesamiento sobre su equipo hacia una organización. Una organización puede entrar en de un acuerdo contractual con un despacho de servicio, para servicios rendidos, que pueden estar del rango de asistencia limitado en el mantenimiento de actividades normales aplicaciones a procesamiento específico, proveyendo un ambiente "stand by" en el evento de un desastre. En algunos lugares, los usuarios pueden correr sus propios programas y operar el equipo. La organización y la administración de un despacho de servicio, debe como un mínimo, cumplir con los requerimientos de una organización contratada. En suma a esto, el contrato debe proveer claramente para:

1.La seguridad sobre los programas y la información, y acuerdos de remedio desde en el evento de no cumplirlo.
2.Soporte del staff de sistemas en el on site apropiado.
3.Tarifas arregladas o variables basadas sobre el uso de recursos actuales de la computadora

Un despacho de servicios, como cualquier vendedor, debe ser una organización respetable con buen orden financiero.

Un método para asegurar la existencia de controles empleados por el despacho de servicios es la revisión de la tiempos compartidos, desarrollada por auditores independientes o contadores independientes. Cosas que se encuentran y recomendaciones deberán ser discutidas en un reporte detallado, el cual puede ser usado por la administración para hallar decisiones sobre el alcence de los controles internos dentro del despacho de servicios por otros auditores de sistemas, en sus revisiones,. los reportes cubren materias como son:

1.El ambiente de la computadora y los controles generales.

2.Controles de aplicación.

4.2 EJEMPLOS DE SEGREGACIÓN DE FUNCIONES EN EL CENTRO DE CÓMPUTO.

De acuerdo con lo establecido en los temas anteriores, la mejor segregación de tareas dentro del centro de cómputo, se cree, son las siguientes:

4.2.1 ENTRADA DE DATOS (CAPTURA DE DATOS)

La entrada de datos dentro de el lugar de procesamiento de la información es la responsabilidad del área de control de la información. Esta área desarrolla los sigs. tareas:

-Recibe documentos fuentes de varios departamentos y asegura un apropiado salvaguarda de tales documentos hasta que el procesamiento este completo y los documentos fuente y las salidas sean regresadas.

-Prepara documentos fuentes con totales de control exactos.

-Horarios para procesar las entradas.

-Verifica logs y distribuye las salidas al departamento apropiado con especial cuidado a la información confidencial.

El departamento de control de información debe ser proceaar el trabajo con el personal autorizado. Un supervisor debe ser asignado para asegurar que el trabajo esta apropiadamente preparado y submitido para su procesamiento. Este individuo debe también asegurar que todas las excepciones y entradas negadas es traída a la atención de el departamento que lo originó y re-submitido en un tiempo después. Si la entrada de la información es on line y controlada en el departamento que lo originó, la información debe ser protegida y propiamente editada por el sistema. Será entonces la responsabilidad de ése administrador del departamento en particular para asegurar que la información es autorizada, exacta y completa cuando es entrada dentro del sistema. Un sistema on line provee varias ediciones de la pantalla para desarrollar una verificación básica de las entradas que se meten a la computadora (por ejemplo, checar el rango, checar alfanuméricos, checar límites). El administrador del departamento o el supervisor deberán proveer una adecuada separación de tareas siendo responsables de los errores o de entradas negadas. Todas las transacciones re-entradas deben ir através de las mismos ediciones como la primera vez que se introdujeron.

En estos días en las empresas mexicanas esta función, esta siendo delegada a las áreas usuarias, que se encargan de capturar sus propios datos.

4.2.2 BIBLIOTECARIO

El bibliotecario debe ser un individuo de tiempo completo, que usualmente reporta al administrador del control de la información.
El algunas pequeñas empresas, sin embargo, esta función puede ser desarrollada por un miembro de la sección de control de la información. EL bibliotecario se le requiere, que registre, de salida y reciba, y salvaguarde todos los programas y archivos de información que son mantenidos en las cintas de la computadora y/o en discos en un centro de cómputo.

La mayoría de las organizaciones utilizan un sistema de administración de cintas automatizado (TMS, TAPE MANAGEMENT SYSTEM) para asistir en el mantenimiento del inventarios y movimiento de los rieles de la cinta.

4.2.3 GRUPO DE CONTROL

El grupo de control es responsable por la colección, conversión y control de las entradas y el balanceo y distribución de las salidas a la comunidad de usuarios. EL grupo de control de entradas/salidas debe estar en un área separada donde sólo el personal autorizado está permitido. El supervisor del grupo de control usualmente reporta al administrador de las operaciones del centro de cómputo.

4.2.4 OPERACIONES

Las operaciones son sinónimo de centro de procesamiento de la información. Esta incluye todo el staff requerido para que corra la computadora eficiente y efectivamente. El área debe ser segura y solo personal autorizado debe tener acceso. Nadie excepto el personal de operaciones debe tener acceso al centro de cómputo.

La responsabilidad para el centro de cómputo recae en gran parte en el administrador de operaciones, quien reporta directamente al director del centro de cómputo. Dentro de las operaciones de la computadora, los controles de la administración pueden ser subdivididos dentro de tres categorías.

1.- SEGURIDAD FÍSICA: EL centro de procesamiento de la información, incluyendo la mainframe, periféricos, medios magnéticos e información almacenada en la media, constituye una gran inversión tanto

en el valor del activo como en su impacto en la habilidad de la organización sobre la efectividad de la función.

La seguridad física define varias medidas(por ejemplo, controles) que protegen a la organización de perdidas de las capacidades del procesamiento de la computadora causada por un robo, fuego, inundación, destrucción maliciosa y fallas eléctricas o mecánicas. Las medidas de seguridad física debe ser suficientemente para tratar con cualquier pérdida que pueda ocurrir.

2.- SEGURIDAD DE LA INFORMACIÓN. La seguridad de la información son los estándares y procedimientos diseñados para proteger la información en contra de divulgación no autorizada, accidental o intencional, modificación o destrucción. Una parte critica del control de la administración ejercida por el centro de procesamiento de la información nos provee de un nivel adecuado de seguridad de la información. La seguridad de la información cubre muchos aspectos de seguridad y debe ser continuamente modificada y expandida para cubrir avances tecnológicos del de sistemas, que están teniendo lugar en un rango rápido.

Los programas de seguridad de información deben integrar efectivamente:

*Seguridad física como: La salvaguarda del hardware utilizado durante el procesamiento de la información y el medio sobre el cual la información esta siendo almacenada.

*Educación a los empleados que comprenda la necesidad de la seguridad de la información y privacidad. Los empleados deben también entender la acción disciplinaria que será tomada en contra de cualquiera que viole las guías de la organización en esta área.

*Seguridad lógica como: Son el software o controles de cables construidos dentro del sistema para prevenir y detectar acceso sin autorización a la información.

3.-CONTROLES DE PROCESAMIENTO

Son necesarios para asegurar que la organización recibe a tiempo, completa, exacta y procesamiento de la información segura. Estos controles son particularmente pertinentes para el trabajo desarrollado por los grupos de operaciones de la computadora, el cual incluye:

*Control de la informacion:Es responsable por toda la información necesaria para correr varios sistemas y para asegurar que la informacion de salida recibida es completa. Adecuar, manuales de control actualizados son esenciales para cada sistema. Los manuales deben establecer la fuente de varias formas de entrada, el medio involucrado, y el tiempo de máquina en el cual la entrada debe estar disponible.
*Control de la producción: Debe ser responsable para el horario de los job, submisión del job y el medio de administración.

Calendarización de los jobs puede ser hecho manualmente o con un paquete de calendarización automatizado. Un calendario efectivo es esencial si los recursos de la computadora son para ser usados como una eficiencia óptima.

*Operaciones del computador: Deben ser responsables del monitoreo de la ejecución de varias tareas operativas en el computador, proveyendo recursos tal como cintas, discos y estaciones especiales y corregir cualquier problema durante la ejecución de aquellos sistemas.

