



Universidad Michoacana de San Nicolás de Hidalgo



Facultad de Contaduría y Ciencias Administrativas

TÍTULO DE LA TESIS:

“Propuesta para la implementación de administración de riesgos en el centro de cómputo de la FCCA”

Para obtener el título de

Licenciado en Informática Administrativa

Autor: Raymundo Bedolla Díaz

Asesor: M.A. Erik Alfaro Calderón

Coasesor: Dr. Gerardo Alfaro Calderón

Morelia, Mich. Junio de 2013

AGRADECIMIENTOS

A mis padres, porque creyeron en mí y porque me sacaron adelante, dándome ejemplos dignos de superación y entrega, porque en gran parte gracias a ustedes, hoy puedo ver alcanzada mi meta, ya que siempre estuvieron impulsándome en los momentos más difíciles de mi carrera, y porque el orgullo que sienten por mí, fue lo que me hizo ir hasta el final.

Va por ustedes, por lo que valen, porque admiro su fortaleza y por lo que han hecho de mí.

A mis hermanos, tíos, primos, abuelos y amigos.

Gracias por haber fomentado en mí el deseo de superación y el anhelo de triunfo en la vida.

Mil palabras no bastarían para agradecerles su apoyo, su comprensión y sus consejos en los momentos difíciles.

A todos, espero no defraudarlos y contar siempre con su valioso apoyo, sincero e incondicional.

A mi asesor y Coasesor, por la orientación y la ayuda que me brindaron para la realización de esta tesis, por su apoyo y amistad que me permitieron aprender mucho más de lo estudiado en este proyecto.

ÍNDICE

Introducción	2
Definición del problema	2
Objetivo general	3
Objetivos específicos	3
Formulación de hipótesis	3
Justificación	3
 CAPÍTULO I: Administración de Riesgos	 5
Generalidades de la administración de riesgos	5
Definición de Riesgo	6
Factores del entorno general	8
Factores del entorno específico	16
Definición de Administración de Riesgos	27
 CAPÍTULO II: Problemas más comunes en centros de cómputo	 29
Análisis de Riesgos	31
Plan de Contingencias	32
Riesgos en el centro de cómputo	38
Riesgos relacionados con la informática	39
 CAPÍTULO III: Centros de Cómputo	 49
Definición de Centros de Cómputo	49
Misión del Centro de Cómputo	52
Hardware	54
Software	65
Interacción Hardware-Software	73
 CAPÍTULO IV: Organización de los Centros de Cómputo	 84
Principales departamentos del Centro de Cómputo	85
Planificación del Centro de Cómputo	86
Instalaciones físicas del Centro de Cómputo	93
 PROPUESTA	 114
 BIBLIOGRAFÍA	 121

INTRODUCCIÓN

Para tener éxito hoy en día las organizaciones y los directivos deben de identificar y gestionar el riesgo. En cada organización la dirección y el consejo de administración requieren conocer cual es la exposición al riesgo de la entidad de la cual son responsables; por lo que es de gran importancia que ésta pueda realizar un análisis de los factores que generan los riesgos, ya sean de carácter interno o externo, a partir de tener una herramienta oportuna que le permita reaccionar adecuadamente si los riesgos no son controlables por la dirección.

Una de las actuaciones de análisis y supervisión de riesgos más efectivas está constituida por la realización de auditorias, herramientas fundamentales para la comprobación del cumplimiento de los planes de Seguridad y base de la mejora permanente de los mismos.

DEFINICIÓN DEL PROBLEMA

Por la situación anterior, la elevada importancia del centro de cómputo obliga a tener una administración de riesgos y dado que una vez realizada una inspección se pudo comprobar que en el centro de cómputo de la Facultad de Contaduría y Ciencias Administrativas de la Universidad Michoacana de San Nicolás de Hidalgo no se cuenta con un sistema de administración de riesgos, se entiende lo importante que es contar con una, puesto que los riesgos tanto humanos (como robo de información, daño de los equipos de cómputo y mal manejo de la información) como tecnológicos (fallas en el cableado, terremotos, incendios, descarga eléctrica, etc.) están a la orden del día, los cuales pueden ocasionar problemas de gran importancia en el andar de la organización, dichos problemas pueden ser causados voluntaria o involuntariamente; asimismo saber: ¿es factible minimizar los riesgos del centro de cómputo de la FCCA mediante una propuesta de administración de riesgos?

OBJETIVO GENERAL

Desarrollar esta propuesta de la implantación de un sistema de Administración de Riesgos en el centro de cómputo de la Facultad de Contaduría y Ciencias Administrativas, para en un corto, mediano y largo plazo obtener el mejor aprovechamiento de los recursos con los que cuenta la entidad y por ende una mejor administración de la información para la toma de decisiones, de esta manera estar prevenidos a percances y no se tendrán pérdidas financieras.

OBJETIVOS ESPECÍFICOS

- Recopilar información sobre las actividades administrativas que desarrolla la empresa mediante la aplicación de entrevistas a los empleados y jefes de la misma.
- Establecer los procedimientos a usarse para la prevención, evaluación y control de los puntos débiles y vulnerabilidades mediante formatos.

FORMULACIÓN DE HIPÓTESIS

Con la implementación de un sistema de Administración de Riesgos en el centro de cómputo de la Facultad de Contaduría y Ciencias Administrativas se obtendrían de manera eventual ciertos beneficios que a un plazo mayor beneficiarían a la Facultad en general.

JUSTIFICACIÓN

Ya que, en el centro de cómputo es donde se concentran todos los recursos necesarios para el procesamiento de la información y distribución de la misma y que además su función primordial es complementar la labor administrativa para hacerla más segura, fluida y así simplificar; y que el centro de cómputo es responsable de centralizar, custodiar y procesar la

mayoría de los datos con los que operan la empresa. En base a estos procedimientos del centro de cómputo y una vez procesada la información se tomarían de manera más acertada y a tiempo las decisiones que llevarán a la empresa a un mejor desempeño. Estos beneficios abarcarían en mayor medida el ámbito financiero y administrativo.

MARCO TEÓRICO

CAPITULO I: ADMINISTRACIÓN DE RIESGOS

Generalidades de la administración de riesgos

Considerando que dentro de las operaciones comerciales de una compañía, en ocasiones se suscitan riesgos de negocio que implican una serie de actividades o eventos inciertos externos (ambiente como son: las acciones de los competidores, clientes, legisladores, gobiernos, grupos de intereses especiales, otros, las variables: tasas de interés, inflación cambios reglamentarios, demanda en el mercado, oferta de mano de obra, posibles eventos catastróficos: tormentas, terremotos, guerra, terrorismo, otros) e internos (relativas al desarrollo adecuado de las marcas, a la atención a clientes, al número de proveedores, a los empleados, al cumplimiento de objetivos mediante los procesos operativos, el uso adecuado de las tecnologías, los posibles eventos que interrumpirían las actividades como son: las practicas poco éticas, fraudes, actos ilegales y pérdida del control de negocios) que afectan adversamente la capacidad de una organización para ejercitar exitosamente sus estrategias y alcanzar sus objetivos.

Ante tales riesgos que afectan la estrategia, los procesos y la información de una empresa la Administración de Riesgos de Negocio presenta una forma integrada y sistemática de identificar todos los recursos de dichos riesgos y responder ante ellos.

Por tanto, la Administración de riesgos puede ser definido como el proceso de identificación y gestión global de los riesgos clave del negocio con el objeto de mitigar la exposición total de la empresa.

Este proceso busca alinear la estrategia, los procesos, las personas, la tecnología y el conocimiento con el propósito de evaluar y administrara las incertidumbres que la empresa

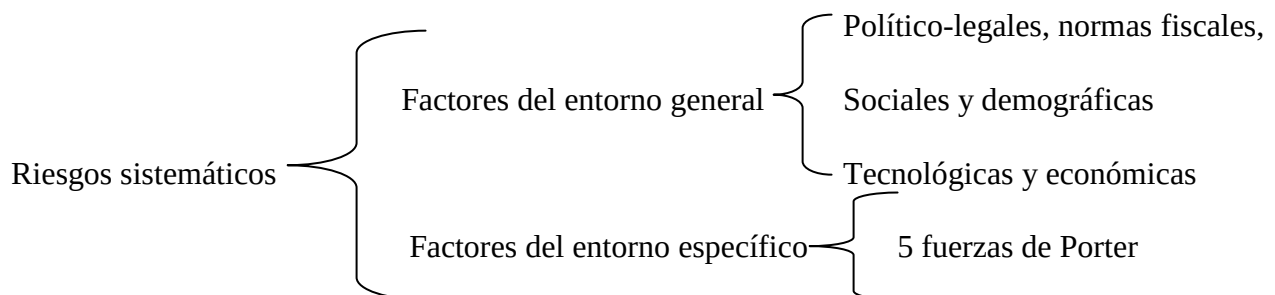
enfrenta al crear valor. Primero, equipa a los responsables asignados a dicho proceso con un marco útil para definir las tareas esenciales de administración de riesgos. En segundo lugar, es un proceso sistemático para construir y mejorar todas las capacidades de administración de riesgos, el cual, conforme va evolucionando, proporciona la plataforma de lanzamiento para una verdadera administración integral de riesgos.

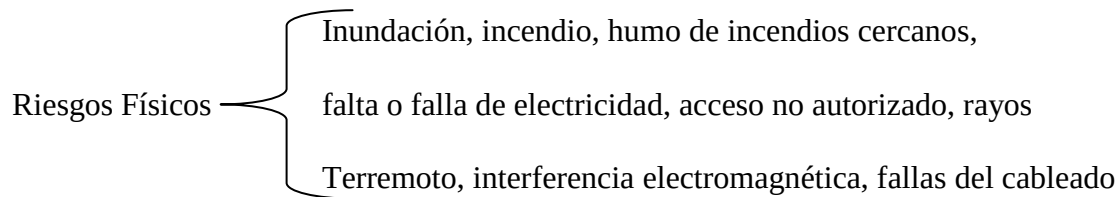
Riesgo sistemático. Se le conoce como riesgo de mercado y está asociado con los cambios en la economía a causa de factores internos o externos. Este tipo de riesgos no se puede compensar con la adquisición de una cierta diversidad de acciones porque todas están en las mismas condiciones.

El riesgo no sistemático. Se debe a factores propios o internos de la empresa es único para ella e independiente de los factores, económicos, políticos o sociales, a estos se asocian los cambios tecnológicos, competencia, huelgas. En este tipo de riesgo es posible compensar sus efectos comprando acciones de diversas empresas, de manera que si una acción se ve afectada por una causa negativa, se espera que a las otras no les suceda lo mismo y se pueda compensar el efecto negativo.

Definición de Riesgo.

Álvaro Soldano (2009). Define al riesgo como: La probabilidad de que ocurra algún hecho indeseable. El riesgo está relacionado con su entorno y con factores como:





Riesgos Humanos.

Riesgos en equipos de información.

Se puede definir el entorno como el conjunto de hechos y factores externos a la empresa relevantes para ella, con los que interacciona y sobre los que puede influir pero no controlar, que se concretan en un conjunto de normas y relaciones establecidas que condicionan su actividad.

El papel del entorno en la vida de la empresa es tal, que incluso algunos autores le dan la categoría de ser uno más de sus elementos, junto con el elemento humano, el capital y la organización.

Dado el grado de interrelación que existe entre la empresa y el entorno, esta deberá tener una actitud de análisis permanente del entorno para identificar a tiempo las repercusiones que tiene en ella. Así, este análisis le permitirá:

- a) Detectar a tiempo las oportunidades y amenazas que el entorno presenta para su supervivencia, lo que le permitirá que pueda aprovechar las primeras y facilitará que transforme las amenazas en oportunidades.
- b) Identificar los cambios internos que tiene que poner en marcha para mejorar su relación con el entorno y facilitar su adaptación a él.

El primer aspecto a abordar en el análisis del entorno es reconocer y clasificar los factores que en él se manifiestan. Así, se suele distinguir entre los factores que afectan de forma general o global a todas las empresas y los que afectan de forma específica a cada una. Estos dos grupos de factores conforman el entorno general y el entorno específico.

- I) Entorno general. Engloba los factores que reflejan las grandes tendencias de la realidad exterior de la empresa. Son los factores más alejados de la empresa sobre los que su capacidad de influir es mínima. Estos factores afectan, más o menos directamente, a todas las empresas.
- II) Entorno específico. Los factores del sector en el que opera cada empresa y por lo tanto inciden directa e inmediatamente en ellas. Al tratarse de factores más cercanos, la empresa puede ejercer alguna influencia sobre ellos.

LOS FACTORES DEL ENTORNO GENERAL

Factores político-legales.

Son los referentes a todo lo que implica una posición de poder en nuestra sociedad, en sus diferentes niveles (Estado, Comunidades Autónomas y Corporaciones Locales), que tendrán una repercusión económica. Se incluyen en ellos elementos como:

- a) El sistema institucional. Influirá decisivamente en la empresa el grado de poder y de proximidad a ella que tenga cada uno de los niveles del Estado.
- b) Las ideologías y partidos políticos relevantes. Dependiendo de la ideología del partido político que esté en el poder se establecerán unas directrices u otras respecto a aspectos

relacionados con el aumento de empleo, tipos de contratos, subvenciones, impuestos, etc. y esto repercutirá en la empresa.

- c) La estabilidad y riesgos políticos. Una empresa de un país caracterizado por una estabilidad política, tendrá una mayor estabilidad económica que aquella que esté en un país políticamente inestable.
- d) El marco exterior. Se engloban en él aspectos como las tendencias de integración supranacional, emergencia de nuevos países desarrollados, acuerdos internacionales, relaciones Este-Oeste y Norte-Sur y guerras y conflictos en el mundo.
- e) La legislación que afecta a la empresa. Se refiere al conjunto de normas jurídicas que ordenan la actividad de la empresa. Dada la entidad del tema, se le dedica un apartado especial más adelante. La actividad reguladora de la economía por parte del Estado y las Comunidades Autónomas se concreta en las normas jurídicas que dictan, la legislación, que son de obligado cumplimiento desde que son publicadas en los correspondientes Boletines Oficiales (BOE o BOA).

La actividad legisladora del Estado abarca todos los campos necesarios para regular la convivencia social. Los campos que más específicamente afectan a las empresas son el fiscal, el mercantil y el laboral, aunque ha de quedar claro que no son los únicos y que puede haber legislación en campos más generales que afectan también a la actividad empresarial, piénsese por ejemplo en la importancia de temas como el de la comunidad o separación de bienes en el matrimonio a la hora de exigir el pago de deudas al empresario, el de la contaminación o el de la responsabilidad civil o penal.

A continuación se da una panorámica de las normas legales que más afectan a las empresas en los tres campos citados. La relación no pretende ser exhaustiva, habiéndose seleccionado

únicamente la más significativa y válida para todo tipo de empresas, ni entra en detalles ya que no es el objeto de la asignatura. Además, la selección hecha únicamente se refiere a los aspectos fiscales, mercantiles y laborales, sin considerar las fuentes y normas legales generales que también afectan a la empresa.

Hay que destacar también que las normas que se citan aquí hacen referencia únicamente a la empresa en funcionamiento. Los trámites para su constitución y puesta en marcha se explican en otros temas de la asignatura.

Normas fiscales

- a)** Pagar los tributos que le afecten.
- b)** Repercutir a los clientes los impuestos indirectos que correspondan.
- c)** Hacer las correspondientes retenciones a cuenta del Impuesto a la Renta Personal. cuando pague rendimientos del trabajo o del capital a terceros.
- d)** En el caso de los impuestos indirectos hacer periódicamente las liquidaciones correspondientes con Hacienda y en el caso de las retenciones a cuenta en los directos realizar los correspondientes ingresos en Hacienda.
- e)** Llevar los libros de registro obligatorios para cada impuesto, en función del régimen al que se esté acogido y de las características jurídicas de cada empresa: libros registros del IVA de facturas emitidas y recibidas, en unos casos, libros registros de ingresos y gastos, de bienes de inversión... Estos libros se legalizan en Delegación de Hacienda.

Normas mercantiles

- a)** Seguir el Plan General de Contabilidad Llevar una contabilidad ordenada y adecuada que permita el seguimiento cronológico de sus operaciones y elaborar periódicamente balances e inventarios.
- b)** Llevar los libros contables obligatorios establecidos por el Código de Comercio: libro Diario y libro de Inventarios y Cuentas Anuales (las Cuentas Anuales son: el Balance, la Cuenta de pérdidas y ganancias y la Memoria), así como los que establezcan otras disposiciones especiales como por ejemplo el libro de Actas para las sociedades sujetas al Impuesto sobre Sociedades.
- c)** Llevar aquellos libros que exijan las normas reguladoras de las diferentes formas jurídicas de sociedades como por ejemplo en las sociedades anónimas el libro Registro de acciones nominativas o el de Socios en las sociedades limitadas.
- d)** Potestativamente, la empresa podrá llevar cuantos libros auxiliares quiera.
- e)** Legalizar los libros obligatorios en el Registro Mercantil y, si se desea, los voluntarios.
- f)** En el caso de sociedades, publicitar las Cuentas Anuales mediante depósito en el Registro Mercantil.
- g)** Auditar las Cuentas Anuales, si la empresa esta obligada.
- h)** Conservar durante seis años los libros, correspondencia y justificantes.

Normas laborales.

- a)** Pagar las cuotas empresariales a la Seguridad Social.
- b)** Afiliar los trabajadores a la Seguridad Social y comunicar altas, bajas y modificaciones.
- c)** Contratar a los trabajadores según los diferentes tipos de contratos existentes, y una vez firmado entregarlo en el Registro Nacional de Empleos.