4.2.5 ADMINISTRADOR DE LA SEGURIDAD

La administración de la seguridad debe empezar con un comité de administración debe entender y evaluar riesgos de seguridad. La alta gerencia debe desarrollar y esforzarse por una política escrita que claramente establezca los estándares y los procedimientos que van a ser seguidos. Las tareas de la administración de la seguridad debe estar definida en las políticas. Este individuo debe ser un empleado de tiempo completo, quien reporta directamente al director del centro de cómputo y provee una adecuada separación de tareas.

Sin embargo, si es una pequeña organización no será práctico contratar a alguien para este puesto. El individuo desarrollando la función deberá asegurar que las políticas de la seguridad de la corporación está siendo cumplida con los usuarios y que los controles son adecuados para prevenir un acceso sin autorización para los activos de la organización.(incluyendo información, programas y equipo). Las funciones del administrador de la seguridad usualmente se requiere que esta persona :

1. Mantenga reglas de acceso para archivos y recursos.

2. Mantenga seguridad y confidencialidad sobre la expedición y el apropiado mantenimiento de ID's y passwords autorizados.

3. Monitorear las violaciones de seguridad y tomar acciones correctivas para asegurar que se lleve a cabo una seguridad adecuada.

4. Revisar periódicamente y evaluar las políticas de seguridad y sugerir cualquier cambio necesario a la administración.

4.2.6 CONTROL DE CALIDAD, AUDITORÍA EN INFORMÁTICA

EL grupo de control de calidad, usualmente desarrolla la prueba y verificación para asegurar que los programas y documentación se adhiera para los estándares y nombre convenciones primarias para que los programas sean movidos a producción. En algunas organizaciones este grupo puede ser una parte del control de la información pero bajo ninguna circunstancia debe ser una función del staff de programación.

4.2.7 PROGRAMADOR DE APLICACIONES

El área de programación de aplicaciones está hecha de programadores de aplicación, quienes son responsables del mantenimiento de sistemas en la producción. Ellos deben trabajar en un ambiente probado solamente y no debe moverse de versiones de prueba dentro del ambiente de producción. Programadores de aplicación no deben tener acceso al sistema de programas de librerías.

4.2.8 PROGRAMADOR DE SISTEMAS

Son responsables para el mantenimiento del hardware y el software del sistema incluyendo el sistema operativo. Esta función permite un acceso irrestricto de todo el sistema. consecuentemente, los programadores de sistemas deben ser individuos en los que se pueda confiar y su trabajo debe ser cuidadosamente supervisado. Ellos, deben mantener sus logs de su trabajo y sólo tener acceso a las librerías de trabajo del sistema de un software específico que ellos mantienen.

4.2.9 ADMINISTRADOR DE LA BASE DE DATOS

EL (DBA) administrador de la base de datos reporta directamente al director del centro de cómputo. Esta posiciones responsable para la seguridad y la clasificación de la información, de la información compartida

almacenada en un gran sistema de base de datos. El responsable de la administración de la base de datos para el actual diseño, definición y en mantenimiento apropiado de la base de datos de la organización.

4.2.10 ANALISTA DE SISTEMAS

Son especialistas que diseñan los sistemas basados en las necesidad del usuario. Ellos están usualmente involucrados durante la fase inicial del ciclo de vida del desarrollo del sistema en (SDCC SYSTEMS DEVELOPMENT LIFE CYCLE).Las funciones de un analista de sistema son similares a las de un líder de proyecto. Este individuo es responsable por la interpretación de las necesidades del usuario y la determinación de programas y programadores necesarios para crear una aplicación en particular.

4.3 TÉCNICAS PARA SEPARAR FUNCIONES

Un método probado para asegurar que las transacciones son propiamente autorizadas y registradas y que los activos de la organización están salvaguardados, es la separación de tareas. Cuando las tareas son separadas, el acceso a la computadora, la librería de información de la producción, los programas de producción y los JCL, la documentación de la programación, el sistema operativo y las utilerías asociados pueden ser limitadas, daños potenciales de las acciones de cualquier persona es por consiguiente reducido. El centro de cómputo de la organización debe ser estructurada de tal forma que la mayoría de la separación posible de tareas sea lograda.

- USO DE TABLAS DE AUTORIZACIÓN DEL PASSWORD.

Las tablas de autorización de passwords definen quién esta autorizado para actualizar, modificar, borrar y/o ver la información.

Estos privilegios son proveídos por el sistema, transacción o un nivel de campo. Sumado a ésto, las tablas de autorización de passwords, deben ser seguras en contra de acceso no autorizado, con protección del password adicional o encriptación de información. Un control de log debe registrar toda la actividad del usuario y este log debe ser revisado por la administración apropiada. Todas las excepciones a estos puntos deben ser investigadas.

- USO DE FORMAS AUTORIZADAS.

La autorización de formas provee una copia que establece quién debe tener acceso a que. Las formas de autorización deben ser apropiadamente evidenciada con un nivel de aprobación de la administración. generalmente todos los usuarios deben ser autorizados para el acceso a un sistema específico vía una petición escrita de la administración. En una gran organización o aquéllos con sites remotos, logs de firma de autorización debe ser mantenido y las peticiones escritas deben ser comparadas con la firma del log para asegurar que la autorización requerida sea o es apropiada.

Sumado a esto, debe hacer procedimientos para asegurar que la administración revise periódicamente los privilegios de los accesos para asegurar que están actualizados y apropiados para la función de job de los usuarios.

- SUPERVISIÓN

Esta provee una gran responsabilidad para las tareas desarrollados por los empleados. En este nivel, las funciones específicas pueden ser desarrolladas basadas en un gran nivel de autoridad y responsabilidad.

Algunos ejemplos típicos son: aprobación de transacciones de dólares, revisión y manejo de excepciones y manejar los defaults del sistema.

- REPORTES DE EXCEPCIÓN

Los reportes de excepción debe ser manejado en un nivel de supervisión y requerida evidencia (por ejemplo, iniciales sobre un reporte) que la excepción ha sido apropiadamente manejada. La administración debe también asegurar que las excepciones están siendo resueltas en una manera de tiempo.

- CONTROLES SOBRE EL ACCESO A LA INFORMACIÓN.

Esto es proveído por una combinación de una adecuada seguridad física, del sistema y aplicaciones, tanto en el área de usuario como en el centro de cómputo.

EL ambiente físico debe ser seguro para prevenir al personal no autorizado al acceso de los diferentes dispositivos conectados a la unidad central de proceso y así permitir el acceso a la información. El sistema y la seguridad de la aplicación son capas adicionales de seguridad, que pueden prevenir de individuos sin autorización de lograr acceso a la información de la organización.

4.4 POLÍTICAS DE PERSONAL

- DESCRIPCIÓN DE PUESTOS EN EL CENTRO DE CÓMPUTO.

Proveen a los empleados con una clave entendimiento de las responsabilidades de su trabajo y definen la línea de reporte. Esta información es importante para el auditor de sistemas para identificar la separación de tareas entre varias funciones del trabajo.

Las descripciones de puestos en los sistemas de información deben presentarse por escrito, ser claras en la delegación de autoridad y responsabilidad, mantenerse actualizadas, ir acompañadas de definiciones y de las habilidades técnicas necesarias y utilizarse como base para la evaluación del desempeño.

Deberían revisarse las descripciones de puestos en los sistemas de información para suficiencia, claridad, inclusión de narraciones sobre habilidades técnicas y utilidad como base para la evaluación del desempeño.

1. Obtener y revisar las descripciones de puestos en el departamento de sistemas de información para conocer su exactitud y claridad.

2. Comparar las descripciones de las responsabilidades actuales y determinar su exactitud.

3. Detectar, por medio de entrevistas y análisis, si la línea directa de autoridad esta en proporción con las responsabilidades.

4. Evaluar los cambios organizacionales y las descripciones de puestos, en lo que se refiere a exactitud y ver si resultan adecuados dentro del contexto de los actuales objetivos y políticas de los sistemas de información.

5. Entrevistar al personal de sistemas de información para determinar si conoce las descripciones de puestos y los ha comprendido.

6. Revisar las fechas efectivas de las descripciones de puestos para garantizar su vigencia.

7.Determinar la inclusión de relatos de conocimientos técnicos, habilidades e inventario de aptitudes y evaluar su adecuación.

8.Conocer la actualidad de los relatos de conocimientos técnicos, habilidades y el inventario de aptitudes.

9.Obtener los informes del desempeño del personal de sistemas de información y comparar los comentarios con las descripciones de puestos correspondientes, para así determinar si estas han servido como base general para evaluación.

-PRÁCTICAS DE CONTRATACIÓN

Estas prácticas son importantes para asegurar que el mas efectivo y eficiente staff es elegido y que la organización esta en conjunción con los requerimientos de reclutamiento legal. Esto puede incluir:

1. Revisión de su pasado.
2. Acuerdos de confidencialidad
3. Empleado ligado para proteger en contra del robo
4. Conflicto de acuerdos interesantes

- POLÍTICAS DE PROMOCIÓN

Deben ser justas y entendibles por los empleados. Las políticas deben ser basadas sobre un criterio objetivo y considerar una educación individual, experiencia y un nivel de la responsabilidad.

-POLÍTICAS DE TÉRMINO DE CONTRATACIÓN

Las políticas de terminación deben estar establecidas por escrito, para proveer una clara definición de pasos para la separación del empleado. Es importante que las políticas sean estructuradas para proveer una adecuada protección para los activos de la computadora de la organización y la información. Las prácticas de la terminación deben estimar:

1. Terminación Voluntaria
2. Terminación Involuntaria
3. Terminación Inmediata
4. Medidas de seguridad las cuales incluyen :
   *Regreso de todas las llaves de acceso, tarjetas de ID y gafetes para prevenir un fácil acceso físico.
   * Borrado de un logon ID y de sus passwords para prohibir acceso al sistema.
5. Otras

Procedimientos de terminación deben estimar lo siguiente:

1. Notificación a los demás empleados de la terminación de la persona, para incrementar la prevención acerca del estatus del empleado terminado.
2. Arreglar las rutinas de pago final para remover al empleado de la nómina activa.
3. Regresar toda la propiedad a la organización.
4. Arreglos para firmar de no competitividad y/o acuerdos de confidencialidad.

Es importante tener buenas prácticas de terminación laboral tanto para la organización, como para el empleado. Por lo mismo nos debemos de asegurar que:

1.El personal del centro de cómputo, cuando ha sido separado de la empresa, se le pague lo debido en términos legales.

2.Verificar que a los empleados que sean separados de la organización se les requiera que dejen o reintegren todos los documentos proporcionados por la organización, particularmente los que pueden utilizarse para activar terminales o abrir puertas de áreas restringidas.

3.Comprobar que el personal de sistemas de información, cuándo es notificado de la terminación de la relación laboral, sea acompañado inmediatamente fuera de las áreas de la empresa, sin darle oportunidad de dañar las instalaciones de cómputo o los archivos de datos de la organización.

4.Vigilar que las palabras clave o cualquier otro dispositivo de acceso a las terminales o a otros recursos de cómputo sean cambiadas inmediatamente después de la terminación de la relación laboral de los empleados.

5.Revisar los procedimientos de personal para determinar si los procedimientos de terminación de la relación laboral aplicables al personal de sistema de información concuerdan con los descritos en los puntos 1 a 4.

6.Determinar que estos procedimientos se lleven a cabo.

-ROTACIÓN DEL TRABAJO

La rotación del trabajo provee un control adicional, sobre los individuos que no desarrollan las mismas tareas todo el tiempo. Esto provee una oportunidad para un individuo, de notar en el trabajo que realiza, posibles irregularidades.

-VACACIONES .

Asegurar que una vez al año, como un mínimo, alguien como el empleado regular, desarrollará la función del trabajo. Esto reduce la oportunidad para cometer actos ilegales.

- CAPACITACIÓN DEL PERSONAL.

Se debe proporcionar a los empleados una base justa y regular para todas las funciones que se benefician de tal entrenamiento. Esto es particularmente indicado con la implementación del nuevo hardware y/o software.

Se debe orientar a los empleados al ser contratados, con capacitación continua que ayude a mantener su conocimiento técnico, sus destrezas y sus habilidades.

Se deberían evaluar las medidas para la orientación y capacitación de los empleados.

1.Analizar los manuales de inducción para verificar que se proporcionen a los nuevos empleados programas de orientación, incluyendo seguridad y control.

2.Asegurar, mediante sesiones de orientación, que los empleados de nuevo ingreso están consientes de los objetivos de la organización y del departamento.

3.Entrevistar a los empleados para determinar si saben de los programas de capacitación patrocinados por la empresa, o de los requisitos de educación continua de las organizaciones profesionales relacionadas con los sistemas de información, de las cuales ellas son miembros o por medio de las que pueden recibir certificados.

4.Revisar los cronogramas de capacitación, las descripciones de cursos, los métodos y las técnicas de capacitación para determinar si son adecuados.

- CAPACITACIÓN CRUZADA

La capacitación cruzada de individuos decrementa dependencia sobre un empleado. Este también provee un respaldo para el personal en el evento de su ausencia por cualquier razón y así provee una continuidad de las operaciones.

- CALENDARIZACIÓN Y TIEMPO DE REPORTE

Una apropiada calendarización provee una operación más eficiente. El tiempo de reporte permite a la administración monitorear el proceso de calendarización. La administración puede entonces determinar si el staffing es adecuado y la operación esta corriendo eficientemente. Es una herramienta para identificar una necesidad para cambiar o para contratar personal adicional.

-POLÍTICAS DE SEGURIDAD ESCRITAS

Todas las políticas deben estar por escrito. La política de seguridad de la organización deben ser claramente establecidas, lo que la organización considera riesgos de seguridad, que medidas de prevención han sido establecidas, quién es responsable para monitorear y esforzar estas medidas y que acciones deben de tomarse, si hay violaciones. Las políticas y procedimientos son estándares que deben cumplirse. Una política de seguridad debe ser comunicada a todo el personal periódicamente. Las evidencias deben ser obtenidas que todos los individuos han leído y entendido el establecimiento de la seguridad.

-COMITÉS DE VIGILANCIA

Proveen a la organización con la dirección en armonía con la misión corporativa y sus objetivos. Ellos usualmente consisten en varios administradores de diferentes áreas de negocios cuyo propósito es revisar y actuar de acuerdo a todas las peticiones que los nuevos sistemas necesitan. Son responsables por el uso eficiente de recursos de procesamiento de datos para lograr metas de la organización. Ellos establecen las prioridades y proveen soporte para varios proyectos.

-PLANEACIÓN ESTRATÉGICA

Establece objetivos de la organización o departamentales dentro del movimiento. La planeación comprensiva ayuda a asegurar una organización efectiva y eficiente. La planeación estratégica es tiempo y un proyecto orientado.

-SEGURO

Un seguro concerniente al centro de cómputo en un área altamente técnica. Las políticas deben establecer cubrir áreas específicas de pérdidas y variedades de problemas de procesamiento de información. tales contingencias deben incluir:

1. Pérdida debido a la interrupción de la organización
2. Pérdida por daño al equipo, al medio del archivo, al papel y a los registros.
3. Pérdida por daño físico como dispersadores de agua, aire acondicionado y dispositivos de enfriamiento de agua.
4. Robo de información y programas del sistema.
5. Gastos resultantes del procesamiento alternativo, políticas de exclusión y suministros.