- d)** Pagar a sus trabajadores las nóminas según lo pactado en convenios colectivos y contratos, y efectuar la retención a cuenta del IRPF y la retención para la Seguridad Social.
- e)** Llevar el libro de matrícula del personal y el de visitas de la Inspección de Trabajo. (No es obligatorio desde 2002.)
- f)** Respetar y exponer el calendario laboral.
- g)** Poner los medios necesarios para prevenir los riesgos laborales.
- h)** Contratar los servicios de una Mutua de Accidentes de Trabajo.

Factores sociales y demográficos.

Son los relativos a los aspectos y modelos culturales así como a las características demográficas de una sociedad. Destacaremos los siguientes:

- a)** Valores y creencias básicas de la sociedad. Como las actitudes respecto al consumo, al ocio, al trabajo, a la conservación del medio ambiente, hacia la empresa, el clima de relaciones laborales... influirán en las empresas ya que según el concepto que se tenga de estos aspectos, se potenciarán más o menos. Debe destacarse la importancia que actualmente tienen el medio ambiente y los valores ecológicos implicando directamente a las empresas, las cuales tienden a elaborar políticas de cambio (se recicla el papel, se evita la contaminación, los residuos, basuras). A mayor rapidez de adaptación mayores ventajas.
- b)** Las modas y los estilos de vida. La empresa se verá afectada por los cambios en los modos de vida de la sociedad y tendrá que adecuar su actividad a ellos. Por ejemplo, los

modelos culturales en los que se da mucha importancia a la imagen pueden obligar a un cambio en el aspecto externo de la empresa, que se manifestará a través del diseño de sus instalaciones, en los logotipos, en la imagen de marca etc.

- c) Las variables demográficas. El volumen de población y su composición por sexo y edad, la natalidad, la mortalidad, la nupcialidad, la tasa de actividad, las migraciones etc. ocasionarán oportunidades de negocio o amenazas para la empresa.

Factores tecnológicos.

Son los derivados de los avances científicos y son estimulados por las consecuencias económicas favorables del empleo de la tecnología como instrumento para competir. Las empresas que se incorporen al cambio técnico verán incrementada su eficiencia y como consecuencia sus beneficios a largo plazo aumentarán. Entre los factores tecnológicos destacan los referentes a:

- a) Nuevos materiales, productos o procesos de producción.
- b) Mejoras en el transporte de las personas y mercancías.
- c) Avances en los medios informáticos y en las telecomunicaciones.
- d) Know-How sobre la tecnología y las técnicas de gestión que precisa la empresa.

Factores económicos.

Son los que afectan a las relaciones de producción, distribución y consumo de una empresa, es decir, a la forma en que la sociedad decide usar los recursos.

De entre todos que afectan a la empresa, los más significativos son:

a) La política fiscal. Es la actuación del Estado sobre la economía mediante decisiones referentes al gasto público y a los impuestos.

- Decisiones sobre el gasto público. Una política expansiva aumentará los gastos públicos traduciéndose en un aumento de la demanda agregada, ya que el Estado para prestar sus servicios demandará los servicios del sector privado, además, de una forma indirecta, hará que la renta de muchos particulares aumente, aumentando, por lo tanto, la capacidad de consumo de los mismos (por ejemplo pensionistas y parados). Si la política es restrictiva y el gasto disminuye ocurrirá el proceso contrario.
- Decisiones sobre los impuestos. Si se lleva a cabo una disminución de los impuestos se producirá un aumento de los beneficios de las empresas, y, por tanto, un aumento de la inversión, lo que puede provocar un incremento de la producción y del empleo y por lo tanto un aumento del consumo privado al aumentar la renta de los particulares. Si los impuestos aumentan sucederá lo contrario.

b) La política monetaria. Es el control que hace el Banco Central Europeo sobre la cantidad de dinero en circulación mediante el control del tipo de interés.

Si crecen los tipos de interés se encarecerán los préstamos y a las empresas les sea más caro obtener financiación para llevar a cabo sus planes de inversión, además se incentivará el ahorro al ser remunerado mejor y se reducirá el consumo, por lo que la demanda de productos de las empresas disminuirá y por lo tanto disminuirá el empleo. Si los tipos de interés bajan se producirá el efecto contrario.

- c) La inflación. Es el crecimiento continuo y generalizado de los precios de los bienes y servicios. Influirá en la economía y como consecuencia en las empresas. La inflación no repercute sobre todas las empresas por igual, sino que puede perjudicar a unas más que a otras en función de cómo consigan minimizar los siguientes efectos negativos:
- Provoca un aumento de los costes de los factores. Como consecuencia, las empresas de aquellos países que tengan una inflación elevada serán menos competitivas que las de los países sin inflación y respecto a las del país que tengan una estructura de costes no tan afectada por ella.
 - Genera incertidumbre. A mayor grado de incertidumbre, las empresas tendrán dificultades en su planificación, desconocerán cuánto les costará producir determinados bienes y a cuánto podrán venderlos, así los planes a largo plazo se verán más afectados, reduciéndose la inversión.
- d) El tipo de cambio. Es el precio de una moneda expresado en otra. Los tipos de cambio afectan a aquellas empresas que se relacionan con el exterior en la compra-venta de los productos. Si el euro se deprecia, los bienes que producen las empresas españolas son más baratos en el extranjero y los bienes extranjeros son más caros en el mercado nacional; como consecuencia las exportaciones se elevan y disminuyen las importaciones. Esto repercute en la economía de nuestro país y en las empresas que lo forman. Si el euro se aprecia ocurrirá el fenómeno contrario.
- e) El ciclo económico. Consiste en las fluctuaciones económicas de la producción total, el PIB, acompañada de fluctuaciones de la mayoría de las variables económicas entre las que cabe destacar el nivel de desempleo y la tasa de inflación.

Un ciclo económico tiene varias fases y en cada una de ellas la repercusión en la actividad económica y como consecuencia en las empresas será diferente. Estas repercusiones se pueden resumir así:

- *Depresión o fondo*: Se producirá una disminución de las ventas y como consecuencia de los beneficios de la empresa, a causa de la estrechez de la demanda.
- *Recuperación o expansión*: En esta fase se produce un aumento de los gastos produciéndose un aumento de la demanda y de las ventas de las empresas y, por tanto, de sus beneficios. Debido a esto, las expectativas serán más favorables animándose la inversión.
- *Auge o cima*: En esta fase al haber aumentado tanto la producción se producirán rigideces en la oferta de ciertas materias primas con la que cada vez será más difícil aumentar la producción, que sólo lo hará mediante nuevas inversiones que eleven la productividad de los recursos ya empleados.
- *Recesión*: Al disminuir las ventas, los precios y los beneficios caerán, se producirá una disminución de las inversiones y algunas empresas empezarán a quebrar ya que la capacidad productiva no usada aumentará. Esta dinámica de recesión conducirá a un período de depresión generalizada que llevará de nuevo a la primera fase de depresión.

LOS FACTORES DEL ENTORNO ESPECÍFICO

Dentro de los riesgos socioeconómicos encontramos los del entorno específico de la empresa, y dicho entorno está formado por aquel conjunto de factores que afectan a ésta de forma directa en función del sector en el que actúe. La empresa debe observar atentamente la evolución de su sector para así conocer los cambios que se están produciendo en las fuerzas competitivas

del mismo y en la presión competitiva existente, puesto que de la competencia en el sector van a depender los beneficios de la empresa y su rentabilidad.

M. Porter (1980) establece las siguientes cinco fuerzas competitivas que determinan el grado de rivalidad entre las empresas de un sector.

- 1) Grado de rivalidad existente entre los competidores actuales.
- 2) Amenaza de entrada de nuevos competidores.
- 3) Amenaza de productos sustitutivos.
- 4) Poder negociador de los proveedores.
- 5) Poder negociador de los clientes.

Grado de rivalidad existente entre los competidores actuales.

La rivalidad entre los competidores actuales lleva a las empresas a utilizar estrategias en precios, publicidad, nuevos productos, mejora en el servicio, etc. para mejorar su posición en el sector. Pero en la mayoría de los sectores económicos, las medidas que toma una empresa son fácilmente observables por las empresas competidoras y dan lugar a la puesta en marcha por parte de las empresas rivales de medidas contrarrestadoras.

Algunas formas de competir pueden ser perjudiciales para todo el sector, desde el punto de vista de la rentabilidad. Por ejemplo, si se bajan los precios de los productos, para que la rentabilidad sea la misma deberá compensarse con una reducción en los costes o con una inferior calidad del producto, etc. Además, la bajada de los precios es rápida y fácilmente igualable por los competidores y, una vez igualada, disminuyen los ingresos para todas las empresas, a menos que sea compensada con un aumento considerable en la demanda del producto. Por el contrario, otras formas de competir, como las campañas publicitarias, pueden ampliar la demanda o aumentar la diferenciación del producto en el sector económico para beneficio de todas las empresas.

El grado de rivalidad establecida entre las empresas depende de los siguientes factores:

- a)** El número de competidores en el sector. Cuantas más empresas haya en el sector el grado de competencia será mayor.
- b)** Las posibilidades de crecimiento del sector. La rivalidad entre competidores será mayor a medida que el sector vea disminuir su tasa de crecimiento, puesto que unas empresas sólo podrán crecer a costa de la cuota de mercado de las otras.
- c)** La existencia de costes fijos elevados. Si existen costes fijos elevados las empresas tendrán que trabajar a plena capacidad para que su peso en los costes unitarios sea la menor posible; así pues, la oferta en el mercado aumentará, creciendo la competencia entre empresas.
- d)** La diferenciación del producto. A menor diferenciación de productos mayor competencia puesto que los compradores cambiarán de vendedor sin notar diferencias en el producto.
- e)** El exceso de capacidad productiva. Si existe un exceso de capacidad productiva en el sector la oferta será mayor que la demanda y la rivalidad será mayor entre las empresas.
- f)** Existencia de intereses estratégicos de las empresas. La rivalidad será mayor cuanto más interés, por motivos estratégicos, tengan éstas en estar presentes en el sector.
- g)** La existencia de fuertes barreras de salida de un sector. La intensidad de la competencia será mayor en sectores en los que haya factores que impidan a las empresas abandonar el sector tales como la posesión por parte de las empresas de activos muy especializados de difícil venta o reutilización; barreras emocionales como la lealtad a los empleados, por identificación con el negocio, por temor por la propia carrera, por orgullo etc.

Amenaza de entrada de nuevos competidores.

Si en un sector entran nuevas empresas la competencia aumentará y provocará una bajada en la rentabilidad ya que, por un lado, obligará a bajar los precios y, por otro, producirá un aumento en los costes, puesto que si las empresas desean mantener o aumentar su cuota de mercado deberán incurrir en gastos adicionales, como campañas publicitarias, reestructuración de su red de transportes, etc.

La amenaza de entrada de nuevos competidores en un sector depende de:

- a) Barreras para la entrada. Tales como la necesidad de grandes inversiones para instalarse.
- b) La dificultad de acceso a canales de distribución, el know-how necesario, la diferenciación del producto, los requisitos exigidos por la Administración etc.
- c) Reacción esperada. La reacción que las nuevas empresas esperen que tengan las empresas ya instaladas, de cara hace más difícil su entrada o permanencia en el sector afectará también a la posibilidad de nuevos ingresos.

Amenaza de productos sustitutivos.

La entrada de productos sustitutivos en el mercado hará que los precios bajen para hacer frente a la competencia efectuada y por lo tanto baje también la rentabilidad del sector.

Que los nuevos productos reemplacen a los ya existentes en el mercado dependerá de la relación existente entre las prestaciones y el precio de los nuevos productos y de los ya existentes. Para proteger su producto, las empresas del sector deberán intentar diferenciarlo de los otros

modificando su imagen ante el público, mejorando la relación prestaciones/precio e intensificando su política comercial.

Poder de negociación de los proveedores.

Los proveedores pueden aumentar su poder de negociación sobre las empresas de un sector amenazando con elevar los precios o reducir la calidad de los productos o servicios, con lo que la rentabilidad del sector comprador disminuiría.

El poder de negociación que tengan los proveedores dependerá de los siguientes factores:

- a) El grado de concentración del sector de los proveedores. Cuantos menos proveedores existan su capacidad de negociación será mayor.
- b) Que no existan productos sustitutivos para la venta en su sector. Es decir, que el cliente sólo pueda comprar ese producto y no otro.
- c) Que la empresa no sea un cliente importante del proveedor. Cuanto menor sea el cliente menos capacidad de negociación tendrá frente al proveedor.
- d) Que los proveedores vendan un producto que sea un *input* importante para el negocio del comprador. Es decir, que la actividad del cliente dependa del producto ofrecido por el proveedor.
- e) Que los productos del grupo proveedor estén diferenciados o requieren costes elevados por cambio de proveedor. La diferenciación de productos siempre conlleva la fidelización del cliente. Por otro lado si cambiar de proveedor lleva aparejados costes importantes al cliente no le queda más remedio que seguir con el mismo proveedor.
- f) Que el proveedor represente para el cliente una amenaza real de integración vertical hacia delante. La posición de fuerza del proveedor frente al cliente será tanto mayor cuanto más

fácil sea que aquel pueda entrar a operar como competidor en el mismo sector del cliente con lo que ya no lo necesitaría como comprador.

Debe recordarse que lo anteriormente dicho no es sólo aplicable a empresas suministradoras sino también a la mano de obra, que es proveedora de trabajo y puede ejercer un gran poder negociador en muchos ramos, como es el caso de sectores con escasez de mano de obra o de mano de obra muy especializada o fuertemente sindicalizada.

Poder negociador de los clientes.

Los compradores pueden forzar la competencia entre las empresas del sector exigiendo bajadas de precios, mejoras en la calidad o mayores servicios por parte de los vendedores. Su poder negociador depende de los siguientes factores:

- a) El grado de concentración de los compradores y el volumen de sus compras en relación con las ventas totales del proveedor. Si hay pocos clientes y compran gran parte de la producción su poder será mayor.
- b) La importancia de los productos comprados en la estructura de costes del comprador. Cuanto más importantes sean, la presión que ejercerá el comprador al vendedor buscando mejores condiciones de venta será mayor.
- c) La importancia que el producto comprado tenga para la calidad de los productos o servicios del comprador. Cuanta mayor importancia tenga, la sensibilidad a los precios por parte del comprador será menor.
- d) La rentabilidad y margen del cliente. Cuanta menor rentabilidad obtenga en su actividad más presión hará para comprar en mejores condiciones.

- e) La diferenciación de los productos. A menor diferenciación mayor será la presión que podrá ejercer el cliente al vendedor ante la amenaza de acudir a otro vendedor.
- f) La existencia de bajos costes de cambio de proveedor. Cuanto más fácil sea cambiar de proveedor más posibilidades de éxito tendrán las exigencias del cliente.
- g) La posibilidad de integración vertical hacia atrás. Cuanto más real sea la amenaza de que el cliente pueda pasar a fabricar el producto que compra, su poder negociador será mayor.
- h) La información que el cliente tenga sobre el mercado. Cuanta más información tenga el cliente y más transparente consiga que el mercado sea para él, podrá conseguir mejores condiciones de compra.

EL ANÁLISIS DAFO

Acrónimo de DEBILIDADES-AMENAZAS-FORTALEZAS y OPORTUNIDADE (SWOT en inglés: Strengths, Weakness, Opportunities and Treats), es una especie de “CONOCETE a TI MISMO” empresarial. Se realiza en todo tipo de proyectos empresariales: creación de nuevas empresas, lanzamiento de productos, planes de mejora, etc. Hoy en día se emplea más que el otro tipo de análisis empresarial más común y que se trata en el siguiente apartado, el del “Núcleo competitivo” de M. Porter.

- ✓ Los puntos débiles o DEBILIDADES de una empresa son los aspectos internos que suponen una desventaja comparativa frente a empresas competidoras.
- ✓ Los puntos fuertes, FORTALEZAS son aquellos aspectos positivos internos de la empresa que suponen una ventaja comparativa frente a empresas competidoras.

Las fortalezas y debilidades (análisis interno) resultan importantes puesto que pueden ayudarnos a entender la posición competitiva de nuestra empresa en un entorno de negocio concreto. Suelen ser aspectos relativos a las propias capacidades de los promotores, que condicionan de alguna forma el planteamiento del proyecto y juegan generalmente a presente. Deben compararse con el ambiente competitivo que rodea a nuestra empresa. Cada empresa ha de decidir cuáles son las variables (factores críticos de éxito -FCE-) apropiadas a utilizar según los mercados y segmentos en los que compete.

Ejemplos:

- Capacidades/Incapacidades en actividades clave (directiva, comercial, de gestión, ...)
- Recursos financieros adecuados/inadecuados
- Habilidades y recursos tecnológicos superiores/peores
- Propiedad o no de la tecnología principal.
- Ventajas/desventajas en costes.
- Programas de I+D.
- Imagen en los consumidores buena o inexistente.
- Líder en el mercado o seguidor.
- Conocimiento/desconocimiento del negocio
- Existencia o no de una red de distribución
- Cartera de productos
- Instalaciones preexistentes, eficientes u obsoletas.
- etc.

✓ Las amenazas, son situaciones del entorno que si no se afrontan, pueden situar a la empresa en peor situación competitiva. Ejemplos:

- Entrada de nuevos competidores con costes más bajos.
- Incremento en ventas de productos sustitutivos.
- Crecimiento lento del mercado.
- Cambio en las necesidades y gustos de los consumidores.
- Incremento de barreras y requisitos reglamentarios costosos.
- Creciente poder de negociación de clientes y/o proveedores, etc.