-OTROS

Libros de bolsillo de los empleados que se describen los siguientes puntos:

1. Expectaciones de la organización
2. Beneficios de los empleados
3. Políticas de vacaciones
4. Reglas de tiempo extra
5. Empleados externos
6. Desarrollo de evaluaciones

Acciones disciplinarias :

1. Tiempo extra sin aprobación
2. Ausencia excesiva
3. Brecha de confianza y/o seguridad

y por último:

1.Procedimientos de emergencias

- SELECCIÓN DE PERSONAL

Las prácticas de reclutamiento y promoción de personal deben basarse en criterios objetivos y considerar la educación, la experiencia y los riesgos de trabajo pertinentes para los requerimientos del puesto y del grado de responsabilidad.

Se debería determinar la adecuación del proceso de selección de personal tomando en cuenta los siguientes puntos:

1. Identificar y evaluar los métodos utilizados en la provisión de personal para puestos vacantes.
2. Reconocer los criterios utilizados para reclutar y seleccionar a los miembros del personal y evaluar si cada uno de éstos es adecuado.
3. Entrevistar a la gerencia de sistemas de información para saber si las descripciones de puestos se utilizan como base para el reclutamiento.
4. Revisar los documentos adecuados para determinar la existencia de un criterio específico en la evaluación y selección de candidatos.
5. Examinar los registros de personal y entrevistar al gerente de sistemas de información para determinar las bases de selección del personal actual.
6. Cuidar que las políticas de filtración sean adecuadas tanto en las relaciones del empleado como en los sistemas de información.

- PROCEDIMIENTO PARA EL ASEGURAMIENTO DEL PERSONAL

EL personal de sistemas de información debe estar sujeto a un aseguramiento o afianzamiento antes de ser contratado.

Se deberían revisar los procedimientos relacionados con el aseguramiento del personal de sistemas de información.

1. Revisar la documentación de políticas de reclutamiento de personal para verificar que se hayan cubierto los procedimientos de aseguramiento.
2. Entrevistar a las personas responsables de la contratación de personal de sistemas de información para determinar si hay procedimientos adicionales de seguridad aplicables a este tipo de personal.
3. Examinar los archivos del personal de sistemas de información para comprobar que:

*Los procedimientos de investigación para aseguramiento relacionados con la contratación del personal de nuevo ingreso se han efectuado de acuerdo con los estándares de la empresa.

*Se han aplicado los procedimientos de una investigación periódica con respecto al aseguramiento.

4.5 SELECCIÓN DE EQUIPO Y APLICACIONES DE UN CENTRO DE CÓMPUTO.

Las actividades para la instalación de un nuevo equipo de cómputo son:

1. Determinar las actividades reales por las que se ha decidido comprar dicho equipo, siendo relevante darnos cuenta de nuestras necesidades.

2. Determinar los objetivos, finalidades y funciones que nos va a dar este equipo y para que.

3. Determinar quiénes serán los usuarios y cuál será la jerarquía de éstos.

4. Hacer un análisis de nuestros recursos tanto actuales como potenciales tomando en cuenta:

1. Recursos materiales
2. Recursos humanos

5. Hacer un estudio de factibilidad donde se considera un estudio de costo-beneficio.

6. Determinar el equipo que cubrirá nuestras necesidades actuales y también que contemple nuestras futuras necesidades en cierta manera y que haya cubierto la propuesta anterior.

7. Determinar qué lugar está disponible para el equipo y que cumpla con las especificaciones del fabricante, así como las características de ubicación para el mejor rendimiento.

8. Buscar asesoría a especialistas en administración, diseño, ambientación, y paquetería, manejadores de datos que cubran de mejor manera nuestras necesidades, etc..

9. Hacer una conferencia sobre el cambio que se experimentará con la adquisición de este equipo, tratando de que la gente tome conciencia de los beneficios gracias ha estos avances y no sientan que se les está desplazando.

10. Determinar las personas que tendrán que capacitarse y de qué manera, a quiénes tendremos como programadores, capturistas, supervisor, operador, analistas, etc.

Con la tecnología en materia de hardware, se ha hecho posible que los equipos de cómputo se vuelvan cada vez más económicos, por otro lado el software se ha encarecido y con frecuencia se vuelve difícil de encontrar disponible en el mercado, de manera que se pueda ajustar a las necesidades de la organización.

Para que una organización adquiera software de aplicación para la misma, debe realizar una evaluación de software en el sentido serio y profesional, como las siguientes:

ETAPA No.1:
Cuando se identifica una necesidad concreta para la adquisición de algún paquete de software, lo primero que debe hacerse es formar un comité que deberá estar formado por personas responsables del centro de cómputo, quienes concretaran esta necesidad de información.

ETAPA No.2:
Dentro del comité, se discutirá la necesidad y se dialogará con el usuario para que el personal técnico capte las verdaderas necesidades.

ETAPA No.3. EL comité hará un análisis del mercado para conocer cuáles productos cubren las necesidades específicas del proyecto. Para identificar el más idóneo, se deben considerar los siguientes parámetros de evaluación:

1.- Alcance práctico del producto. Se debe tomar en cuenta si las facilidades que ofrece el producto son las que se requieren en la organización.

2.-Compatibilidad con el software existente. De lo contrario podría cambiarse la filosofía original del producto.

3.- Sencillez para la exploración del producto. Esto debe tomarse muy en cuenta para que sea fácil para el usuario, de no ser así, a éste se la tendría que someter a un curso de especialización del mismo, lo que nos llevaría tiempo, ademas el producto tendería a olvidarse si su uso no es continuo.

4.- Mantenimiento para actualizaciones futuras. EL producto debe sufrir algunas modificaciones que se requieren.

5.- Sencillez para la instalación del producto. Hay que tomar en cuenta esto, de manera que no se requiera de personas especializadas para ello.

6.- Soporte por parte del proveedor. Es importante contar con éste en el caso de que se presentara un problema difícil de resolver de manera local.

7.- Material didáctico que proporciona el proveedor. Es necesario para la exploración del producto de manera completa y de calidad.

8.- Cantidad de usuarios del producto en el mercado. Es preferible que más personas cuenten con éste para intercambiar opiniones y usos de éste que nos permita tener un idea más completa del uso del producto.

9.- Costo del producto. Hay que tomar en cuenta el costo del mismo para hacer un análisis del costo-beneficio y poder determinar las conveniencias de la adquisición.

ETAPA No. 4:
Es recomendable que se consideren un máximo de tres proveedores y a cada uno por separado sea el que pida una demostración de su producto.

ETAPA No. 5:
Realizar una junta de trabajo entre los miembros del comité, con el objetivo de determinar una decisión con respecto al producto a adquirir.

ETAPA No. 6: Iniciar trámites de adquisición. Una vez adquirido el producto, se procederá a realizar el proceso de instalación y puesta en marcha.

Para la selección del equipo como ya se menciono se deberá hacer un estudio, a éste estudio se le denomina estudio de factibilidad tecnológica:

Se debe preparar y documentar un estudio de factibilidad tecnológica para cada alternativa.

Se deberían revisar los informes de los estudios de factibilidad tecnológica.

1. Revisar el reporte del estudio de factibilidad tecnológica para ver si se ha enfocado adecuadamente los puntos siguientes:

- Necesidades del equipo y su disponibilidad.
- Necesidades de software del sistema y su disponibilidad.
- Equipo de comunicaciones y necesidades de software y su disponibilidad.
- Restricciones de espacio y tiempos vigentes implícitas en los requisitos de información del departamento usuario y la manera de satisfacerlas.
- Factibilidad operacional del proyecto nuevo en la combinación de hardware, software y ambiente de comunicación.

2. Examinar el informe del estudio de factibilidad tecnológica para ver si se han considerado los siguientes aspectos legales relativos a la tecnología:

- Consideraciones legales relativas a la transferencia interestatal o internacional de tecnología o información.
- Restricciones legales relativas al uso de tecnología y trámites para obtener la aprobación de la autoridad correspondiente.

3. Verificar que exista un consenso entre los departamentos usuarios y los diseñadores, acerca de los aspectos tecnológicos del proyecto.