✓ Las oportunidades son situaciones del entorno que aprovechándolas pueden permitir mejorar la situación competitiva de la empresa. Por ejemplo:

- Posibilidad de entrar en nuevos mercados o segmentos.
- Posibilidad de atender a grupos adicionales de clientes.
- Ampliación de la cartera de productos para satisfacer nuevas necesidades.
- Crecimiento rápido del mercado.
- Diversificación de productos relacionados.
- Eliminación de barreras comerciales en mercados exteriores atractivos.
- Nuevas líneas de apoyo institucional, etc.

Estas *Oportunidades* y *Amenazas* (análisis externo) son siempre aspectos relativos a la evolución del entorno, que condicionan de alguna forma la viabilidad del negocio y actúan en general como tendencia, es decir, juegan en cierto modo a futuro. Suelen ser, en general:

- Aspectos legislativos (regulaciones, necesidad de homologaciones).

- Aspectos socioculturales (hábitos de vida, modas).
- Aspectos demográficos (evolución de la pirámide de población, aspectos migratorios).
- Aspectos económicos (renta disponible, etc.).
- Aspectos políticos (liberalización del comercio, barreras arancelarias u otro tipo de proteccionismo nacional).
- Aspectos tecnológicos (avances técnicos).
- Posibles ventajas de situación, locales (especialización local o acceso a materias primas, proximidad al mercado u otra ventaja en costes).

EJEMPLO:

En la matriz DAFO se establecen 4 cuadrantes que reflejan las posibles estrategias a adoptar por la empresa:

FIGURA 1: Matriz DAFO

MATRIZ DAFO	PUNTOS FUERTES	PUNTOS DÉBILES
Oportunidades (O)	Estrategias OFENSIVAS (O/F) *Se usan las fuerzas del listado F para aprovechar las oportunidades (O)	Estrategias DE REORIENTACIÓN (O/D) *Se superan las debilidades (D) , aprovechando las oportunidades (O)
Amenazas (A)	Estrategias DEFENSIVAS (A/F) *Se evitan las amenazas (A) con las fuerzas (F)	Estrategias DE SUPERVIVENCIA (A/D) * Se busca reducir las debilidades y eludir las amenazas

El desarrollo práctico de la matriz se completa analizando de forma aislada cada cuadrante. Es decir, si se elige el primero (Puntos Fuertes-Amenazas) se tendrán que identificar cada uno de los puntos fuertes que la empresa en cuestión tiene y cada una de las amenazas que posee del exterior, de forma que cada intersección deberá ser analizada para estudiar las consecuencias y las acciones que de dicha situación puedan derivarse. Con esta información se podrá formular y orientar la futura estrategia, teniendo en cuenta las peculiaridades de la actividad e información económica de cada sector.

Esta reflexión debe ayudar a enfocar la estrategia del negocio (especialmente la reflexión sobre la necesaria combinación Oportunidad-Fortaleza, aunque también pueden establecerse estrategias que tiendan a corregir las Debilidades o defenderse de las Amenazas).

Lo que se pretende con esta matriz no es determinar qué estrategia sería la mejor, sino sólo contemplar y comparar las estrategias viables o, al menos, las más significativas.

Riesgos físicos:

- Inundación.
- Incendio.
- Humo proveniente del incendio de otros lugares cercanos
- Falta o falla de energía eléctrica.
- Accesos no autorizados o mal controlados como correspondería.
- Dependiendo de la ubicación, terremotos.
- Interferencia electromagnética que afecte la integridad de los datos que viajan por el cableado estructurado.

- Rayos.

- Fallas en el cableado estructurado por roedores u otras alimañas que pudieran comer o dañar el mismo.

Riesgos humanos:

- Que quede mal cerrada la puerta de acceso permitiendo acceso no autorizado.

- Que quede un servidor sin bloquear correctamente y que alguien pudiera tomar control físico del servidor.

- Robo de equipamiento.

- Sabotaje.

- Fallas en el software al aplicar parches sin haber testeado.

- Atentados.

- Manifestaciones con desmanes.

Riesgos del equipamiento informático / telecomunicaciones:

- Fallas generales de hardware (discos, placas de red, tarjetas madre, micrófonos, etc.)

- Fallas de equipos de comunicaciones.

- Fallas en el sistema de UPS o falta de mantenimiento de los mismos.

- Fallas en el software, bases de datos, etc.

DEFINICIÓN DE ADMINISTRACIÓN DE RIESGOS:

(Information Systems Audit and Control Association (ISACA) 2009): La Administración de Riesgos es el proceso de garantizar que el impacto de de las amenazas que explotan las vulnerabilidades estén dentro de límites y costos aceptables. En un enfoque general, este se logra mediante un equilibrio entre la exposición al riesgo y los costos de mitigación, así como la implementación de acciones preventivas y controles apropiados.

En este sentido, el riesgo es la probabilidad de que un incidente, evento o transacción ocasione pérdidas financieras o daños patrimoniales a la organización, su personal, sus activos o su reputación en general, lo cual se puede sintetizar en la siguiente fórmula:

Riesgo Total = Valor de activos x Amenazas x Vulnerabilidades.

CAPITULO II: PROBLEMAS MÁS COMUNES EN UN CENTRO DE CÓMPUTO

El objetivo principal del presente acápite consta en la preparación del alumno en la identificación plena y fácil de los principales y más comunes problemas que se presentan en un centro de cómputo tanto en el software, como en el hardware.

Hardware

Los principales problemas que se presentan con el HW, y los más comunes son:

- Defectos de fabricación y ó daños físicos que puedan tener durante su transporte.
- Que el manual de uso este en otro idioma ajeno al que manejamos.
- Las piezas que pudiera ser dañadas no son muy comunes y por tanto difíciles de conseguir.
- Cuando se trabaja con conexión a red, es muy común que por falta de conocimiento den órdenes que la puedan bloquear o provocar que ésta se caiga.
- Que las impresoras deben recibir trato especial porque la configuración de estas es muy específica.

Software

Los principales problemas que presenta el SW son entre otros:

- Los archivos necesarios para su instalación no están contenidos en el CD de instalación.
- El ambiente en que se desarrolla no es compatible con el sistema operativo que está siendo usado por el PC.

- El idioma, no siempre está en el que nosotros hablamos y por tanto nos es difícil su manejo.
- Algunas órdenes, comandos u operaciones son muy complejos y puede producir que al darlas de manera equivocada bloquee el equipo.
- El problema principal y más común que puede ser causa de más problemas que ningún otro factor es la falta de experiencia y la ignorancia.

Seguridad en los Accesos por Software

Siendo muchas las amenazas que pueden sufrir las computadoras y las redes, es muy variado el software disponible.

¿Los "malos"?	¿Los "buenos"?
Virus que infectan las aplicaciones.	Antivirus.
Sniffers que capturan los datos y contraseñas que circulan por una red.	Cortafuegos, que ejercen un control sobre los accesos al sistema.
Programas que revientan los passwords.	Herramientas para encriptar, codificar ficheros o mandar correo electrónico seguro.
Caballos de Troya que se instalan en nuestra computadora y toman el control	Programas que verifican la integridad de un sistema avisando cuando pasa “algo raro”.

Espías que se ocultan en la computadora e informan a terceros.

Programas que analizan los ficheros “.log” de acceso a un sistema.

Gusanos que saltan de computadora en computadora.

Detectores de vulnerabilidades que identifican puntos débiles de un sistema.

Los buenos y los malos son los usuarios no el software; imagine un software para detectar contraseñas, normalmente el informático de la empresa puede utilizarlo para detectar contraseñas de sus propios usuarios y avisar a aquellos que han puesto contraseñas fáciles de detectar. Pero también pueden utilizarlo un hacker para acceder a los documentos.

ANÁLISIS DE RIESGOS

Las empresas que utilizan sistemas de información llegan a ser, casi inevitablemente, dependientes de ellos, lo cual es un arma de doble filo, pues se corre el riesgo de que un fallo provoque el caos. Realizar un análisis de riesgos es el primer paso que debe darse para conseguir la seguridad adecuada. Permite detectar los puntos débiles sobre los que aplica o reforzar medidas de seguridad.

Principales riesgos

Los principales riesgos a los que se enfrenta un sistema, sus posibles consecuencias y medidas de seguridad son: los errores humanos, fallos de los equipos, robo de la información o equipos, virus, sabotaje, fraude, desastres naturales, entre otros.

Medidas de seguridad

- a) Medidas de seguridad activa. Son aquellas cuyo objetivo es anular o reducir los riesgos existentes o sus consecuencias para el sistema.
- b) Medidas de seguridad pasiva. Están destinadas a estar preparado si llega a producirse el desastre.

EL PLAN DE CONTINGENCIAS

El Plan de Contingencias constituye una presentación formal y responsable de acciones específicas a tomar cuando surja un evento o condición que no esté considerado en el proceso normal de operación de un centro de cómputo. Es decir, se trata de un conjunto de procedimientos de recuperación para casos de desastre; es un plan formal que describe pasos apropiados que se deben seguir en caso de un desastre o emergencia. Materializa un riesgo, ya que se pretende reducir el impacto de éste.

El Plan de Contingencia contempla tres tipos de acciones las cuales son:

- La Prevención, conformada por el conjunto de acciones a realizar para prevenir cualquier contingencia que afecte la continuidad operativa, ya sea en forma parcial o total, del centro de cómputo, las instalaciones auxiliares, recursos, información procesada, en tránsito y almacenada. De esta forma se reducirá su impacto, permitiendo restablecer a la brevedad posible los diferentes servicios interrumpidos
- Detección. Deben contener el daño en el momento, así como limitarlo tanto como sea posible, contemplando todos los desastres naturales y eventos no considerados.
- Recuperación. Abarcan el mantenimiento de partes críticas entre la pérdida del servicio y los recursos, así como su recuperación o restauración.

Introducción

Manuel Aranda Ogayar (2004). Para tener éxito hoy en día las organizaciones y los directivos deben de identificar y gestionar el riesgo. En cada organización la dirección y el consejo de administración requieren conocer cual es la exposición al riesgo de la entidad de la cual son responsables; por lo que es de gran importancia que ésta pueda realizar un análisis de los factores que generan los riesgos, ya sean de carácter interno o externo, a partir de tener una herramienta oportuna que le permita reaccionar adecuadamente si los riesgos no son controlables por la dirección.

Para esto proponemos realizar un análisis de las técnicas que permitan conocer de una forma imparcial y lo suficientemente amplia, la validez de la organización y gestión que la organización mantiene en materia de Seguridad Integral, evaluando cada uno de los aspectos fundamentales que la determinan.

Una de las actuaciones de análisis y supervisión de riesgos más efectivas está constituida por la realización de auditorias, herramientas fundamentales para la comprobación del cumplimiento de los planes de Seguridad y base de la mejora permanente de los mismos.

Generalidades

A través de la historia el hombre convive con riesgos que pueden ser provocados por los fenómenos de la naturaleza, el desarrollo tecnológico desarrollado por él mismo, los actos malintencionados generados por los seres humanos y otros riesgos. Desde sus primeros pasos hasta el gran salto de la era industrial, en que las estructuras sociales se hacen extremadamente complejas, la convivencia con los riesgos se producía de forma natural.

A partir de la revolución industrial iniciada en el siglo diecinueve, las condiciones de producción y de la vida ciudadana en general crean y se ven expuestas a nuevos y más graves riesgos, que precisan de una respuesta acorde con la innovación y la importancia que entrañan.

En esa dinámica acelerada del desarrollo industrial, se alcanzan los años cincuenta del siglo veinte, cuando algunas empresas incorporan la función de la Gerencia de Riesgos, dedicada inicialmente a la compra y gestión de los seguros.

Con posterioridad, la Gerencia de Riesgos amplía su campo de acción, al asesoramiento en la decisión de otras políticas de la empresa en su estrategia corporativa y operacional, en particular en el aseguramiento y fiabilidad de los procesos y las acciones de seguridad como principales herramientas que contribuyen a garantizar la continuidad de las operaciones.

En la última década, tras las reformas del sistema financiero, se ha producido una verdadera revolución de los medios y formas con los que las empresas gestionan sus recursos financieros. La apertura es prácticamente total y en la mayoría de las empresas se utilizan con asiduidad toda la gama de instrumentos que se desarrollan de forma continua en los principales mercados, cuya globalización ha originado un grado de incertidumbre al que hasta hace muy poco no estábamos acostumbrados.

En paralelo, han ido surgiendo nuevos riesgos motivados por la utilización de estos mecanismos, cuyo efecto, en algunos casos, ha supuesto cuantiosas pérdidas en importantes entidades y el cuestionamiento de los directivos de las mismas. Los Consejos de Administración de numerosas empresas han empezado a tomar conciencia del problema y en algunos casos se ha decidido volver a los instrumentos tradicionales, mientras que en otros se ha optado por prepararse para gestionar el riesgo mediante adecuados sistemas de control interno.

En el contexto empresarial el riesgo puede definirse como: *"los factores, acontecimientos, tanto internos como externos, a que está expuesta la empresa, y que ponen en peligro la consecución de los objetivos"*.

La incertidumbre de los riesgos del negocio empresarial, especialmente cuando se acomete un proceso nuevo, se reduce con el análisis previo de los componentes directos y de los factores del entorno que puede influir en el desarrollo esperado.

Cuando nos referimos a los factores externos que representan riesgos para la empresa, porque pueden afectar su control interno, consideramos que hay que tener en cuenta que las condiciones existentes en el momento de diseñar las acciones que forman parte del proceso de control pueden cambiar, dejando de ser eficaz el sistema. Siendo necesario que al mismo tiempo que se identifiquen los riesgos, la empresa identifique los factores que van modificando los riesgos y la capacidad de la entidad para conseguir sus objetivos.

Existen situaciones de cambio permanente que con más frecuencia afectan la estabilidad de las empresas. Estas situaciones originan notables oportunidades y ventajas y, en paralelo, desequilibrios que causan algunos inconvenientes "planetarios", que se resumen en los siguientes, y cuya aparición requiere de una atención especial, para que se reevalúe el análisis de riesgos o para que se tomen medidas concretas, estas son:

- Cambios en el entorno operacional.
- Nuevas tecnologías.
- Nuevas actividades y nuevos productos.
- Nuevos sistemas de información.
- Crecimiento rápido.
- Rotación excesiva del personal.
- Avances tecnológicos.

- Internacionalización. Globalización.
- Vulnerabilidad de los mercados financieros.
- Desplazamiento de los poderes públicos por grandes grupos globales.
- Deterioro medioambiental. Cambio climático.
- Comunicaciones más capaces y más rápidas.
- Crecimiento demográfico descompensado.
- Movimientos migratorios masivos.
- Demandas sociales: consumidores, ecologistas, sindicatos.
- Tendencias socio-políticas extremas.
- Paraísos laborales. Deslocalización.

Para tener éxito hoy en día las organizaciones y los directivos deben de identificar y gestionar el riesgo de manera efectiva mediante controles internos.

En cada organización la dirección y el consejo de administración requieren conocer cual es la exposición al riesgo de toda la entidad de la cual son responsables, riesgo al que pudiéramos denominar "Riesgo Global o Riesgo de la Empresa".

En general, este, conceptualmente puede ser definido como la sumatoria de los riesgos de las diferentes unidades que integran la entidad; estos a su vez como la suma de los riesgos de cada una de sus áreas.

Es de gran importancia que la dirección pueda realizar un análisis de los factores que generan los riesgos, ya sean de carácter interno o externos, a partir de tener

una información oportuna que le permita reaccionar adecuadamente si los riesgos no son controlables por la dirección, por depender de factores externos sobre los que no es posible ejercer influencia.

Definición de Riesgo

Del concepto de riesgo, además de los ya expresados hay muchas acepciones y diferentes usos de éste término, defendidas por diferentes autores, y visto desde diferentes puntos de vista.

Entre las variadas formas de interpretar el riesgo, podemos encontrar:

- Contingencia o posibilidad de que suceda un daño, desgracia o contratiempo.
- Conjunto de circunstancias que pueden disminuir el beneficio.
- Exposición. Peligro, es una contingencia inminente o muy probable, en tanto que riesgo y exposición pueden expresar desde la mera posibilidad a diversos grados de probabilidad.
- Esta fase tiene por objeto la identificación del riesgo delimitando su contenido y alcance para diferenciarlo de otros riesgos. Se basa en la identificación específica de sus elementos característicos como son: el bien y el daño.

El sentido semántico del término riesgo, se aplica a toda situación en la que por la concurrencia de una serie de factores se puede llegar a producir un hecho no deseado, accidental. Los actores protagonistas de tal situación de riesgo pueden estar dados por la interrelación de determinados elementos, los cuales se muestran a continuación:

- Los peligros, como acontecimientos no deseados que pueden liberar unos agentes agresivos (fuentes dañinas).
- Los activos sobre los que pueden repercutir los agentes agresivos.

- Los efectos directos, consecuenciales y a largo plazo, que se pueden producir sobre los activos.

RIESGOS EN EL CENTRO DE CÓMPUTO

Es importante en toda organización contar con una herramienta, que garantice la correcta evaluación de los riesgos, a los cuales están sometidos los procesos y actividades que participan en el área informática; y por medio de procedimientos de control se pueda evaluar el desempeño del entorno informático.

Viendo la necesidad en el entorno empresarial de este tipo de herramientas y teniendo en cuenta que, una de las principales causas de los problemas dentro del entorno informático, es la inadecuada administración de riesgos informáticos, esta información sirve de apoyo para una adecuada gestión de la administración de riesgos, basándose en los siguientes aspectos:

- La evaluación de los riesgos inherentes a los procesos informáticos.
- La evaluación de las amenazas ó causas de los riesgos.
- Los controles utilizados para minimizar las amenazas a riesgos.
- La asignación de responsables a los procesos informáticos.
- La evaluación de los elementos del análisis de riesgos.

Los sistemas de información computarizados son vulnerables a una diversidad de amenazas y atentados por parte de:

- Personas tanto internas como externas de la organización.

- Desastres naturales.
- Por servicios, suministros y trabajos no confiables e imperfectos.
- Por la incompetencia y las deficiencias cotidianas.
- Por el abuso en el manejo de los sistemas informáticos.
- Por el desastre a causa de intromisión, robo, fraude, sabotaje o interrupción de las actividades de cómputos.

Todos estos aspectos hacen que sea necesario replantear la seguridad con que cuenta hasta ahora la organización, aunque también hay algunas entidades que están haciendo un trabajo prominente en asegurar sus sistemas informáticos.

Es fundamental que los directivos de las organizaciones que no se han ocupado lo suficiente en implementar un estricto sistema de seguridad se preocupen en:

- Reconocer la necesidad de establecer normas de seguridad para los datos, políticas, normas y directrices.
- Comprender que el papel que desempeñan en la organización, esta relacionado con la seguridad del ciclo de vida del sistema de información.
- Establecer una planificación formalizada para la seguridad informática.
- Gestionar los medios necesarios para administrar correctamente la función de la seguridad informática.

RIESGOS RELACIONADOS CON LA INFORMATICA

En efecto, las principales áreas en que habitualmente ha incursionado la seguridad en los centros de cómputos han sido:

- Seguridad física.
- Control de accesos.
- Protección de los datos.
- Seguridad en las redes.

Por tanto se ha estado descuidando otros aspectos intrínsecos de la protección informática y que no dejan de ser importantes para la misma organización, como por ejemplo:

- Organización y división de responsabilidades
- Cuantificación de riesgos
- Políticas hacia el personal
- Medidas de higiene, salubridad y ergonomía
- Selección y contratación de seguros
- Aspectos legales y delitos
- Estándares de ingeniería, programación y operación
- Función de los auditores tanto internos como externos
- Seguridad de los sistemas operativos y de red
- Plan de contingencia

Otro error es desconocer las relaciones existentes entre los elementos y factores de la seguridad. El resultado a todo esto es: "una perspectiva limitada de la seguridad informática para la organización".

A los fines de llevar una revisión completa y exhaustiva de este tema, se propone que los especialistas en seguridad informática apliquen un enfoque amplio e integral, que abarque todos los aspectos posibles involucrados en la temática a desarrollar, identificando aquellos

concernientes a garantías y resguardos, y, después de haber efectuado un análisis exhaustivo de los mismos, presentarlos en detalle y agrupados convenientemente.

Los principales riesgos informáticos de los negocios son los siguientes:

- **Riesgos de Integridad:** Este tipo abarca todos los riesgos asociados con la autorización, completitud y exactitud de la entrada, procesamiento y reportes de las aplicaciones utilizadas en una organización. Estos riesgos aplican en cada aspecto de un sistema de soporte de procesamiento de negocio y están presentes en múltiples lugares, y en múltiples momentos en todas las partes de las aplicaciones; no obstante estos riesgos se manifiestan en los siguientes componentes de un sistema:
 - *Interface del usuario:* Los riesgos en esta área generalmente se relacionan con las restricciones, sobre las individualidades de una organización y su autorización de ejecutar funciones negocio/sistema; teniendo en cuenta sus necesidades de trabajo y una razonable segregación de obligaciones. Otros riesgos en esta área se relacionan a controles que aseguren la validez y completitud de la información introducida dentro de un sistema.
 - *Procesamiento:* Los riesgos en esta área generalmente se relacionan con el adecuado balance de los controles detectivos y preventivos que aseguran que el procesamiento de la información ha sido completado. Esta área de riesgos también abarca los riesgos asociados con la exactitud e integridad de los reportes usados para resumir resultados y tomar decisiones de negocio.
 - *Procesamiento de errores:* Los riesgos en esta área generalmente se relacionan con los métodos que aseguren que cualquier entrada/proceso de información de

errores (*Exceptions*) sean capturados adecuadamente, corregidos y reprocesados con exactitud completamente.

- *Interface*: Los riesgos en esta área generalmente se relacionan con controles preventivos y detectivos que aseguran que la información ha sido procesada y transmitida adecuadamente por las aplicaciones.
 - *Administración de cambios*: Los riesgos en esta área pueden ser generalmente considerados como parte de la infraestructura de riesgos y el impacto de los cambios en las aplicaciones. Estos riesgos están asociados con la administración inadecuada de procesos de cambios organizaciones que incluyen: Compromisos y entrenamiento de los usuarios a los cambios de los procesos, y la forma de comunicarlos e implementarlos.
 - *Información*: Los riesgos en esta área pueden ser generalmente considerados como parte de la infraestructura de las aplicaciones. Estos riesgos están asociados con la administración inadecuada de controles, incluyendo la integridad de la seguridad de la información procesada y la administración efectiva de los sistemas de bases de datos y de estructuras de datos. La integridad puede perderse por: Errores de programación (*buena información es procesada por programas mal contruidos*), procesamiento de errores (*transacciones incorrectamente procesadas*) ó administración y procesamiento de errores (*Administración pobre del mantenimiento de sistemas*).
- **Riesgos de relación**: Los riesgos de relación se refieren al uso oportuno de la información creada por una aplicación. Estos riesgos se relacionan directamente a la información de toma de decisiones (*Información y datos correctos de una*

persona/proceso/sistema correcto en el tiempo preciso permiten tomar decisiones correctas).

- **Riesgos de acceso:** Estos riesgos se enfocan al inapropiado acceso a sistemas, datos e información. Estos riesgos abarcan: Los riesgos de segregación inapropiada de trabajo, los riesgos asociados con la integridad de la información de sistemas de bases de datos y los riesgos asociados a la confidencialidad de la información. Los riesgos de acceso pueden ocurrir en los siguientes niveles de la estructura de la seguridad de la información:
 - *Procesos de negocio:* Las decisiones organizacionales deben separar trabajo incompatible de la organización y proveer el nivel correcto de ejecución de funciones.
 - *Aplicación:* La aplicación interna de mecanismos de seguridad que provee a los usuarios las funciones necesarias para ejecutar su trabajo.
 - *Administración de la información:* El mecanismo provee a los usuarios acceso a la información específica del entorno.
 - *Entorno de procesamiento:* Estos riesgos en esta área están manejados por el acceso inapropiado al entorno de programas e información.
 - *Redes:* En esta área se refiere al acceso inapropiado al entorno de red y su procesamiento.
 - *Nivel físico:* Protección física de dispositivos y un apropiado acceso a ellos. Algunos de los métodos de prevenir el acceso ilegal a los servicios informáticos incluyen:
 - Claves y contraseñas para permitir el acceso a los equipos.

- Uso de cerrojos y llaves.
 - Fichas ó tarjetas inteligentes.
 - Dispositivos biométricos (Identificación de huellas dactilares, lectores de huellas de manos, patrones de voz, firma/escritura digital, análisis de pulsaciones y escáner de retina, entre otros).
- **Riesgos de utilidad:** Estos riesgos se enfocan en tres diferentes niveles de riesgo:
 - Los riesgos pueden ser enfrentados por el direccionamiento de sistemas antes de que los problemas ocurran.
 - Técnicas de recuperación/restauración usadas para minimizar la ruptura de los sistemas.
 - Backups y planes de contingencia controlan desastres en el procesamiento de la información.
-
- **Riesgos en la infraestructura:** Estos riesgos se refieren a que en las organizaciones no existe una estructura información tecnológica efectiva (*hardware, software, redes, personas y procesos*) para soportar adecuadamente las necesidades futuras y presentes de los negocios con un costo eficiente. Estos riesgos están asociados con los procesos de la información tecnológica que definen, desarrollan, mantienen y operan un entorno de procesamiento de información y las aplicaciones asociadas (*servicio al cliente, pago de cuentas, etc.*). Estos riesgos son generalmente se consideran en el contexto de los siguientes procesos informáticos:
 - *Planeación organizacional:* Los proceso en esta área aseguran la definición del impacto, definición y verificación de la tecnología informática en el negocio.

Además, verifica si existe una adecuada organización (*gente y procesos*) asegura que los esfuerzos de la tecnología informática será exitosa.

- *Definición de las aplicaciones:* Los procesos en esta área aseguran que las aplicaciones satisfagan las necesidades del usuario y soporten el contexto de los procesos de negocio. Estos procesos abarcan: la determinación de comprar una aplicación ya existente ó desarrollar soluciones a cliente. Estos procesos también aseguran que cualquier cambio a las aplicaciones (*compradas o desarrolladas*) sigue un proceso definido que confirma que los puntos críticos de proceso/control son consistentes (*Todos los cambios son examinados por usuarios antes de la implementación*).
- *Administración de seguridad:* Los procesos en esta área aseguran que la organización está adecuadamente direccionada a establecer, mantener y monitorizar un sistema interno de seguridad, que tenga políticas de administración con respecto a la integridad y confidencialidad de la información de la organización, y a la reducción de fraudes a niveles aceptables.
- *Operaciones de red y computacionales:* Los procesos en esta área aseguran que los sistemas de información y entornos de red están operados en un esquema seguro y protegido, y que las responsabilidades de procesamiento de información son ejecutados por personal operativo definido, medido y monitoreado. También aseguran que los sistemas son consistentes y están disponibles a los usuarios a un nivel de ejecución satisfactorio.

- *Administración de sistemas de bases de datos:* Los procesos en esta área están diseñados para asegurar que las bases de datos usadas para soportar aplicaciones críticas y reportes tengan consistencia de definición, correspondan con los requerimientos y reduzcan el potencial de redundancia.
- *Información / Negocio:* Los procesos en esta área están diseñados para asegurar que existe un plan adecuado para asegurar que la tecnología informática estará disponible a los usuarios cuando ellos la necesitan.
- **Riesgos de seguridad general:** Los estándares IEC 950 proporcionan los requisitos de diseño para lograr una seguridad general y que disminuyen el riesgo:
 - *Riesgos de choque de eléctrico:* Niveles altos de voltaje.
 - *Riesgos de incendio:* Inflamabilidad de materiales.
 - *Riesgos de niveles inadecuados de energía eléctrica.*
 - *Riesgos de radiaciones:* Ondas de ruido, de láser y ultrasónicas.
 - *Riesgos mecánicos:* Inestabilidad de las piezas eléctricas.

Seguidamente veremos otros riesgos que afectan a la protección informática puesto que aumentan los puntos de vulnerabilidad de los sistemas:

Concentración de procesamiento de aplicaciones mas grandes y de mayor complejidad: Una de las causas más importantes del incremento en los riesgos informáticos probablemente sea el aumento en la cantidad de aplicaciones o usos que se le da a las computadoras y la consecuente concentración de información y tecnología de software para el procesamiento de datos, generalmente la información y programas están concentrados en las manos de pocas personas. Como consecuencia de ello, se corre el riesgo de sufrir lo que en la jerga de seguridad informática suele denominarse "Amnesia Corporativa" debido a algún desastre ocurrido en las

computadoras, y de quedar expuesta a una suspensión prolongada del procesamiento y por ende el mal funcionar de la compañía generándose una situación de caos para la misma y en todos los niveles de la organización.

Dependencia en el personal clave: Además del peligro que encierra algún desastre en los sistemas informáticos, existen otras situaciones potencialmente riesgosas de las cuales la más importante es, quizá, la dependencia hacia individuos clave. La dependencia en individuos clave, algunos de los cuales poseen un alto nivel de desempeño técnico, con frecuencia pone a la compañía en manos de relativamente pocas personas, siendo que éstas por lo general son externas a la organización. Este tipo de situaciones ha conducido a situaciones donde las empresas se han visto expuestas al chantaje, la extorsión, mal uso y fraudes en la explotación de los sistemas informáticos.

La amenaza no solo se restringe al abuso del tipo descrito aquí. Este personal especializado con frecuencia posee el conocimiento único y no registrado de las modificaciones o el funcionamiento de las aplicaciones. La supervisión y el control de su trabajo resulta difícil como lo es el conocimiento de lo que si funcionaría sin contar con las habilidades del especialista.

Desaparición de los controles tradicionales: Muchas de las nuevas y extensas aplicaciones omiten las auditorías tradicionales y los controles impresos por razones de volumen. Las aplicaciones contienen verificadores automáticos que aseguran la integridad de la información que se procesa. Este gran cambio en el criterio sobre el control de los empleados y las brechas respecto a la comunicación, crean situaciones de seguridad totalmente diferentes.

Huelgas, terrorismo e inestabilidad social: El nivel actual de riesgo en computación se debe revisar también dentro del contexto de inestabilidad social en muchas partes del mundo. Ha habido ataques físicos a diversas instalaciones, sin embargo algunas veces se trata de la incursión de personal interno y no de agitadores. Este tipo insidioso de riesgo es, en potencia, la fuente de más alto perjuicio para la institución. Este riesgo, solo, genera una amplia posibilidad de nuevas amenazas ante las cuales hay que responder.

Los ataques internos por parte del personal de una institución pueden tomar la forma de huelga; ésta, aunque no sea violenta, puede ser tan perjudicial como el ataque físico. Las huelgas

han sucedido en grandes instalaciones que operan en línea en diferentes partes del mundo y por tanto en nuestro país también.

Mayor conciencia de los proveedores: Hasta hace pocos años este tema no constituía motivo de gran preocupación para los proveedores, pero la conciencia acerca de la exposición a los riesgos los ha obligado a destinar presupuestos considerables para la investigación acerca de la seguridad. Como resultado, se dispone de un mayor número de publicaciones de alta calidad para los usuarios, lo que permite mejorar la estructura y el enfoque para la seguridad de las computadoras; asimismo, ha intensificado el interés por reducir en forma progresiva el riesgo causado por un desastre en las computadoras.

CONCLUSIÓN

Por todo lo expuesto, resulta mas que obvio la necesidad de un nuevo modelo de seguridad que cubra tanto los aspectos conocidos o clásicos como aquellos no convencionales, además de que los tratados que se han desarrollado sobre seguridad enfocan su atención únicamente en aquellos aspectos tradicionales dejando por consiguiente una brecha de vulnerabilidad en la organización al no cubrir por completo los aspectos de protección relacionados a la misma. Podemos entonces aseverar que este accionar trae consigo que la compañía sea vulnerable. [Web1]

CAPITULO III: CENTRO DE CÓMPUTO

INTRODUCCIÓN.

Con esta parte introductoria se pretende crear un conocimiento sobre lo que es un centro de cómputo citando alguna definición, de igual manera se integraran los elementos que lo integran (tecnologías de información y comunicación) y las funciones que este tiene dentro de la organización. Esto con el fin de una vez entendido el concepto de lo que es un centro de cómputo pasar a la importancia que este tiene en la organización así como también saber como fluye la información dentro de el para la toma de decisiones. Al final de este trabajo se podrán valorar los riesgos y vulnerabilidades a los que el centro de cómputo y la información están expuestos pudiendo repercutir en las actividades de la organización.

Definición de Centro de Cómputo.

Arenal Blanco, Santiago (2005) Representa una entidad dentro de la organización, la cual tiene como objetivo satisfacer las necesidades de información de la empresa, de manera veraz y oportuna. Su función primordial es complementar la labor administrativa para hacerla más segura, fluida y así simplificar. El centro de cómputo es responsable de centralizar, custodiar y procesar la mayoría de los datos con los que operan la empresa.

La seguridad de la información comprende diversos aspectos entre ellos la disponibilidad, comunicación, identificación de problemas, análisis de riesgos, la integridad, confidencialidad, recuperación de los riesgos.

Precisamente la reducción o eliminación de riesgos asociado a una cierta información es el objeto de la seguridad de la información y la seguridad informática. Más concretamente, la seguridad de la información tiene como objeto los sistemas el acceso, uso, divulgación, interrupción o destrucción no autorizada de información. Los términos seguridad de la

información, seguridad informática y garantía de la información son usados frecuentemente como sinónimos porque todos ellos persiguen una misma finalidad al proteger la confidencialidad, integridad y disponibilidad de la información. Sin embargo, no son exactamente lo mismo existiendo algunas diferencias sutiles. Estas diferencias radican principalmente en el enfoque, las metodologías utilizadas, y las zonas de concentración. Además, la seguridad de la información involucra la implementación de estrategias que cubran los procesos en donde la información es el activo primordial. Estas estrategias deben tener como punto primordial el establecimiento de políticas, controles de seguridad, tecnologías y procedimientos para detectar amenazas que puedan explotar vulnerabilidades y que pongan en riesgo dicho activo, es decir, que ayuden a proteger y salvaguardar tanto información como los sistemas que la almacenan y administran. La seguridad de la información incumbe a gobiernos, entidades militares, instituciones financieras, los hospitales y las empresas privadas con información confidencial sobre sus empleados, clientes, productos, investigación y su situación financiera.

Ricardo Hernández Jiménez (1997), definió el centro de cómputo como la unidad de servicio encargado del diseño e implementación de sistemas y de la administración de los recursos computacionales de la empresa. Su trabajo se enfoca hacia el desarrollo de herramientas que faciliten la labor del resto de dependencias de la empresa.

Es una dependencia de importancia estratégica, responsable del procesamiento automático de datos, se caracteriza por disponer de equipos de cómputo optimizados para la carga de trabajo requerida en la organización.

En México es conocido como centro de computo y es el lugar donde se administra, almacena procesa la información de la organización para después estar disponible a las personas de mayor autoridad para dar uso a las necesidades.