ELEMENTOS DE LA FACTIBILIDAD Y PROCESO DE SELECCIÓN DEL SOFTWARE

Cuando se selecciona el software, el equipo de gente que debe incluir el estudio de factibilidad pueden ser: el director del proyecto del desarrollo del software, quien supervise el proceso de desarrollo del proyecto, el ingeniero del sistema del software quien proporcione la definición de los requerimientos del sistema, análisis del sistema el desarrollo de un documento de diseño funcional y la planeación y la conducción y el análisis de los requerimientos del software.

Personas involucradas en los siguientes papeles de soporte: especialistas en aplicación y especialistas en el sector del negocio, especialistas en la planeación de la capacidad y en la Base de Datos, administrador de

datos, especialista de soporte técnico y de red, personal del vendedor, función de seguridad y calidad que asegure el desarrollo y distribución de un producto contractual aceptable.

Responsabilidad de control del proyecto sobre la dirección de configuración del software, procedimiento de biblioteca del programa de cómputo y planeación de proyecto, expertos en la materia que proporcionen ayuda en definir los requerimientos de las aplicaciones y la administración del sistema de información cuya responsabilidad es asegurar que el software consistente con las metas y objetivos establecidos por la organización.

DEFINICIÓN DE LOS REQUERIMIENTOS

La clave es la definición de los requerimientos del sistema. Las siguientes son tareas que deberán ser consideradas para la definición de los requerimientos: Establecer el ámbito, objetivos, antecedentes y estatutos del proyecto, establecer los requerimientos del negocio y datos requeridos para cumplir con las necesidades del negocio, desarrollar los requerimientos de seguridad, control y ejecución, consolidar la definición de todos los requerimientos y analizar y evaluar las soluciones alternativas.

ALTERNATIVAS DE SOFTWARE

El software puede ser comprado como un paquete a un vendedor o puede ser desarrollado dentro de la organización, o por un despacho externo, el análisis del requerimiento del sistema debe de incluir una evaluación de lo siguiente: costo del software, disponibilidad de soporte, plan de distribución incluyendo requerimientos anticipados, requerimientos y restricciones, productos propuestos por los vendedores del paquete, productos que corresponden cercanamente a los requerimientos definidos, selección de la recomendación para un vendedor y producto en particular, razones para seleccionar o rechazar alternativas, compatibilidad del software de sistema interno existente, tales como: SMBD y software de comunicaciones, conducción de estabilidad financiera del proveedor del software y soporte técnico del proveedor del software.

ANÁLISIS COSTO BENEFICIO

EL análisis costo-beneficio proporciona a la administración del sistema de información un análisis del costo de implementación del sistema de información un análisis del costo de implementación del software y los beneficios que podrán ser derivados del software propuesto, lo siguiente será incluido en el análisis: costo operativo del sistema actual, recursos y facilidades requeridas para mantener el sistema actual, recursos y facilidades requeridas para mantener el sistema actual, planeación del proyecto, recursos y facilidades incrementar en el futuro el sistema propuesto. Habilidad para incrementar en el futuro el sistema, oportunidad para proporcionar gran eficiencia y uso efectivo del costo de los recursos de procesamiento y costo operativo del sistema propuesto.

ASPECTOS REGULATORIOS Y LEGALES

En algún caso la petición del desarrollo del sistema puede estar basado en algún cambio, en alguna ley por requerimientos regulatorios, todos los requerimientos deben ser incluidos en el estudio de factibilidad y en la definición de requerimientos.

IMPLEMENTACION Y PROCEDIMIENTO DE CONTROL DE CAMBIOS

Los controles de implementación para el software del sistema incluyen controles sobre el diseño del nuevo software, revisión del software, controles sobre la colocación del software aprobado en producción y

controles para asegurar que todos los archivos de datos son correctamente convertidos, verificados y reconciliados antes de la implementación. Tipicamente la petición de software nuevo o modificación al software existente son inicializados por los usuarios, esto esta basado en las necesidades o en promover la eficiencia del procesamiento. Hasta la terminación del proyecto del sistema y desarrollo del programa el software puede ser examinado en tres etapas:

ETAPA I: Examinar el programa para verificar la lógica de los programas individuales.

ETAPA II: Examinar el sistema que involucra verificar la lógica de los programas para asegurar la consistencia ya que van a ser enlazados y que cumplan con los requerimientos del sistema.

ETAPA III: Revisión paralela del nuevo software simultáneamente con el software existente.
El objetivo de la revisión paralela es determinar si el sistema se puede dar abasto con los datos reales y manipular los volúmenes reales.

Todos los resultados de las pruebas deben ser documentados, analizados y aprobados por el usuario antes de trasladarlo a producción. Los procedimientos del control de cambios esta diseñado, para asegurar que los usuarios y la administración del sistema de información están siguiendo los procedimientos específicos en la petición de cambios. Las modificaciones al software deben cubrir los mismos pasos que los controles de implementación, los cambios al software deben ser completamente examinados, documentados, revisados y aprobados por el usuario antes de trasladarlos a producción.

4.6 DOCUMENTACIÓN EN LOS CENTROS DE CÓMPUTO

La correcta elaboración de la documentación tiene una gran importancia, ya que muchos de los programas y procesos desarrollados anteriormente quedaban rápidamente obsoletos ya que carecían de información acerca de su constitución y funcionamiento.

El propósito de la documentación es brindar información pertinente acerca de los procesos, operaciones y funcionamiento de los sistemas software y hardware que son utilizados por la organización.

La documentación es generada directamente para los usuarios, operadores y técnicos quienes son los que usan, operan y mantienen el software y/o hardware respectivamente.

MANUAL DEL USUARIO

EL manual del usuario es un instructivo para instalar y operar el sistema o paquete de programación.

Dependiendo de la complejidad del sistema y de la extensión de su documentación, el manual del usuario podrá ser presentado en un solo documento, o bien, como un conjunto de guías que tratan en forma independiente, los aspectos básicos de operación e instalación. Estas guías son:

1.-Guia de instalación.

Define la manera y los medios de transportar el sistema de programación al equipo de explotación de cómputo. Esta guía deberá incluir los siguientes aspectos:

- EL equipo.
- Las instrucciones de instalación necesarias para que el sistema o paquete funcione apropiadamente.
- Procedimiento de instalación.
- Descripción de pruebas que permitan constatar la correcta instalación.

2.-Guía de operación.

Define la manera de utilizar el sistema; enfatiza aspectos que permiten al usuario obtener el mejor provecho de las funciones que el sistema realiza. Esta guía debe incluir cuatro aspectos importantes:

- EL panorama general del sistema:
  Es una descripción breve del sistema que permite al usuario conocer las funciones que dicho sistema puede realizar.
  La información debe ser estructurada y objetiva, para lo cual es muy útil un modelo conceptual.

- La interface hombre-máquina:
Incluye todos los medios existentes para la comunicación bidireccional entre el sistema de programación y el usuario, es decir:
  *Desplegados.
  *Reportes.
  *Mensajes.
  *Alarmas.
  *Tableros.

- Recomendaciones de uso.

- Glosario de términos utilizados.

De acuerdo a varios manuales de usuario consultados, se sugiere que lleven por lo menos las siguientes partes:

1.- INTRODUCCIÓN
  1.1 IDENTIFICACIÓN
  1.2 REVISIÓN DEL SISTEMA
  1.3 REVISIÓN DEL DOCUMENTO
2.- DOCUMENTOS A LOS QUE HACE REFERENCIA
3.- EJECUCIÓN DE PROCEDIMIENTOS
4.- MENSAJES DE ERROR
5.- NOTAS

1.1 Identificación.

Esta parte se debe incluir el nombre del programa, el número de versión e identificacion del número del sistema en la organización.

1.2 Revisión del sistema.

Esta parte enfatiza el propósito del sistema y las características del mismo para motivar al uso de este documento.