Un centro de cómputo representa una entidad dentro de la organización la cual tiene como objetivo satisfacer las necesidades de información de la empresa, de manera veraz y oportuna. Su función primordial es apoyar la labor administrativa para hacerla más segura, fluida, y así simplificarla. El centro de cómputo es responsable de centralizar, custodiar y procesar la mayoría de los datos con los que opera la compañía. Prácticamente todas las actividades de los demás departamentos se basan en la información que les proporciona dicho centro.

La toma de decisiones depende en gran medida de la capacidad de respuesta del proceso de datos. Por lo anterior, casi no se escatima la inversión para proveerlo del equipo técnico (material y humano) necesario. De hecho, en la mayoría de las organizaciones el centro de cómputo absorbe la mayor parte del presupuesto.

La importancia que tiene el centro de cómputo dentro de la organización, o coloca en una posición que influye incluso en una gran parte de las decisiones administrativas y de proyección de las empresas.

Un centro de cómputo significa la culminación de la sistematización de la empresa. El análisis y diseño de sistemas de información implica un alto grado de eficiencia administrativa dentro de la organización, de lo contrario difícilmente se podrían llevar a la practica los diseños. Se puede afirmar que el centro de cómputo reclama que los mecanismos administrativos de la organización estén claramente establecidos. Aun más, si no lo estuvieran, dicho centro esta preparado para colaborar a fin de establecerlos. En otras palabras, el centro de cómputo predica la buena administración.

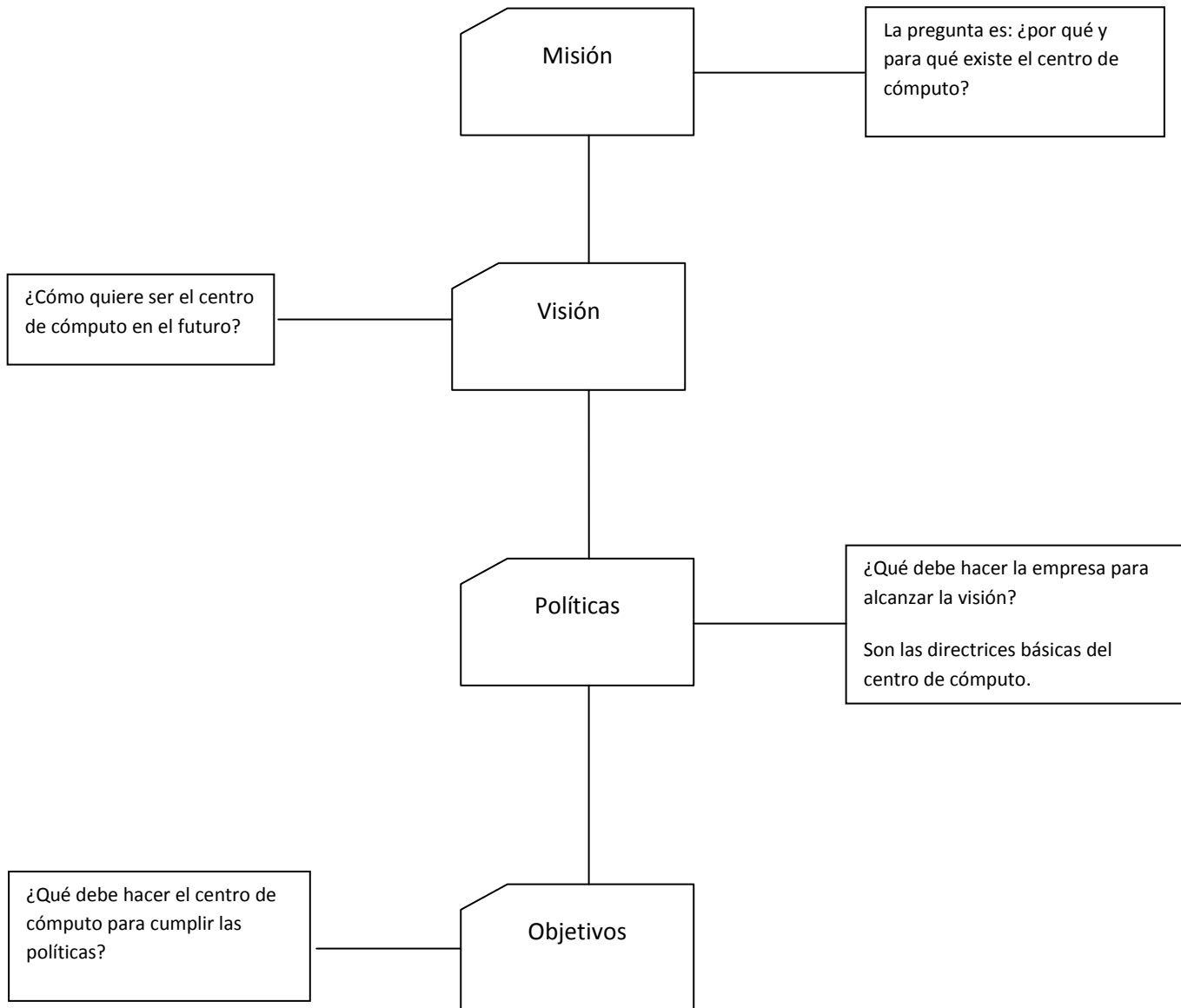
Misión de un centro de cómputo:

La misión de una empresa u organización es la definición específica de lo que la empresa es, de lo que la empresa hace (a qué se dedica o por qué se establece) y a quién sirve con su funcionamiento. Representa la razón de ser de la empresa; orienta toda la planificación y todo el funcionamiento de la misma; y se redacta estableciendo: La actividad empresarial fundamental; el concepto de producto genérico que ofrece; el concepto de tipos de cliente a los que pretende atender. Así pues la computadora como herramienta de solución para problemas de cálculo de operaciones, enseñanza, realización de trabajo, etc. Establece las bases para determinar el objetivo de un centro de cómputo, como es el de prestar servicios a diferentes áreas de una organización o entidad educativa ya sea dentro de la misma institución, o bien fuera de ella, tales como: producción, control de operaciones, captura de datos, programación, dibujo, biblioteca, unidad informática, etc. Los diversos servicios que puede prestar un centro de cómputo, pueden dividirse en departamentos a áreas específicas de trabajo.

Mientras que la visión es la definición de lo que la empresa quiere ser en un futuro (hacia dónde quiere llegar). Recoge las metas y logros planteados por las organizaciones. Una declaración de visión es una breve representación filosófica de cómo quiere ser la empresa y como desea ser percibida en un futuro por sus clientes, empleados, propietarios y otras personas importantes

Organización de los centros de cómputo:

FIGURA 2: Objetivos del centro de cómputo



<http://elprofejorge.blogdiario.com/img/acc.pdf>

Elementos que componen un centro de cómputo:

Para tener una visión organizada de los componentes básicos de un centro de cómputo como sistema de computación integral, podemos dividir sus elementos en tres categorías como:

- Hardware
- Software
- Humanware

Hardware.

Según el glosario de informática (2008) define al hardware como la parte física o solida de una computadora u otro elemento informático.

Poet R. (2008), en su diccionario informático, denomina hardware o soporte físico al conjunto de elementos materiales que componen una computadora. Hardware también son los componentes físicos de una computadora tales como el disco duro, dispositivos de CD-ROM, etc. En dicho conjunto se incluyen los dispositivos electrónicos y eléctricos, circuitos, tarjetas, armarios o cajas, periféricos de todo tipo y otros elementos físicos.

El hardware es el conjunto de elementos físicamente visualizables en un sistema integral de computación o Central de Tecnologías de Información. Es el equipo propiamente dicho. Bajo este término se incluye tanto a la computadora como a los equipos periféricos: impresoras, discos, monitores, unidades de respaldo, etc. Llamamos entonces hardware al conjunto de dispositivos mecánicos y electrónicos que forman parte de la computadora. Es el primer elemento de un sistema de computación y comprende a toda la maquinaria y al equipamiento relacionado al mismo.

Contrasta con el elemento software el cual puede ser descrito como el conjunto de instrucciones que le dicen a la computadora qué hacer. También contrasta con los datos que son los hechos y cifras que se almacenan en el hardware y son controlados por el software.

Para ejemplificar el papel que tiene el hardware se comparará con una orquesta.

El equipamiento de un sistema de computación y las instrucciones asociadas para hacerle funcionar pueden ser comparados con el funcionamiento de una orquesta, esta analogía es útil para entender el modo de trabajo de un sistema de computación. Los músicos y sus instrumentos están ligados al concepto de hardware, las partituras son el software y dentro de éste, el sistema operativo actúa como el director de la orquesta.

El software bajo esta analogía puede ser cambiado de acuerdo al trabajo a realizar, de la misma manera en que los músicos cambian las partituras para producir música (información) diferente. El director, como la parte controladora del sistema (sistema operativo), trabaja con el software para obtener del sistema (computadora /orquesta) lo que la audiencia (usuario) desea.

El hardware se puede clasificar en: básico, el estrictamente necesario para el funcionamiento normal del equipo; y complementario, el que realiza funciones específicas.

Un sistema informático se compone de una unidad central de procesamiento (UCP/CPU), encargada de procesar los datos, uno o varios periféricos de entrada, los que permiten el ingreso de la información y uno o varios periféricos de salida, los que posibilitan dar salida (normalmente en forma visual o auditiva) a los datos procesados.

Tipos de hardware

(Dembowski, Klaus 2000). Una de las formas de clasificar el hardware es en dos categorías: por un lado, el "básico", que abarca el conjunto de componentes indispensables necesarios para otorgar la funcionalidad mínima a una computadora; y por otro lado, el hardware "complementario", que, como su nombre indica, es el utilizado para realizar funciones específicas (más allá de las básicas), no estrictamente necesarias para el funcionamiento de la computadora.

Así es que: un medio de entrada de datos, la unidad central de procesamiento (C.P.U.), la memoria RAM, un medio de salida de datos y un medio de almacenamiento constituyen el "hardware básico".

Los medios de entrada y salida de datos estrictamente indispensables dependen de la aplicación: desde el punto de vista de un usuario común, se debería disponer, al menos, de un teclado y un monitor para entrada y salida de información, respectivamente; pero ello no implica que no pueda haber una computadora (por ejemplo controlando un proceso) en la que no sea necesario teclado ni monitor; bien puede ingresar información y sacar sus datos procesados, por ejemplo, a través de una placa de adquisición/salida de datos.

Las computadoras son aparatos electrónicos capaces de interpretar y ejecutar instrucciones programadas y almacenadas en su memoria; consisten básicamente en operaciones aritmético-lógicas y de entrada/salida. Se reciben las entradas (datos), se las procesa y almacena (procesamiento), y finalmente se producen las salidas (resultados del procesamiento). Por ende

todo sistema informático tiene, al menos, componentes y dispositivos hardware dedicados a alguna de las funciones antedichas; a saber:

1. Procesamiento: Unidad Central de Proceso o CPU
2. Almacenamiento: Memorias
3. Entrada: Periféricos de entrada (E)
4. Salida: Periféricos de salida (S)
5. Entrada/Salida: Periféricos mixtos (E/S)

Desde un punto de vista básico y general, un dispositivo de entrada es el que provee el medio para permitir el ingreso de información, datos y programas (lectura); un dispositivo de salida brinda el medio para registrar la información y datos de salida (escritura); la memoria otorga la capacidad de almacenamiento, temporal o permanente (almacenamiento); y la CPU provee la capacidad de cálculo y procesamiento de la información ingresada (transformación).

Un periférico mixto es aquél que puede cumplir funciones tanto de entrada como de salida; el ejemplo más típico es el disco rígido (ya que en él se lee y se graba información y datos).

Unidad central de procesamiento

La CPU, siglas en inglés de Unidad Central de Procesamiento, es el componente fundamental del computador, encargado de interpretar y ejecutar instrucciones y de procesar datos. En los computadores modernos, la función de la CPU la realiza uno o más microprocesadores. Se conoce como microprocesador a una CPU que es manufacturada como un único circuito integrado.

Las unidades centrales de proceso (CPU) en la forma de un único microprocesador no sólo están presentes en las computadoras personales (PC), sino también en otros tipos de dispositivos que incorporan una cierta capacidad de proceso o "inteligencia electrónica", como pueden ser: controladores de procesos industriales, televisores, automóviles, calculadores, aviones, teléfonos móviles, electrodomésticos, juguetes y muchos más. Actualmente los diseñadores y fabricantes más populares de microprocesadores de PC son Intel y AMD; y para el mercado de dispositivos móviles y de bajo consumo, los principales son Samsung, Qualcomm y Texas Instruments.

El microprocesador que, es el circuito integrado central y más complejo de un sistema informático; a modo de ilustración, se le suele asociar por analogía como el «cerebro» de un computador. El procesador puede definirse, como un circuito integrado constituido por millones de componentes electrónicos agrupados en un paquete. Es el encargado de ejecutar los programas, desde el sistema operativo hasta las aplicaciones de usuario; sólo ejecuta instrucciones programadas en lenguaje de bajo nivel, realizando operaciones las aritméticas y lógicas simples, tales como sumar, restar, multiplicar, dividir, las lógicas binarias y accesos a memoria, se monta en la llamada placa base, sobre un zócalo conocido como zócalo de CPU, que permite las conexiones eléctricas entre los circuitos de la placa y el procesador. Sobre el procesador ajustado a la placa base se fija un disipador térmico de un material con elevada conductividad térmica, que por lo general es de aluminio, y en algunos casos de cobre. Éste es indispensable en los microprocesadores que consumen bastante energía, la cual, en gran parte, es emitida en forma de calor: en algunos casos pueden consumir tanta energía como una lámpara incandescente (de 40 a 130 vatios).

Adicionalmente, sobre el disipador se acopla uno o dos ventiladores (raramente más), destinados a forzar la circulación de aire para extraer más rápidamente el calor acumulado por el disipador y originado en el microprocesador. Complementariamente, para evitar daños por efectos térmicos, también se suelen instalar sensores de temperatura del microprocesador y sensores de revoluciones del ventilador, así como sistemas automáticos que controlan la cantidad de revoluciones por unidad de tiempo de estos últimos.

La gran mayoría de los circuitos electrónicos e integrados que componen el hardware del computador van montados en la placa madre.

La placa base, también conocida como placa madre o con el anglicismo board, es un gran circuito impreso sobre el que se suelda el chipset, las ranuras de expansión (slots), los zócalos, conectores, diversos integrados, etc. Es el soporte fundamental que aloja y comunica a todos los demás componentes: Procesador, módulos de memoria RAM, tarjetas gráficas, tarjetas de expansión, periféricos de entrada y salida. Para comunicar esos componentes, la placa base posee una serie de buses mediante los cuales se transmiten los datos dentro y hacia afuera del sistema.

La tendencia de integración ha hecho que la placa base se convierta en un elemento que incluye a la mayoría de las funciones básicas (vídeo, audio, red, puertos de varios tipos), funciones que antes se realizaban con tarjetas de expansión. Aunque ello no excluye la capacidad de instalar otras tarjetas adicionales específicas, tales como capturadoras de vídeo, tarjetas de adquisición de datos, etc.

También, la tendencia en los últimos años es eliminar elementos separados en la placa base e integrarlos al microprocesador. En ese sentido actualmente se encuentran sistemas denominados “System on a Chip” que consiste en un único circuito integrado que integra varios módulos electrónicos en su interior, tales como un procesador, un controlador de memoria,

una GPU, Wi-Fi, bluetooth, etc. La mejora más notable en esto está en la reducción de tamaño frente a igual funcionalidad con módulos electrónicos separados. La figura muestra una aplicación típica, en la placa principal de un teléfono móvil.

Memoria RAM

Del inglés Random Access Memory, literalmente significa "memoria de acceso aleatorio". El término tiene relación con la característica de presentar iguales tiempos de acceso a cualquiera de sus posiciones (ya sea para lectura o para escritura). Esta particularidad también se conoce como "acceso directo", en contraposición al Acceso secuencial.

La RAM es la memoria utilizada en una computadora para el almacenamiento transitorio y de trabajo (no masivo). En la RAM se almacena temporalmente la información, datos y programas que la Unidad de Procesamiento (CPU) lee, procesa y ejecuta. La memoria RAM es conocida como Memoria principal de la computadora, también como "Central o de Trabajo"; a diferencia de las llamadas memorias auxiliares, secundarias o de almacenamiento masivo (como discos duros, unidades de estado sólido, cintas magnéticas u otras memorias).

Las memorias RAM son, comúnmente, volátiles; lo cual significa que pierden rápidamente su contenido al interrumpir su alimentación eléctrica.

Las más comunes y utilizadas como memoria central son "dinámicas" (DRAM), lo cual significa que tienden a perder sus datos almacenados en breve tiempo (por descarga, aún estando con alimentación eléctrica), por ello necesitan un circuito electrónico específico que se encarga de proveerle el llamado "refresco" (de energía) para mantener su información.

La memoria RAM de un computador se provee de fábrica e instala en lo que se conoce como “módulos”. Ellos albergan varios circuitos integrados de memoria DRAM que, conjuntamente, conforman toda la memoria principal.

Periféricos

Se entiende por periférico a las unidades o dispositivos que permiten a la computadora comunicarse con el exterior, esto es, tanto ingresar como exteriorizar información y datos. Los periféricos son los que permiten realizar las operaciones conocidas como de entrada/salida (E/S).

Aunque son estrictamente considerados “accesorios” o no esenciales, muchos de ellos son fundamentales para el funcionamiento adecuado de la computadora moderna; por ejemplo, el teclado, el disco duro y el monitor son elementos actualmente imprescindibles; pero no lo son un *escáner* o un *plóter*. Para ilustrar este punto: en los años 80, muchas de las primeras computadoras personales no utilizaban disco duro ni *mouse* (o ratón), tenían sólo una o dos disqueteras, el teclado y el monitor como únicos periféricos.

Dispositivos de entrada de información

De esta categoría son aquellos que permiten el ingreso de información, en general desde alguna fuente externa o por parte del usuario. Los dispositivos de entrada proveen el medio fundamental para transferir hacia la computadora (más propiamente al procesador) información desde alguna fuente, sea local o remota. También permiten cumplir la esencial tarea de leer y cargar en memoria el sistema operativo y las aplicaciones o programas informáticos, los que a su vez ponen operativa la computadora y hacen posible realizar las más diversas tareas.

Entre los periféricos de entrada se puede mencionar: teclado, mouse o ratón, escáner, micrófono, cámara, lectores ópticos de código de barras, Joystick, lectora de CD, DVD o BluRay (sólo lectoras), placas de adquisición/conversión de datos, etc.

Pueden considerarse como imprescindibles para el funcionamiento, (de manera como hoy se concibe la informática) al teclado, al ratón y algún dispositivo lector de discos; ya que tan sólo con ellos el hardware puede ponerse operativo para un usuario. Los otros son más bien accesorios, aunque en la actualidad pueden resultar de tanta necesidad que son considerados parte esencial de todo el sistema.

Dispositivos de salida de información

Son aquellos que permiten emitir o dar salida a la información resultante de las operaciones realizadas por la CPU (procesamiento).

Los dispositivos de salida aportan el medio fundamental para exteriorizar y comunicar la información y datos procesados; ya sea al usuario o bien a otra fuente externa, local o remota.

Los dispositivos más comunes de este grupo son los monitores clásicos (no de pantalla táctil), las impresoras, y los altavoces.

Entre los periféricos de salida puede considerarse como imprescindible para el funcionamiento del sistema, al monitor. Otros, aunque accesorios, son sumamente necesarios para un usuario que opere un computador moderno.

Dispositivos Mixtos

Son aquellos dispositivos que pueden operar de ambas formas: tanto de entrada como de salida. Típicamente, se puede mencionar como periféricos mixtos o de Entrada/Salida a: discos rígidos, disquetes, unidades de cinta magnética, lecto-grabadoras de CD/DVD, discos ZIP, etc.

También entran en este rango, con sutil diferencia, otras unidades, tales como: Tarjetas de Memoria flash o unidad de estado sólido, tarjetas de red, módems, tarjetas de captura/salida de vídeo, etc.

Si bien se puede clasificar al pendrive (lápiz de memoria), memoria flash o memoria USB o unidades de estado sólido en la categoría de memorias, normalmente se los utiliza como dispositivos de almacenamiento masivo; siendo todos de categoría Entrada/Salida.

Los dispositivos de almacenamiento masivo también son conocidos como "Memorias Secundarias o Auxiliares". Entre ellos, sin duda, el disco duro ocupa un lugar especial, ya que es el de mayor importancia en la actualidad, en el que se aloja el sistema operativo, todas las aplicaciones, utilitarios, etc. que utiliza el usuario; además de tener la suficiente capacidad para albergar información y datos en grandes volúmenes por tiempo prácticamente indefinido

La pantalla táctil (no el monitor clásico) es un dispositivo que se considera mixto, ya que además de mostrar información y datos (salida) puede actuar como un dispositivo de entrada, reemplazando, por ejemplo, a algunas funciones del ratón o del teclado.

Hardware gráfico

El hardware gráfico lo constituyen básicamente las tarjetas gráficas. Dichos componentes disponen de su propia memoria y unidad de procesamiento, esta última llamada unidad de procesamiento gráfico (o GPU, siglas en inglés de Graphics Processing Unit). El objetivo básico de la GPU es realizar los cálculos asociados a operaciones gráficas, fundamentalmente en coma flotante, liberando así al procesador principal (CPU) de esa costosa tarea (en tiempo) para que éste pueda efectuar otras funciones en forma más eficiente. Antes de esas tarjetas de vídeo con

aceleradores por hardware, era el procesador principal el encargado de construir la imagen mientras la sección de vídeo (sea tarjeta o de la placa base) era simplemente un traductor de las señales binarias a las señales requeridas por el monitor; y buena parte de la memoria principal (RAM) de la computadora también era utilizada para estos fines.

Dentro de ésta categoría no se deben omitir los sistemas gráficos integrados (IGP), presentes mayoritariamente en equipos portátiles o en equipos prefabricados (OEM), los cuales generalmente, a diferencia de las tarjetas gráficas, no disponen de una memoria dedicada, utilizando para su función la memoria principal del sistema. La tendencia en los últimos años es integrar los sistemas gráficos dentro del propio procesador central. Los procesadores gráficos integrados (IGP) generalmente son de un rendimiento y consumo notablemente más bajo que las GPU de las tarjetas gráficas dedicadas, no obstante, son más que suficiente para cubrir las necesidades de la mayoría de los usuarios de un PC.

Actualmente se están empezando a utilizar las tarjetas gráficas con propósitos no exclusivamente gráficos, ya que en potencia de cálculo la GPU es superior, más rápida y eficiente que el procesador para operaciones en coma flotante, por ello se está tratando de aprovecharla para propósitos generales, al concepto, relativamente reciente, se le denomina GPGPU (General-Purpose Computing on Graphics Processing Units).

La Ley de Moore establece que cada 18 a 24 meses la cantidad de transistores que puede contener un circuito integrado se logra duplicar; en el caso de los GPU esta tendencia es bastante más notable, duplicando, o aún más, lo indicado en la ley de Moore.

Desde la década de 1990, la evolución en el procesamiento gráfico ha tenido un crecimiento vertiginoso; las actuales animaciones por computadoras y videojuegos eran impensables veinte años atrás.

SOFTWARE

(Estándar 729 del IEEE) Es el conjunto de los programas de cómputo, procedimientos, reglas, documentación y datos asociados que forman parte de las operaciones de un sistema de computación.

El software es el segundo elemento de un sistema de computación, está constituido por los programas, es decir por el conjunto de instrucciones que se suministran a la máquina para que resuelva algún problema. Bajo el concepto de software entonces, se incluye al conjunto de instrucciones agrupadas en rutinas y programas (junto con la documentación respectiva) que indican cómo resolver problemas de naturaleza diversa en una computadora. En síntesis, el software está formado por instrucciones para que la computadora trabaje. El conjunto o serie de instrucciones para realizar una tarea en particular se llama programa o programa de software. Bajo esta categoría incluimos a los programas preparados por el usuario (software de aplicación) como así también a aquellos programas provistos por el fabricante del equipo o comprado a terceras partes, como son el sistema operativo (software de base) y los lenguajes de programación, utilitarios y los productos para automatización de oficina como procesadores de texto, planillas de cálculo y otros productos de software.

Clasificación del software

Si bien esta distinción es, en cierto modo, arbitraria, y a veces confusa, a los fines prácticos se puede clasificar al software en tres grandes tipos:

❖ **Software de sistema:** Su objetivo es desvincular adecuadamente al usuario y al programador de los detalles del sistema informático en particular que se use, aislándolo especialmente del procesamiento referido a las características internas de: memoria, discos, puertos y dispositivos de comunicaciones, impresoras, pantallas, teclados, etc. El software de sistema le procura al usuario y programador adecuadas interfaces de alto nivel, herramientas y utilidades de apoyo que permiten su mantenimiento. Incluye entre otros:

- ✓ Sistemas operativos
- ✓ Controladores de dispositivos
- ✓ Herramientas de diagnóstico
- ✓ Herramientas de Corrección y Optimización
- ✓ Servidores
- ✓ Utilidades

❖ **Software de programación:** Es el conjunto de herramientas que permiten al programador desarrollar programas informáticos, usando diferentes alternativas y lenguajes de programación, de una manera práctica. Incluye entre otros:

- ✓ Editores de texto
- ✓ Compiladores
- ✓ Intérpretes
- ✓ Enlazadores
- ✓ Depuradores
- ✓ Entornos de Desarrollo Integrados (IDE): Agrupan las anteriores herramientas, usualmente en un entorno visual, de forma tal que el programador no necesite introducir múltiples comandos para compilar, interpretar, depurar, etc. Habitualmente cuentan con una avanzada interfaz gráfica de usuario (GUI).

❖ **Software de aplicación:** Es aquel que permite a los usuarios llevar a cabo una o varias tareas específicas, en cualquier campo de actividad susceptible de ser automatizado o asistido, con especial énfasis en los negocios. Incluye entre otros:

- ✓ Aplicaciones para Control de sistemas y automatización industrial
- ✓ Aplicaciones ofimáticas
- ✓ Software educativo
- ✓ Software empresarial
- ✓ Bases de datos
- ✓ Telecomunicaciones (por ejemplo Internet y toda su estructura lógica)
- ✓ Videojuegos
- ✓ Software médico
- ✓ Software de Cálculo Numérico y simbólico.
- ✓ Software de Diseño Asistido (CAD)
- ✓ Software de Control Numérico (CAM)

Proceso de creación del software

Jacobson, Ivar (2000) Se define como Proceso al conjunto ordenado de pasos a seguir para llegar a la solución de un problema u obtención de un producto, en este caso particular, para lograr la obtención de un producto software que resuelva un problema.

El proceso de creación de software puede llegar a ser muy complejo, dependiendo de su porte, características y criticidad del mismo. Por ejemplo la creación de un sistema operativo es una tarea que requiere proyecto, gestión, numerosos recursos y todo un equipo disciplinado de

trabajo. En el otro extremo, si se trata de un sencillo programa (por ejemplo, la resolución de una ecuación de segundo grado), éste puede ser realizado por un solo programador (incluso amateur) fácilmente. Es así que normalmente se dividen en tres categorías según su tamaño (líneas de código) o costo: de Pequeño, Mediano y Gran porte. Existen varias metodologías para estimarlo, una de las más populares es el sistema COCOMO que provee métodos y un software (programa) que calcula y provee una estimación de todos los costos de producción en un proyecto software (relación horas/hombre, costo monetario, cantidad de líneas fuente de acuerdo a lenguaje usado, etc.).

Considerando los de gran porte, es necesario realizar complejas tareas, tanto técnicas como de gerencia, una fuerte gestión y análisis diversos, por lo cual se ha desarrollado una ingeniería para su estudio y realización: es conocida como Ingeniería de Software.

En tanto que en los de mediano porte, pequeños equipos de trabajo pueden realizar la tarea. Aunque, siempre en casos de mediano y gran porte (y a veces también en algunos de pequeño porte, según su complejidad), se deben seguir ciertas etapas que son necesarias para la construcción del software. Tales etapas, si bien deben existir, son flexibles en su forma de aplicación, de acuerdo a la metodología o proceso de desarrollo escogido y utilizado por el equipo de desarrollo o por el analista-programador solitario.

Los procesos de desarrollo de software poseen reglas preestablecidas, y deben ser aplicados en la creación del software de mediano y gran porte, ya que en caso contrario lo más seguro es que el proyecto o no logre concluir o termine sin cumplir los objetivos previstos, y con variedad de fallos inaceptables. Entre tales procesos los hay ágiles o livianos, pesados y lentos y variantes intermedias; y normalmente se aplican de acuerdo al tipo y porte del software a desarrollar, a criterio del líder del equipo de desarrollo.

Cualquiera sea el proceso utilizado y aplicado al desarrollo del software, y casi independientemente de él, siempre se debe aplicar un modelo de ciclo de vida. Se estima que, del total de proyectos software grandes emprendidos, un 28% fracasan, un 46% caen en severas modificaciones que lo retrasan y un 26% son totalmente exitosos.

Es común para el desarrollo de software de mediano porte que los equipos humanos involucrados apliquen sus propias metodologías, normalmente un híbrido de los procesos anteriores y a veces con criterios propios.

El proceso de desarrollo puede involucrar numerosas y variadas tareas, desde lo administrativo, pasando por lo técnico y hasta la gestión y el gerenciamiento. Pero casi rigurosamente siempre se cumplen ciertas etapas mínimas; las que se pueden resumir como sigue:

- ✓ Captura, Elicitación, Especificación y Análisis de requisitos (ERS)
- ✓ Diseño
- ✓ Codificación
- ✓ Pruebas (unitarias y de integración)
- ✓ Instalación y paso a Producción
- ✓ Mantenimiento

En las anteriores etapas pueden variar ligeramente sus nombres, o ser más globales, o contrariamente, ser más refinadas; por ejemplo indicar como una única fase (a los fines documentales e interpretativos) de análisis y diseño; o indicar como implementación lo que está dicho como codificación; pero en rigor, todas existen e incluyen, básicamente, las mismas tareas específicas.

Instalación

Sommerville, Ian (2005). La instalación del software es el proceso por el cual los programas desarrollados son transferidos apropiadamente al computador destino, inicializados, y, eventualmente, configurados; todo ello con el propósito de ser ya utilizados por el usuario final. Constituye la etapa final en el desarrollo propiamente dicho del software. Luego de ésta el producto entrará en la fase de funcionamiento y producción, para el que fuera diseñado.

La instalación, dependiendo del sistema desarrollado, puede consistir en una simple copia al disco rígido destino (casos raros actualmente); o bien, más comúnmente, con una de complejidad intermedia en la que los distintos archivos componentes del software (ejecutables, bibliotecas, datos propios, etc.) son descomprimidos y copiados a lugares específicos preestablecidos del disco; incluso se crean vínculos con otros productos, además del propio sistema operativo. Este último caso, comúnmente es un proceso bastante automático que es creado y guiado con herramientas software específicas (empaquetado y distribución, instaladores).

En productos de mayor complejidad, la segunda alternativa es la utilizada, pero es realizada o guiada por especialistas; puede incluso requerirse la instalación en varios y distintos computadores (instalación distribuida).

También, en software de mediana y alta complejidad normalmente es requerido un proceso de configuración y chequeo, por el cual se asignan adecuados parámetros de funcionamiento y se testea la operatividad funcional del producto.

En productos de venta masiva las instalaciones completas, si son relativamente simples, suelen ser realizadas por los propios usuarios finales (tales como sistemas operativos, paquetes de oficina, utilitarios, etc.) con herramientas propias de instalación guiada; incluso la configuración

suele ser automática. En productos de diseño específico o «a medida» la instalación queda restringida, normalmente, a personas especialistas involucradas en el desarrollo del software en cuestión.

Una vez realizada exitosamente la instalación del software, el mismo pasa a la fase de producción (operatividad), durante la cual cumple las funciones para las que fue desarrollado, es decir, es finalmente utilizado por el (o los) usuario final, produciendo los resultados esperados.

Mantenimiento

El mantenimiento de software es el proceso de control, mejora y optimización del software ya desarrollado e instalado, que también incluye depuración de errores y defectos que puedan haberse filtrado de la fase de pruebas de control y beta test. Esta fase es la última (antes de iterar, según el modelo empleado) que se aplica al ciclo de vida del desarrollo de software. La fase de mantenimiento es la que viene después de que el software está operativo y en producción.

De un buen diseño y documentación del desarrollo dependerá cómo será la fase de mantenimiento, tanto en costo temporal como monetario. Modificaciones realizadas a un software que fue elaborado con una documentación indebida o pobre y mal diseño puede llegar a ser tanto o más costosa que desarrollar el software desde el inicio. Por ello, es de fundamental importancia respetar debidamente todas las tareas de las fases del desarrollo y mantener adecuada y completa la documentación.

El período de la fase de mantenimiento es normalmente el mayor en todo el ciclo de vida. Esta fase involucra también actualizaciones y evoluciones del software; no necesariamente implica que el sistema tuvo errores. Uno o más cambios en el software, por ejemplo de

adaptación o evolutivos, puede llevar incluso a reversiones y adaptar desde parte de las primeras fases del desarrollo inicial, alterando todas las demás; dependiendo de cuán profundos sean los cambios. El modelo cascada común es particularmente costoso en mantenimiento, ya que su rigidez implica que cualquier cambio provoca regreso a fase inicial y fuertes alteraciones en las demás fases del ciclo de vida.

Durante el período de mantenimiento, es común que surjan nuevas revisiones y versiones del producto; que lo liberan más depurado, con mayor y mejor funcionalidad, mejor rendimiento, etc. Varias son las facetas que pueden ser alteradas para provocar cambios deseables, evolutivos, adaptaciones o ampliaciones y mejoras.

Básicamente se tienen los siguientes tipos de cambios:

- ✓ Perfectivos: Aquellos que llevan a una mejora de la calidad interna del software en cualquier aspecto: Reestructuración del código, definición más clara del sistema y su documentación; optimización del rendimiento y eficiencia.
- ✓ Evolutivos: Agregados, modificaciones, incluso eliminaciones, necesarias en el software para cubrir su expansión o cambio, según las necesidades del usuario.
- ✓ Adaptivos: Modificaciones que afectan a los entornos en los que el sistema opera, tales como: Cambios de configuración del hardware (por actualización o mejora de componentes electrónicos), cambios en el software de base, en gestores de base de datos, en comunicaciones, etc.
- ✓ Correctivos: Alteraciones necesarias para corregir errores de cualquier tipo en el producto software desarrollado

INTERACCIÓN HARDWARE-SOFTWARE

(Maturana, J. (2009). En operación, una computadora es a la vez hardware y software.