1.3 Revisión del documento.

En esta parte normalmente se provee al usuario de las instrucciones y comandos para operar el sistema.

2.-Documentos a los que hace referencia.

Este párrafo lista los documentos a los cuales se hace referencia, tales como formas, catálogos de cuenta etc.. que la organización utiliza para obtener los reportes que el sistema genera.

3.-Ejecución de procedimientos.

Esta parte debe contener:

- Iniciación de procedimientos.
- Entradas del usuario.
- Entradas del sistema o dispositivos externos, incluyendo formatos, frecuencias de uso, unidades de medida, etc.
- Procedimientos para tirar (Shut-down) el sistema.
-. Como reiniciar los procedimientos.
-. Las salidas de los procedimientos.

4.- Mensajes de error.

Debe incluir todos los mensajes de error que pueden ocurrir, su significado y las posibles soluciones o alternativas que puede tomar el usuario.

5.- Notas.

Puede incluir información general que es necesaria y una lista de sinónimos, acrónimos y abreviaturas que son usados en el documento.

EVALUACIÓN DEL MANUAL DEL USUARIO.

1. ¿Está escrito claramente ?

2. ¿El tono de redacción del manual es informal y conversacional?

3. Está diseñado para un lector que no necesariamente ¿conoce todos los términos técnicos?

4. Si el programa incorpora un menú de árbol, entonces ¿el manual incluye dicho árbol?

5. Si el programa incluye formatos de entrada, entonces ¿están producidos dichos formatos en el manual?

6. Para cada dato de entrada en el programa, ¿está el usuario informado del significado del campo, de su rango, de sus unidades de medida, y de la fuente de los datos?

7. ¿Incluye, cómo puede el usuario pedir fácilmente la ayuda?

8. ¿Hay un ejemplo de la salida del programa?

9. Si el manual es mas grande de 30 hojas, entonces incluye un índice (normalmente un apéndice)?

10.¿ Está preparado el manual para servir como un tutorial de uso del sistema para cualquier persona que requiera utilizarlo?

MANUAL DEL OPERADOR

Es un documento que contiene especificaciones para mantener la disponibilidad de hardware y de software en el sistema.
Aquí se presentamos los puntos que debe contener el manual en forma general :

1.- IDENTIFICACIÓN
2.- REVISIÓN DEL SISTEMA
3.- REVISIÓN DEL DOCUMENTO
4.- DOCUMENTOS A LOS QUE HACE REFERENCIA
5.- OPERACIÓN DEL SISTEMA
    5.1 PRENDIDO Y APAGADO
    5.2 INICIALIZACIÓN
    5.3 SHUTDOWN (TIRAR EL SISTEMA)
    5.4 ENTRADA Y SALIDA DE LOS PROCEDIMIENTOS.
    5.5 MONITOREO DE LOS PROCEDIMIENTOS
    5.6 PROCEDIMIENTOS DE RECUPERACIÓN
    5.7 OTROS PROCEDIMIENTOS
6.- ACTIVIDADES DE DIAGNÓSTICO
    6.1 PROCEDIMIENTOS DE DIAGNÓSTICO
    6.2 MANEJO DE HERRAMIENTAS PARA
    6.3 DIAGNOSTICAR
7.- NOTAS

1. IDENTIFICACIÓN

En este punto se especifica el objetivo del manual y se describe en forma general los aspectos de que se trata todo el documento.

2. REVISIÓN DEL SISTEMA

Se refiere a las especificaciones generales del sistema de cómputo, en cuanto a las capacidades y requerimientos. Así como el funcionamiento, interfases e interconexiones.
Las estructuras y módulos de los que se conforma el sistema.

3. REVISIÓN DEL DOCUMENTO

Se refiere de forma general a los temas que abarca el manual y los puntos mas sobresalientes y en los que el operador debe poner especial atención.

4.- DOCUMENTOS A LOS QUE HACE REFERENCIA

En esta parte se especifican las formas o catálogos que el operador debe manejar y a las cuales se debe hacer referencia para verificar los datos que le son necesarios en el control del sistema.

5.- OPERACIÓN DEL SISTEMA

La operación se refiere a las funciones que se deben realizar constantemente para manejar y controlar los accesos de los usuarios al sistema. Los procedimientos que se deben ejecutar para la inicialización, constante chequeo, de la situación del sistema (monitoreo).

Los procedimientos de recuperación y respaldos de cintas y discos tienen que estar perfectamente especificados ya que la información es el elemento de mayor importancia para el sistema. Especificar la operación de periféricos para efectos de montaje de cintas y papelería de impresión.

6.- ACTIVIDADES DE DIAGNÓSTICO

En este punto se especifican las actividades para verificar las fallas del sistema, así como la situación en la que se encuentra el sistema.

También se deben especificar el manejo y ejecución de las herramientas que realizan el chequeo de la situación del sistema para que el operador puede llevarlos a cabo en un momento determinado.

EVALUACIÓN DEL MANUAL DEL OPERADOR

1.¿ Está escrito claramente?

2.¿ Está toda la información requerida por el operador clara y fácil de encontrar?

3. ¿ Están incluidos todos los procedimientos utilizados por el operador del equipo?

4. ¿ Están incluidos todos los procedimientos utilizados por el operador del equipo?

5. ¿ Está incluido un glosario de términos utilizados en el manual?

MANUAL TÉCNICO

Es un documento que contiene los procedimientos adecuados para la instalación, configuración y mantenimiento del equipo.
Hay dos tipos de manuales técnicos.

-MANUAL TÉCNICO DEL EQUIPO -MANUAL TÉCNICO DEL SISTEMA.

El primero es el manual técnico del equipo, donde se determinan los siguientes puntos:

MANUAL TÉCNICO DEL EQUIPO

1.- INSTALACIÓN DEL EQUIPO Y PUESTA EN MARCHA
2.- CONFIGURACIÓN DEL EQUIPO
3.- MANTENIMIENTO DEL EQUIPO

1.- INSTALACIÓN DEL EQUIPO
Contiene los procedimientos necesarios para la correcta instalación del equipo.

2.- CONFIGURACIÓN DEL EQUIPO
Describe la arquitectura del equipo y sus interconexiones.

3.- MANTENIMIENTO DEL EQUIPO
Describe los procedimientos adecuados para el mantenimiento del equipo.

En el centro de cómputo debe haber manuales técnicos de cada uno de los sistemas y del equipo que se utiliza. Ambos tipos de manuales tienen como finalidad conservar información necesaria para el mantenimiento preventivo, correctivo, aditivo y adaptativo del hardware y el software.

Los manuales técnicos del software permiten que una persona o grupos de trabajo puedan modificar, agregar, compilar, ligar, etc.. el código fuente de un sistema que ellos no realizaron. Estos manuales no dan detalle del uso del programa, en si se enfocan a aspectos internos de su funcionamiento. La siguiente lista nos muestra los puntos contenidos en el manual técnico del sistema :

CONSIDERACIONES CON EL MANUAL TÉCNICO DEL EQUIPO O DEL HARDWARE

Los manuales técnicos de equipo deben estar cerca del centro de cómputo, resguardados y clasificados; esto es con la finalidad de que si hay alguna falla del equipo, al técnico no se le dificulte la reparación. Debe haber un manual por cada uno de los dispositivos que se tengan: unidades de cinta, impresoras, discos, procesadores de comunicación, etc.La siguiente lista esboza el contenido de otro manual técnico de equipo:

1.-Caracteristicas técnicas del equipo.
En esta parte de la documentación se deben especificar características como voltaje soportado, nivel de temperatura, requerimientos especiales, etc..

2.-Instalación.
En esta sección se plantea el procedimiento que se debe seguir para la instalación y puesta en marcha del equipo.

3.-Configuración.
Aquí se especifican los "switch", "jumpers" y programas que permiten configurar el sistema a las necesidades especificas del centro de cómputo.