Uno es inútil sin el otro, y cada uno regula al otro. El diseño del hardware especifica qué instrucciones pueden ejecutarse, luego las instrucciones le dicen a la computadora qué tarea hacer. En operación, el hardware y el software son inseparables, en cambio son completamente diferentes cuando están siendo evaluados. El hardware es el mundo de la velocidad de procesamiento, del almacenamiento y la transmisión. El software es el mundo de la lógica, de los sistemas y de los lenguajes de programación. El hardware siempre trata el problema del procesamiento de datos del mismo modo. ¿Cuánto?, ¿Con qué rapidez? En cambio el software se ocupa de los detalles tediosos de un negocio en constante cambio. Es mucho más difícil analizar, diseñar y desarrollar la solución de software que especificar el hardware.

La metáfora de la computadora

El vertiginoso desarrollo experimentado en las últimas décadas por las tecnologías de la información y su exitosa radicalización en casi todas las áreas o actividades del quehacer social, organizacional, económico, y en la interacción del hombre con su medio y recursos, ha puesto muy de moda, no sólo entre los científicos sino que también en la mayoría de las personas, una popular analogía entre la actividad mental-cerebral humana y los computadores electrónicos.

Por ejemplo, a la luz de este símil, un dualista cartesiano no dudaría en afirmar que el hardware, es decir, los componentes mecánicos, eléctricos y electrónicos son el cuerpo o sustancia material del sistema, y que el software o conjunto de programas computacionales, sería el sustrato no material o la mente inmaterial que habita en la máquina. El hardware patente a la percepción sensorial, no explicaría por sí sólo el comportamiento exhibido por el sistema, ya que

por más que se escarbe entre los circuitos eléctricos, componentes mecánicos y flujos electromagnéticos de la máquina, nada habría que se asemejara ni siquiera medianamente a un razonamiento, pensamiento o inferencia. Debe haber en la máquina algún otro tipo de sustancia que sea portadora de tales propiedades y que sea causante directa de los “estados mentales” constatados en la máquina. Consecuentemente, el software inmaterial depositado en el hardware sería el espíritu que anima la máquina y articula sus componentes mecánicos inyectándole de esta forma vida y movimiento. De aquí que el sistema propiamente tal, no sería otra cosa que el software circunstancialmente residente en un hardware particular. Finalmente, para el dualista, el funcionamiento del sistema completo sólo podría explicarse en términos de algún tipo de interacción entre el hardware o sustancia material y el software o la sustancia inmaterial que determina su comportamiento, y el problema radicaría en hallar los términos precisos en que se produce la interacción entre tales componentes.

Por otro lado, desde una perspectiva de la psicología computacional, la metáfora se traduciría de la siguiente manera:

- ❖ La arquitectura básica de los computadores se ajusta a un modelo que, en sus aspectos estructurales, se compone de los siguientes elementos:
 - ✓ Un cerebro compuesto básicamente de una unidad de control y una
 - ✓ Unidad de pensamiento
 - ✓ Una memoria de corto plazo
 - ✓ Una memoria de largo plazo

- ✓ Órganos aferentes de entrada
- ✓ Órganos eferentes de salida

- ❖ La comunicación entre estas partes se efectúa a través de una red nerviosa de buses o canales, que permiten transportar las señales eléctricas de un lugar a otro. El control y la coordinación de todos estos componentes es realizada por una unidad de control, que forma parte del “cerebro” del conjunto. Dentro de la máquina circulan las corrientes eléctricas rigurosamente sincronizadas gracias a un reloj interno que envía impulsos con una frecuencia determinada estableciendo el ciclo base de la unidad de control. Por otra parte, la Unidad de Pensamiento, es la zona del “cerebro” encargada de efectuar las operaciones aritméticas y lógicas, tales como el manejo de los operadores “and”, “or”, “not” e inferencias del tipo “if (condición) then...” lo que permite canalizar una determinada secuencia de pasos y bifurcarla hacia otras secuencias dependiendo si se verificó o no la condición.

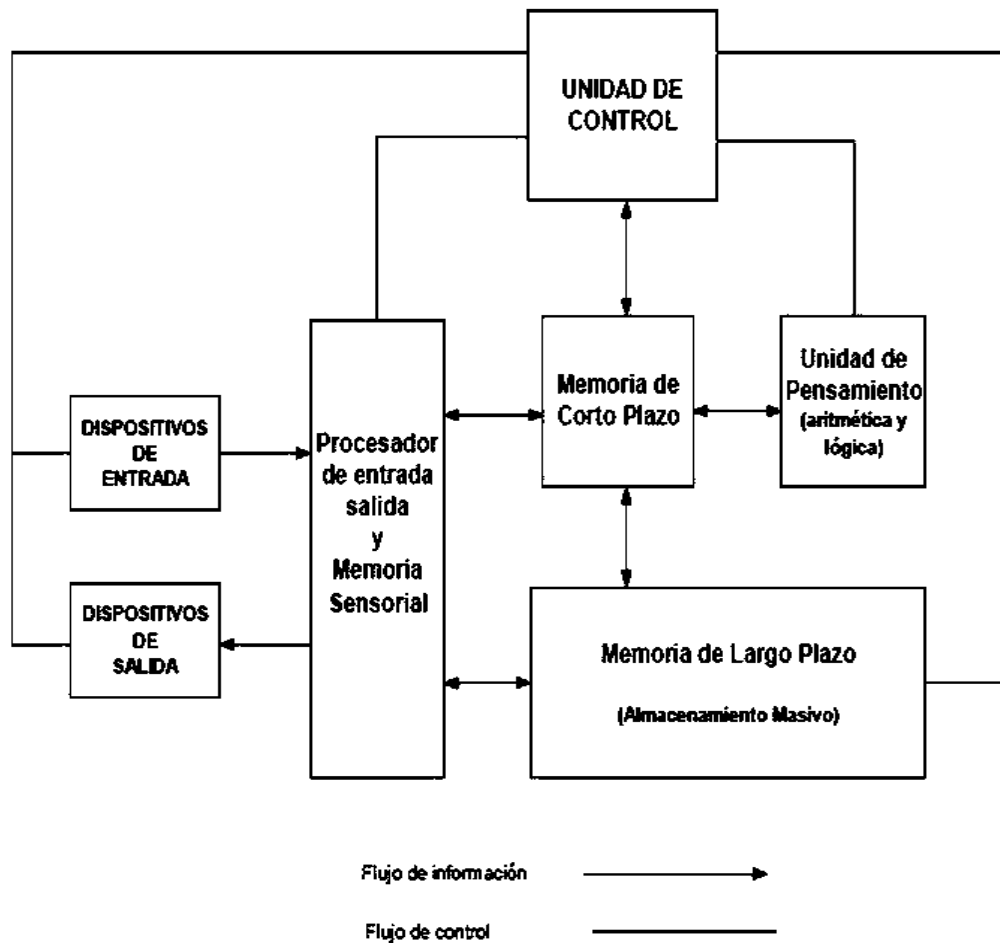
- ❖ La memoria de corto plazo, ubicada en una zona del “cerebro”, está dividida en compartimientos o celdas cada una de las cuales posee una dirección y puede contener distintos tipos de información. Esta memoria es de muy rápido acceso pero de poca capacidad, por lo cual, la escritura de nueva información se realiza con el consiguiente borrado de parte de la que existía anteriormente. La memoria de corto plazo es esencialmente volátil ya que su contenido se pierde cuando se produce una desconexión temporal o se escriben nuevos contenidos muy extensos. No obstante, en esta memoria

siempre se encuentra presente la información necesaria para realizar la actividad actual o más reciente.

- ❖ El propósito de la memoria de largo plazo es conservar grandes cantidades de información y por una cantidad de tiempo indefinida. A diferencia de la memoria a corto plazo, su acceso es más lento pero su capacidad es sustancialmente mayor, y su contenido posee una mayor persistencia en el tiempo.
- ❖ A través de los órganos de entrada, la máquina recoge la información del mundo exterior y mediante los órganos de salida, entrega las respuestas al mundo exterior. Asociados a estos órganos existe un mecanismo altamente especializado en codificación y decodificación de datos que permite convertir las señales del mundo externo en las señales de naturaleza electromagnéticas reconocidas por la máquina y viceversa. En este mecanismo puede localizarse la memoria sensorial, puesto que aquí se encuentran presentes los estímulos provocados por las percepciones sensoriales más recientes.

La arquitectura descrita corresponde a la que clásicamente se conoce como el modelo de Von Neumann, del cual ofrecemos una adaptación en la siguiente figura:

FIGURA 3: Máquina de Von Neumann



http://www.jorgematurana.cl/dv/P09/pct/PCT0906a_Como_interactuan_HW_y_SW.pdf

La interacción del hardware con el software

En relación a esta atrayente y poderosa metáfora, desde una perspectiva técnica sabemos efectivamente que un sistema de computación se compone de programas computacionales que operan en el hardware, y también sabemos que el programa es independiente del hardware en el sentido que puede ejecutarse en cualquier computador digital de similares características.

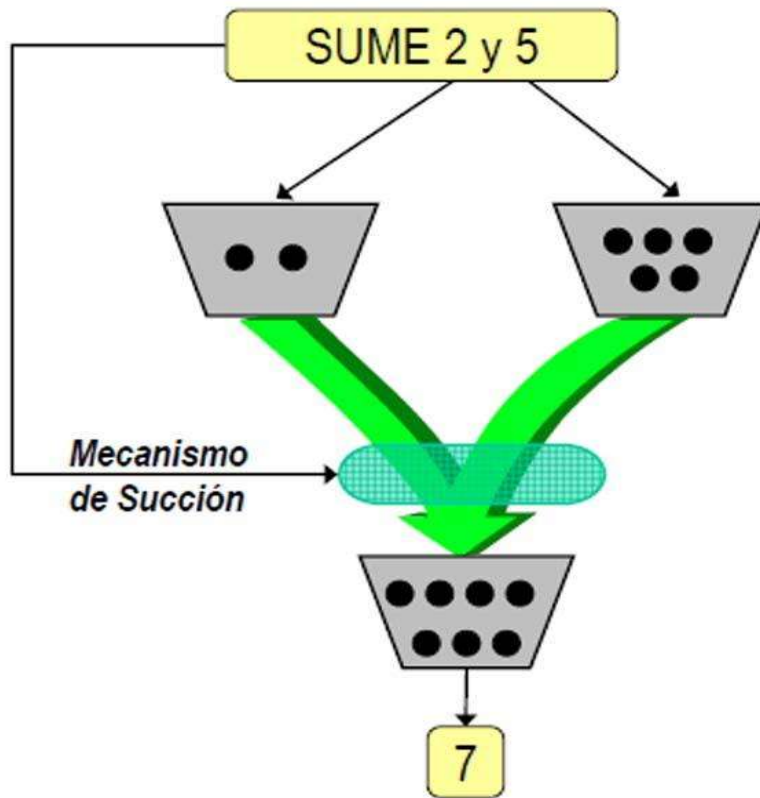
Sin embargo, para apreciar claramente bajo qué términos se verifica algún tipo de interacción entre el hardware y el software, dejando de lado las complicaciones de los circuitos

electrónicos que podrían inducir a confusión, recurriremos al diseño de una máquina sumadora que no obstante su simpleza, nos proporciona una conveniente analogía para estos propósitos.

La máquina en cuestión obedece a una instrucción simple del tipo “SUME a y b”, donde la palabra “SUME” representa la acción a realizar y las variables a, b corresponden a números enteros no negativos sobre los cuales se realizará la operación, en este caso, de suma de enteros. La arquitectura básica de la máquina sumadora consta de dos casillas de entrada donde se almacenan las variables a sumar, y una casilla de salida donde se registra el resultado después de la acción de suma.

Las casillas de entrada están conectadas mediante ductos tubulares al vacío que convergen simultáneamente a la casilla de salida; en la intersección de los tubos se ubica una bomba de succión que al operar succiona las bolillas puestas en las casillas de entrada en dirección a la casilla de salida. Los números se representan mediante bolillas puestas en los respectivos casilleros, de tal forma que la cardinalidad del conjunto de bolillas en cada casillero corresponde a los valores de los números de entrada y salida, respectivamente. Cada vez que la máquina recibe una instrucción, por ejemplo “SUME 2 y 5”, primero realiza la representación física de los literales numéricos mediante el poblamiento de bolillas en las casillas de entrada, y después ejecuta el verbo de acción, que en nuestro caso, consiste en la activación del mecanismo de succión que transporta las bolillas de los dos casilleros de entrada al casillero de salida; posteriormente se realiza la traducción de la cantidad de bolillas en la casilla de salida al respectivo literal numérico que las representa. La siguiente figura muestra el modelo de esta máquina y la operatoria de suma recién descrita.

FIGURA 4: Ejemplo de interacción hardware--software



http://www.jorgematurana.cl/dv/P09/pct/PCT0906a_Como_interactuan_HW_y_SW.pdf

Ahora, si sobre la base de esta máquina alguien nos preguntara cómo es que interactúa el hardware (máquina compuesta de casilleros, bolillas, ductos, bomba de succión, etc.) con el software (conjunto de sentencias o instrucciones de la forma “SUME a y b”), la respuesta sería de la siguiente forma:

- a) Existe una función de representación que traduce los literales numéricos asociados al verbo de acción de la sentencia imperativa, en determinadas cantidades de bolillas físicas que son puestas en las casillas de entrada.
- b) Para el verbo de acción de dicha sentencia existe una función de transformación que lo traduce en el accionamiento de una bomba de succión que transporta las bolillas desde ambos casilleros de entrada al casillero de salida.
- c) Finalmente se ejecuta la inversa de la función de representación que traduce las bolillas en el casillero de salida al respectivo literal numérico.

En otras palabras, lo esencial de la interacción entre software y hardware, es un par de funciones que traducen sucesos lingüísticos en sucesos físicos, en el caso de los literales numéricos se trata de una función de representación, y en el caso del verbo de acción, se trata de una función de proyección que relaciona el verbo con la activación física de un mecanismo de succión (que por lo demás, nada tendría que ver con el contenido semántico de dicho verbo). Por otro lado, nótese que si reemplazamos bolillas por núcleos magnéticos, ductos por buses de comunicación y bomba de succión por circuitos electrónicos, tenemos una ajustada analogía con un computador digital sin perder en absoluto sustancialidad conceptual. El secreto de la interacción estaría dado entonces por la adecuada construcción de funciones que conecten dominios lingüísticos (inmateriales), con dominios físicos (materiales).

Esta misma característica se encuentra presente en el formalismo de las máquinas de Turing, donde estas funciones se encuentran representadas por la función de transición directa, definida como la proyección:

$$\delta: Q \times T \rightarrow Q \times T \times \{L, N, D\}$$

donde, Q es un conjunto de estados finito y no vacío de la unidad de control

T es un alfabeto de cinta

$d \in \{L, N, D\}$ representa la dirección en que se mueve el cabezal de la cinta, según:

si $d = L$, la cabeza se mueve un cuadrado a la izquierda

si $d = N$, el cabezal no se mueve

si $d = D$, el cabezal se mueve un cuadrado a la derecha

De esta forma, el funcionamiento de una máquina de Turing queda espontáneamente determinado por la definición que se establezca para la función de transición directa:

$$(q_1, A_1) \rightarrow (q_2, A_2, d) = \delta(q_1, A_1)$$

lo que significa que (1) la unidad de control se encuentra actualmente en el estado q_1 y el símbolo A_1 se lee del cuadrado actual mediante el cabezal, y (2) al realizar un movimiento atómico, la unidad de control de la máquina cambia al estado q_2 , el símbolo A_1 se reemplaza por A_2 , y la cabeza de la cinta se mueve un cuadrado en dirección d . Lo destacado de esta función, es que relaciona símbolos de estado y alfabéticos, con movimientos físicos.

Volviendo al ejercicio de nuestra máquina sumadora, si ahora se insistiera en la pregunta de si el software es independiente del hardware, entonces deberemos diferenciar entre dos acepciones diferentes de la sentencia “SUME a y b ”. Por un lado, esta sentencia posee un contenido semántico que denota la abstracción matemática de sumar dos números (SUME* a y b), y por el otro, también significa la activación y realización del mecanismo de succión (SUME** a y b).

Evidentemente, la connotación matemática de “ $SUME^* a y b$ ” constituye una abstracción que es independiente de cualquier implementación operativa. Sin embargo, la sentencia “ $SUME^{**} a y b$ ” sólo tiene sentido como parte de una función específica que refiere correlacionalmente a un dominio material. Si el software es lo segundo, entonces no es independiente de la implementación física o material donde se proyecta, aunque si posiblemente, en algún sentido, del tipo de material con que se construya (las bolillas podrían ser de madera o metal, o en vez de bolillas podríamos utilizar moscas, pero la acción de succionamiento no la podemos soslayar). No obstante, en la práctica, no nos presta mucha utilidad hablar de succiones de bolillas, preferimos hablar de sumas de enteros, pero este modo de denotar constituye una interpretación ajena al sistema.

Por otro lado, si se tuviera un mapa acabado de los circuitos e interrelaciones electromagnéticas de un computador, manipulando directamente las magnetizaciones binarias de los circuitos del hardware estaríamos indirectamente modificando el programa y produciendo un cambio de comportamiento en el sistema. Análogamente si se dispusiera de un mapa completo del programa, mediante su manipulación produciríamos modificaciones en la estados magnéticos de la máquina y alterando la respuesta del sistema. La razón de tal coincidencia es simple: ambos aspectos obedecen a una misma función de transición que correlaciona dominios conceptuales y físicos. La “metáfora del computador” no sabemos si es un buen ejemplo de algún aspecto del funcionamiento del cerebro, pero si es un claro paradigma de cómo puede lograrse coincidencia estructural, en este caso sintáctica, de una configuración material y un algoritmo lógico (no-material).