4.-Descripción de partes y funciones.
Aquí se hace un diagrama de los componentes del equipo y se hace una descripción de su funcionamiento.

5.-Lista de posibles fallas.
Aquí se hace una relación de los errores que impiden el óptimo funcionamiento del equipo.

MANUAL TÉCNICO DEL SISTEMA

1.- INTRODUCCIÓN
2.- OBJETIVO DEL SISTEMA
3.- DESCRIPCIÓN GLOBAL DEL SISTEMA
4.- MÓDULOS QUE COMPONEN EL SISTEMA
5.- PARÁMETROS DEL SISTEMA
6.- COMPILACIÓN, LIGADO Y EJECUCIÓN DEL SISTEMA
7.- ESTRUCTURA DE DATOS, ARCHIVOS Y/O BASES DE DATOS

A este contenido básico podemos agregar diagramas de entidad relación, diagramas de flujos de datos y un listado del programa.

1.-.INTRODUCCIÓN
En esta parte se deben especificar los motivos del desarrollo del sistema, el nombre de los diseñadores, el lenguaje seleccionado, fecha de elaboración, computadora en la que se elaboró, computadora en la que se usará y recomendaciones generales sobre medidas de seguridad.

2.-.OBJETIVO DEL SISTEMA
Aquí se debe plantear la necesidad que originó el sistema y la medida en que ha sido satisfecha.

3.- DESCRIPCIÓN GLOBAL DEL SISTEMA
Aquí se debe esquematizar el funcionamiento general del sistema, sus interfaces y relaciones. Se pueden usar diagramas de contexto, de proceso, etc.

4.- MÓDULOS QUE COMPONEN EL SISTEMA
En esta parte se desglosa el sistema en sus módulos, especificando que hace cada uno de ellos, detallando sus valores de entrada y salida.

5.- PARÁMETROS DEL SISTEMA
En una o dos hojas se deben detallar los parámetros que podemos pasar al sistema y lo que cada uno de ellos provocará en el funcionamiento del mismo.

6.- COMPILACIÓN, LIGADO Y EJECUCIÓN DEL SISTEMA
Aquí se deben especificar paso a paso la forma en que el programa se compila, como y con que otros módulos o librerías se liga; Y por último, la forma en que debemos ejecutarlo.

7.- ESTRUCTURAS DE DATOS, ARCHIVOS Y/O BASES DE DATOS
En esta parte deben incluirse los nombres de las bases de datos y/o archivos y su localización física; Y los registros usados en los procesos.

Es recomendable incluir en cada uno de los programas un encabezado que especifique lo siguiente:

- Forma de compilación.
- Forma de ejecución.
- Parámetros usados.
- Archivos de salida.
- Reportes generados.
- Breve explicación de su proceso.

CONCLUSIONES.

CONCLUSIONES

El presente trabajo, se estructuró de tal manera que pueda servir como una herramienta a la administración de centros de cómputo para implantar controles, caminando desde el proceso administrativo aplicado al centro de cómputo, pasando por la revisión, a los controles en los tres tipos de infraestructuras, definiendo seguridad, riesgos, explicando los diversos controles etc., pudimos establecer, a la calidad, como parte integrante del control.

Con ésto nos percatamos de las ventajas que se obtienen de implantar controles en todos los aspectos del centro de cómputo como parte integrante de la organización.

Se entendió la importancia de adecuar las metas del centro de cómputo de acuerdo con los objetivos de la organización.

Se estableció la importancia de poder medir los riesgos, de cómo controlarlos mediante la implantación de medidas de seguridad.

Se vió la importancia que tiene el individuo dentro del centro de cómputo, en lo que respecta al manejo del personal y las políticas de selección de personal en el área de sistemas.

Se afirmó que es importante que el usuario esté consciente de sus derechos, responsabilidades y obligaciones para el centro de cómputo. Todo esto para un mejor funcionamiento.

La importancia de la segregación de funciones, dentro del centro de cómputo, es fundamental entenderla ya que sin una buena separación de tareas, las actividades dentro del mismo se duplicarían y se realizarían esfuerzos en vano.

En sí se cumplió con el objetivo de la presente tesis, que fué el de mostrar la importancia de los controles para poder adquirir la calidad en el funcionamiento del centro de cómputo y así cumplir con las expectativas para las cuales fué creado.

A través de todo el trabajo se dieron una serie de puntos a revisar. Estos puntos son la recopilación de apuntes en otros libros, investigación y observación en Vitro Corporativo de Monterrey , Bancomer, Centro de cómputo de minicomputadoras de la facultad de Química en la U.N.A.M. y en el centro de cómputo de la HP3000 en la Facultad de Contaduría y Administración.

GLOSARIO.

GLOSARIO

1.- **ANÁLISIS COSTO/BENEFICIO.**

Un estudio que proyecta los costos y los beneficios de un nuevo sistema de información. Los costos incluyen los recursos humanos y de máquina necesarios para el desarrollo, asi como los gastos operacionales que demandará el funcionamiento del sistema.

2.- **APLICACIÓN.**

(1) Un uso específico de la computadora. Por ejemplo, sueldos, inventarios y cuentas a cobrar son aplicaciones típicas de negocios.

(2) Sinónimo de programa de aplicación o paquete de software. Por ejemplo, los procesadores de texto, las hojas de cálculo y los gráficos comerciales son aplicaciones. A menudo se refiere al programa que se está ejecutando y a los archivos y bases de datos con los que trabaja.

3.- **CABLEADO.**

(1) Circuito electrónico que está diseñado para realizar una tarea específica.

(2) Dispositivos que están acoplados estrechamente o en proximidad. Por ejemplo, una terminal cableada se conecta directamente a una computadora sin pasar através de una red conmutada.

4.- **COMPUTADORA.**

Una máquina de propósito general que procesa datos de acuerdo con el conjunto de instrucciones que están almacenadas internamente , ya sea temporal o permanentemente. La computadora y todo el equipo conectado a ella se denomina hardware. Las instrucciones que le dicen lo que tiene que hacer se llaman software. Un conjunto de instrucciones que se lleva a cabo una tarea específica se denomina programa, o programa de software.

5.- **CONSULTOR O ASESOR.**

Un especialista independiente. Los consultores pueden actuar como consejeros, o pueden desarrollar funciones detalladas de análisis y diseño de sistemas. Pueden ayudar a los usuarios a formular sus

requerimientos de información y producir un conjunto de especificaciones generalizadas o detalladas a las cuales pueden responder los fabricantes de hardware o software. Los consultores son empleados habitualmente como consejeros de proyecto durante el ciclo completo del desarrollo de un sistema.

6.- **CRIPTOGRAFÍA.**

La conversión de datos a códigos secretos con fines de seguridad.

7.- **DISCO DE SEGURIDAD O DE RESPALDO.**

Un disco que se utiliza para almacenar copias por duplicado de archivos importantes. Los discos flexibles de alta densidad, los cartuchos de discos removibles se emplean como discos de respaldo.

8.- **DOCUMENTACIÓN.**

La descripción narrativa y gráfica de un sistema.

9.- **ENCRIPTACIÓN.**

Codificación de datos con propósito de seguridad, convirtiendo el código de datos estándar en un código propio. Los datos cifrados deben codificarse para ser usados. El cifrado se usa para transmitir documentos por una red o para codificar texto de modo tal que no pueda ser modificado con un procesador de textos.

10.- **ESTUDIO DE FACTIBILIDAD.**

Análisis de un problema para determinar si puede ser resuelto efectivamente. Los aspectos operacionales(¿va a funcionar?), económicos (costos y beneficios) y técnicos (¿puede hacerse?), son parte del estudio. Los resultados de un estudio de factibilidad proveen datos para una decisión de iniciar o no iniciar el proyecto.

11.- **ENERGÍA DE RESPALDO O DE SEGURIDAD.**

Una fuente de alimentación adicional que puede ser utilizada en caso de un eventual corte de la energía de línea.

12.- **JERÁRQUICO.**

Estructura compuesta por diferentes niveles, como un diagrama de organización de una compañía. Los niveles más altos tienen control o prioridad sobre los niveles más bajos. Las estructuras jerárquicas son una relación de uno a muchos, ya que cada elemento tiene uno o más elementos debajo.

13.- **PROGRAMA DE APLICACIÓN.**

Cualquier programa de ingreso de datos, actualización, consulta o informe que procesa datos para un usuario.

14.- **PROTECCIÓN CONTRA COPIAS.**

La resistencia a la copia no autorizada del software. La protección contra copias nunca fue un tema importante en las mini y macro computadoras, ya que el soporte del fabricante siempre ha sido vital en esos ambientes.

15.- **PROTOCOLO CLIENTE/SERVIDOR.**

Un protocolo de comunicaciones que provee una estructura para requerimientos entre una estación de trabajo (cliente) y un servidor en una red. Se refiere al estrato 7 del modelo OSI.

16.- **PROTOCOLO DE COMUNICACIONES.**

Estándar de software o de hardware para transmitir datos entre terminales y computadoras, únicamente entre computadoras. El estándar internacional OSI y SNA de IBM define siete niveles de protocolo para redes de grandes organizaciones; sin embargo, el intercambio de datos entre computadoras personales utiliza protocolos solamente en los últimos niveles inferiores, de dos a cuatro capas.

17.- **PUNTO DE REINICIO/VERIFICACIÓN (RESTART).**

Un método para recuperarse de un fallo de sistema. Un punto de verificación es una copia de la memoria de la computadora que se graba periódicamente en el disco, conjuntamente con los valores corrientes de los registros (última instrucción ejecutada, etcétera). En el caso de un fallo de energía o un fallo de software o de hardware, el último punto de verificación sirve como punto de recuperación.

18.- **RED CONMUTADA O DIAL-UP NETWORK.**

La red telefónica conmutada que está controlada por los gobiernos nacionales de cada país, en los E. U., está administrada por empresas tales como AT & T, MCI, las compañías Bell y muchas otras. En México sólo existe TELMEX, por el momento.

19.- **SERVIDOR DE COMUNICACIONES.**

Una computadora en una red que administra el acceso a redes externas. Puede administrar un grupo de modems y/o proveer puertas de acceso a redes diferentes.

20. **SISTEMA DE CÓMPUTO**.

Un sistema formado por una CPU, todos los dispositivos periféricos conectados a ella y el sistema operativo. Los sistemas de cómputo pueden englobarse en categorías llamadas microcomputadoras (computadoras personales), minicomputadoras y macrocomputadoras.

21.-**SESION DE TERMINAL**.

Tiempo durante el cual un usuario trabaja en una terminal.

22.- TOMA DE DECISIÓN.

Acción de elegir. El equilibrio apropiado entre las decisiones tomadas por personas y por máquinas es una parte importante del diseño del sistema.

BIBLIOGRAFÍA.

1. *The Auditors Assesment of Control Risk.*
Anderson, Ortar Liggett.

2. *Strategic Risk Management : How Global Corporation Manage Financial Risk For Competitive Advantage.*
Anh, Mark J.

3. *La Aventura del Trabajo Intelectual.*
Armando F. Zubizarreta.
Fondo Educativo Interamericano, México 1983.

4. *Computer Security Handbook.*
Becker, Richard H.

5. *Management of Computer Operations.*
Borovits, Israel.

6. *Modern Internal Auditing: Appraising Operations and Controls.*
Briuk, Victor Zinn.

7. *Control y auditoria del computador.*
C. Mair, William
Instituto Mexicano de Contadores Públicos, A.C.

8. *Computer System Performance Management and Capacity Planning.*
Cady, John.

9. *Software Reliability and Safety.*
Cittlewood and D. Miller.

10. *Computer and Comunications Security Strategies for the 1990's.*
Cuopr Armin, James.

11. *Auditing Program Libraries for change Controls.*
Dallas, Dennis A.

12. *Controles y Supervisión.*
Ettinger, Karl E.
Herreros Hermanos.

13. *Programas Analíticos, Plan 85.*
Facultad de Contaduría y Administración, U.N.A.M.
Lic. en Informática.

14. *Controles Internos para Sistemas de Computación.*
Fitzgerald, Jerry.
Limusa.

15. *Sistemas de Información Basados en Computadora Para la Administración Moderna.*
G. Murdick, Roberto.

16. *Principles of EDP Management.*
Gaydasch, Alexander.

17. *Velocidad y Amplitud de la Difusión del Progreso Técnico de todos los Sectores de la Economía Mexicana.*
Investigación encargada al Grupo de Economistas Asociados(GEA) por el CONACYT.

18. *Risk Assesment.*
Genomy, Laurie.

19. *A Handbook of Computer Security Management.*
Hearden, Keith .

20. *Administración de Centros de Cómputo.*
Hernández Jiménez, Ricardo.

21. *Audit, Control and Security of Paperless Systems. Trends, Guidelines, Practices and Techniques.*
Based on the proceedings of the 1990 advanced technology forum.
Conducted by IIA'S International Advanced tecnology comitee.
Sponsored by the Institute of Internal Auditors Research Foundation.
Septiembre 17-19, 1990 Orlando Florida.

22. *La Auditoria Interna de la Administración de Riesgos.*
Instituto Mexicano de Contadores Públicos.

23. *Memoria del Primer Seminario Técnico de Informática en la Administración Pública.*
Presente y Futuro de las Bases de Datos.
Instituto Nacional de Estadística, Geografía e Informática.

24. *Multinational Risk Asessment and Management : Strategies for Investment and Marketing Decisions.*

25. *Management Guide to Computer System Selection and Use.*
Kanter, Jerome.

26. *Computer Data Management and Data Base Technology.*
Katzan, Harry.

27. *How to Prepare Audit Plans for EDP Systems.*
Kuong, Javier F.

28. *Microfoundations of Sistematic Risk.*
Kupiec, Paul Henry.

29. *Las Computadoras y la Información.*
Lawrences, Orilia.
Mc Gawhill.

30. *Risk Management Manual.*
Lenz, Matthew.

31. *Finantial Controls for Management.*
Lewis, Ronello B.

32. *Auditing Internals Controls: A Computational View of The Review Process.*
Meservy, Rayman.

33. *A Handbook of EDP Auditing.*
Michael A.Murphy, Xenia Ley Parker, Albert H. Decker.
Coopers & Lybrand second edition 1989.
Warren, Gorham & La Mont.

34. *A Framework for Evaluating Internal Audit Risk.*
Patton, James M.

35. *EDP Administration and Control.*
Perry, William E.
Prentice-Hall.

36. *EDP Controls and Auditing.*
Porter, W. Thomas.

37. *Controles Elementales de Dirección.*
Ricardi, Ricardo.

38. *Capacitación hacia la calidad total y el mejoramiento continuo.*
Secretaria del trabajo y previsión social.
Oficialia mayor.
Dirección General de Administración de Recursos Humanos.
Dirección de Capacitación y Desarrollo.

39. *Programa de Capacitación.*
Delegación Federal del Trabajo.
Secretaría del Trabajo y Previsión Social.
Dirección General de administración de Recursos Humanos y Servicios Sociales.
Dirección de Capacitación y Desarrollo.
Oficialía Mayor.

40. *Managing Information Security : Administrative, Electronic and Legal Measures to Protect Business Information.*
Scheweitzer, James A.

41. *Distributed Processing System.*
Thieranf, Robert
Prentice-Hall.

42. *Multinational Risk Assesment and Management: Strategies for Investment and Marketing Decisions.*
Tiny, Wenlee.

43. *Diferentes Tipos de Control y su Importancia.*
Vallez Muñoz, Francisco Alberto.
SHCP.

44. *Computer Security Management.*
Van Tassel, Denni.
Prentice-Hall.