Finalmente, nos queda pendiente un aspecto que nos interesa destacar: afirmamos que el software mantiene dependencia directa con la funcionalidad material específica del hardware

(SUM** es sinónimo de succión y no otra cosa), y que en cierto sentido sería independiente del tipo de materiales que compongan el hardware ¿pero, hasta qué punto?: una específica estructura material si tiene que ver con el tipo de material con que esta se construya, puesto que no toda sustancia posee la plasticidad y propiedades necesarias para configurar eficazmente una determinada estructura y funcionalidad material.

CAPITULO IV: ORGANIZACIÓN DEL CENTRO DE CÓMPUTO.

Forma de operar un centro de cómputo.

Un Centro de Cómputo, es el conjunto de recursos físico, lógicos, y humanos necesarios para la organización, realización y control de las actividades informáticas de una empresa.

Las principales funciones que se requieren para operar un centro de cómputo son las siguientes:

- ✓ Operar el sistema de computación central y mantener el sistema disponible para los usuarios.
- ✓ Ejecutar los procesos asignados conforme a los programas de producción y calendarios preestablecidos, dejando el registro correspondiente en las solicitudes de proceso.
- ✓ Revisar los resultados de los procesos e incorporar acciones correctivas conforme a instrucciones de su superior inmediato.
- ✓ Realizar las copias de respaldo (back-up) de la información y procesos de cómputo que se realizan en la Dirección, conforme a parámetros preestablecidos.
- ✓ Marcar y/o señalar los productos de los procesos ejecutados.
- ✓ Llevar registros de fallas, problemas, soluciones, acciones desarrolladas, respaldos, recuperaciones y trabajos realizados.
- ✓ Velar porque el sistema computarizado se mantenga funcionando apropiadamente y estar vigilante para detectar y corregir fallas en el mismo.
- ✓ Realizar labores de mantenimiento y limpieza de los equipos del centro de cómputo.
- ✓ Aplicar en forma estricta las normas de seguridad y control establecidas.
- ✓ Mantener informado al jefe inmediato sobre el funcionamiento del centro de cómputo.

- ✓ Cumplir con las normas, reglamentos y procedimientos establecidos por la Dirección para el desarrollo de las funciones asignadas.

PRINCIPALES DEPARTAMENTOS DE UN CENTRO DE CÓMPUTO.

Dentro de una empresa, el Centro de Cómputo ó Centro de Proceso de Datos cumple diversas funciones que justifican los puestos de trabajo establecidos que existen en él, las cuales se engloban a través de los siguientes departamentos:

- Explotación de sistemas o aplicaciones. La explotación u operación de un sistema informático o aplicación informática consiste en la utilización y aprovechamiento del sistema desarrollado. Ésta constituye el departamento o área de operación del sistema(s) con los que cuenta la organización. Consta de previsión de fechas de realización de trabajos, operación general del sistema, control y manejo de soportes, seguridad del sistema, supervisión de trabajos, etc.
- Soporte técnico a usuarios. El soporte, tanto para los usuarios como para el propio sistema, se ocupa de seleccionar, instalar y mantener el sistema operativo adecuado, del diseño y control de la estructura de la base de datos, la gestión de los equipos de teleproceso, el estudio y evaluación de las necesidades y rendimientos del sistema y, por último, la ayuda directa a usuarios.
- Gestión y administración del propio Centro de Cómputo. Las funciones de gestión y administración de un Centro de Procesamiento de Datos engloban operaciones de supervisión, planificación y control de proyectos, seguridad y control de proyectos, seguridad general de las instalaciones y equipos, gestión financiera y gestión de los propios recursos humanos.

PLANIFICACIÓN DE UN CENTRO DE CÓMPUTO.

En la actualidad se le reconoce a un Centro de Cómputo como un lugar donde se encuentra muchas computadoras trabajando sobre diferentes tipos de esquemas, estos pueden ser de tipo laboral, educativo, entretenimiento, etc., pero no solo en un lugar donde se puede trabajar, es una de las herramientas más importantes en la actualidad para el desarrollo profesional y laboral de las personas. De esta forma llegamos a realizar la siguiente pregunta ¿Cómo optimizar el funcionamiento del centro de Cómputo para proporcionar un servicio eficiente?

Los recursos con los que debe de contar un Centro de Cómputo son los necesarios para que cualquier negocio o empresa funcione adecuadamente esto es: Recursos humanos, materiales, financieros, estructurales y tecnológicos; de los cuales este último se constituye como el más importante derivado de su explosiva evolución. Y es aquí donde radica la importancia de una correcta planificación de inversión y administración adecuada de los recursos informáticos.

Adquisición de software y hardware.

Selección de Software.

Los criterios para seleccionar software son:

2. Software: Conjunto de programas o listas de instrucciones codificadas los cuales le permiten a la computadora realizar una o varias funciones. Varía de acuerdo al nivel:
 - Básico. Sistema Operativo (Seleccionar por Standard Mundial).
 - Soporte: Base de datos (Seleccionar por Standard Mundial).

3. Proveedor: Las características que debe tener el proveedor de informática son:

- Reconocido prestigio mundial y nacional.
- Soporte técnico en instalación.
- Ayuda en problemas.
- Personal especializado.
- Tiempo de atención.
- Comunicación rápida.
- Servicios de capacitación: cursos, material, expositor, costos.
- Cartera de clientes de software iguales al adquirido.
- Documentación: Facilidad de uso.

4. Costos: Se considerará lo siguiente:

- Condición de pago.
- Local.
- Inclusión de entrenamiento.
- Costos de mantenimiento.

Selección de Hardware.

Los criterios para seleccionar hardware son:

a) Equipos:

- La configuración debe estar acorde a las necesidades de la carga del procesamiento de datos.

- Debe tener una capacidad de crecimiento vertical (en el mismo equipo), horizontal (con otros equipos).
- Fabricante de calidad (muy bueno), reconocido prestigio mundial.
- Tiempo de garantía.
- Tecnología de "punta" (Alta)

b) Proveedor. Debe tener las siguientes características:

- Reconocido prestigio local.
- Soporte de mantenimiento: personal especializado, stock de repuestos.
- Tiempo de atención, local apropiado, comunicación rápida.
- Cartera de clientes con equipos equivalentes a los adquiridos.
- Tiempo de entrega oportuno.

c) Precios. Se debe considerar lo siguiente:

- Condiciones de pago.
- Detallado por componentes de la configuración.
- Descuentos por volumen.
- Costo de mantenimiento.

Adquisición de Software

El software para Computadores se puede clasificar en los siguientes tipos:

- Sistema operacional: Es el conjunto de programas que controla las actividades operativas de cada Computadora y de la Red.

- **Paquete de Usuario Final:** Mediante los cuales el usuario de un manera sencilla elabora sus procesos, por ejemplo, hojas de calculo, manejadores de bases de datos, procesadores de palabras, etc.
- **Paquete de Sistemas Aplicativos:** En los que a diferencia de los anteriores, el usuario es simplemente quien los usa. La programación y el desarrollo es compleja, realizada por el Departamento de Sistemas o adquiridos a proveedores externos, por ejemplo, sistema de nomina, sistema de Contabilidad, sistemas de Inventarios, etc.
- **Software Autorizado:** Se considera como Software autorizado, tanto los sistemas operacionales como aquellos paquetes de usuario final y de sistemas aplicativos, que el departamento de sistemas ha instalado, previo visto bueno para su adquisición y con la Autorización legal del proveedor para su uso.

Adquisición del Hardware

La selección del modelo y capacidades del hardware requerido por determinada dependencia, debe ir de acuerdo con el plan estratégico de sistemas y sustentado por un estudio elaborado por el departamento de sistemas, en el cual se enfatizan las características y volumen de información que ameritan sistematización y diferencian los tipos de equipos que se adjudican a las diversas áreas usuarias. Todo estudio determina una configuración mínima para el Computador y los aditamentos o dispositivos electrónicos anexos como unidades externas, impresoras, tarjetas y módems para comunicaciones, elementos para “backups” en cintas magnéticas, etc.; de acuerdo con las necesidades del usuario, así como una evaluación del costo aproximado de la inversión.

Consideraciones generales para la Adquisición de Software y Hardware.

Para realizar cualquier adquisición de Software o Hardware, se deberán considerar los siguientes puntos:

- Solicitud de propuesta. Todo sistema se origina en base a una solicitud que hace el usuario al centro de cómputo, intentando satisfacer una necesidad específica. Los parámetros sobre los cuales debe medirse dicha solicitud son los objetivos y las políticas, los cuales debe fijar el usuario, aunque puede ser que el departamento de análisis le brinde ayuda en su clarificación. Ambos parámetros deben quedar establecidos por escrito.
- Evaluación de propuesta. Previamente debe llevarse a cabo una investigación con el propósito de establecer con seguridad el tipo de Software y Hardware requerido para su implementación, posteriormente se integra toda la información obtenida de dicha investigación y así poder establecer la operatividad de los sistemas a adquirirse.
- Financiamiento. Las fuentes de financiamiento pueden ser principalmente instituciones bancarias a través de créditos. Para el caso de centros de cómputo destinados a la educación pública no existen fuentes de financiamiento, a menos que la institución educativa cuente con un área destinada a la producción de software para empresas privadas, entonces la misma empresa puede ser el origen del financiamiento.
- Negociación de Contrato. La negociación de contrato debe incluir todos los aspectos de operación del Software y del Hardware a implementarse. Aspectos tales como: Actualizaciones, innovaciones, capacitación, asesoría técnica, etc.

Permisos y Licencias.

El uso de Software no autorizado o adquirido ilegalmente, se considera como *pirata* y una violación a los derechos de autor.

El uso de Hardware y de Software autorizado está regulado por las siguientes normas:

- Toda dependencia podrá utilizar UNICAMENTE el hardware y el software que el departamento de sistemas le haya instalado y oficializado mediante el "Acta de entrega de equipos y/o software".
- Tanto el hardware y software, como los datos, son propiedad de la empresa. Su copia o sustracción o daño intencional o utilización para fines distintos a las labores propias de la compañía, será sancionada de acuerdo con las normas y reglamento interno de la empresa.
- El departamento de sistemas llevara el control del hardware y el software instalado, basándose en el número de serie que contiene cada uno.
- Periódicamente, el departamento de sistemas efectuará visitas para verificar el software utilizado en cada dependencia. Por lo tanto, el detectar software no instalado por esta dependencia, será considerado como una violación a las normas internas de la empresa.
- Toda necesidad de hardware y/o software adicional debe ser solicitada por escrito al departamento de sistemas, quien justificará o no dicho requerimiento, mediante un estudio evaluativo.

- El departamento de sistemas instalará el software en cada computador y entregará al área usuaria los manuales pertinentes los cuales quedaran bajo la responsabilidad del Jefe del departamento respectivo.
- Los discos que contienen el software original de cada paquete serán administrados y almacenados por el departamento de sistemas.
- El departamento de sistemas proveerá el personal y una copia del software original en caso de requerirse la reinstalación de un paquete determinado.
- Los trámites para la compra de los equipos aprobados por el departamento de sistemas, así como la adecuación física de las instalaciones serán realizadas por la dependencia respectiva.
- La prueba, instalación y puesta en marcha de los equipos y/o dispositivos, serán realizada por el departamento de sistemas, quien una vez compruebe el correcto funcionamiento, oficializara su entrega al área respectiva mediante el "Acta de Entrega de Equipos y/o Software".
- Una vez entregados los equipos de computación y/o el software por el departamento de sistemas, estos serán cargados a la cuenta de activos fijos del área respectiva y por lo tanto, quedaran bajo su responsabilidad.
- Así mismo, el departamento de sistemas mantendrá actualizada la relación de los equipos de computación de la compañía, en cuanto a número de serie y ubicación, con el fin que este mismo departamento verifique, por lo menos una vez al año su correcta destinación.
- El departamento de sistemas actualizará el software comprado cada vez que una nueva versión salga al mercado, a fin de aprovechar las mejoras realizadas a los programas, siempre y cuando se justifique esta actualización.

Derechos de autor y licencia de uso de software.

El Copyright, o los derechos de autor, son el sistema de protección jurídica concebido para titular las obras originales de autoría determinada expresadas a través de cualquier medio tangible o intangible.

Las obras literarias (incluidos los programas informáticos), musicales, dramáticas, plásticas, gráficas y escultóricas, cinematográficas y demás obras audiovisuales, así como las fonogramas, están protegidos por las leyes de derechos de autor. El titular de los derechos de autor tiene el derecho exclusivo para efectuar y autorizar las siguientes acciones:

- Realizar copias o reproducciones de las obras.
- Preparar obras derivadas basadas en la obra protegida por las leyes de derechos de autor.
- Distribuir entre el público copias de la obra protegida por las leyes de derechos de autor mediante la venta u otra cesión de la propiedad, o bien mediante alquiler, arrendamiento financiero o préstamo.
- Realizar o mostrar la publicidad de la obra protegida por las leyes de derechos de autor.
- Importar el trabajo, y realizar actos de comunicación pública de las obras protegidas.

INSTALACIONES FÍSICAS DEL CENTRO DE CÓMPUTO

Se establece a continuación criterios ideales para establecer la correcta y segura disposición física del centro de cómputo en las organizaciones: Edificio, área y espacio:

Edificio.

Es trascendental la ubicación del edificio y su construcción misma para la operación eficiente del centro de cómputo y como primera medida, debe considerarse si se trata de un

edificio nuevo de construir o uno ya existente a adecuarse, para ello se mencionan los siguientes puntos:

- a) Realizar un estudio de la zona a fin de evitar estar expuestos al peligro por sismos, contaminación, incendio, explosión, inundación, radiaciones, interferencia de radar, vandalismo, disturbios sociales, así como riesgos provocados por las industrias cercanas y todo lo que pueden ocasionar problemas con el equipo de procesamiento de datos y archivos.
- b) Seleccionar la parte más segura dentro del edificio para el centro de cómputo y contar con facilidades de energía eléctrica, acometidas telefónicas, aire acondicionado, servicios públicos y salida de emergencia adecuada.
- c) Cuando el acceso al centro de cómputo deba efectuarse a través de otros departamentos, será necesario prever el paso de las máquinas a través de diferentes puertas, ventanas, pasillos, montacargas, etc. Los elevadores deberán soportar cuando menos una carga estándar de 1135kg. (2500 lbs.) y ser lo suficientemente largos para acomodar los equipos en este.
- d) Se deben definir claramente las rutas de acceso del personal para la carga de documentos, respaldos en unidades magnéticas, elaboración de reportes, etc., cuidando que no existan sobre el piso escalones, rampas, cables, etc.
- e) La construcción del piso debe soportar el peso de los equipos que serán instalados. Las designaciones típicas de los equipos IBM no rebasan de los 340kg/m².
- f) La puerta de acceso al centro de cómputo debe tener 95cm. de ancho mínimo y abrir hacia afuera.
- g) Se deben de usar materiales de construcción no combustible y resistente al fuego.

- h) Recubrir las paredes con pintura lavable, con el objeto de que no se desprenda polvo y sea fácil su limpieza.
- i) Construir el mínimo de ventanas exteriores (o ninguna) a fin de evitar interferencias.
- j) Si el falso plafón se utiliza como pleno para el retorno del aire acondicionado, deberá pintarse el techo real con pintura de aceite o sintética de color claro.

Área y Espacio

Se recomienda que en el área del centro de cómputo existan separadores de aluminio y cristal o cuartos independientes para la instalación de todo el equipo y debemos considerar lo siguiente:

- a) La configuración definitiva del sistema a instalar: el procesador, impresoras, estaciones de trabajo, módems, multiplexores y demás periféricos.
- b) Para hacer una distribución adecuada se deberá poseer un plano del local elegido en escala 1:50 sobre el que se ubicarán las plantillas de los equipos cuidando sus áreas de servicio y pruebas (espacio adicional al área del equipo para su mantenimiento).
- c) Es necesario plantear la secuencia de conexión de los equipos para los direccionamientos de los mismos.
- d) Se recomienda la ubicación de la consola del sistema como máximo a 6 metros de distancia del rack del procesador y que sea visible el panel de control del mismo.
- e) Por el polvo que desprenden las impresoras y el ruido que hacen al imprimir, se deben instalar en un cuarto independiente junto con una estación de trabajo a un metro de distancia de la impresora del sistema para facilitar el suministro de los reportes.
- f) Se debe tener en cuenta el espacio a ocupar del equipo adicional como son: Comunicaciones, módems, teléfonos, no-break, un archivo mínimo, cintas de respaldo,

una mesa de trabajo, mueble para manuales y papelería, además del espacio para futuro crecimiento.

Energía Eléctrica y Tierra Física

Instalación Eléctrica

La instalación eléctrica es un factor fundamental para la operación y seguridad de los equipos en el que se debe completar el consumo total de corriente, el calibre de los cables, la distribución efectiva de contactos, el balanceo de las cargas eléctricas y una buena tierra física. Una mala instalación provocaría fallas frecuentes, cortos circuitos y hasta que se quemen los equipos.

La instalación eléctrica para el área de sistemas, debe ser un circuito exclusivo tomado de la sub-estación o acometida desde el punto de entrega de la empresa distribuidora de electricidad, usando cables de un solo tramo, sin amarres o conexiones intermedias. Para el cálculo de la línea se debe tomar un factor de seguridad de 100% en el calibre de los conductores para una caída máxima de voltaje de 2%. Se debe construir una tierra física exclusiva para esta área, la cual se conecte a través de un cable con cubierta aislante al centro de carga del área de cómputo.

Construcción de la Tierra Física

- a) Se deberá elegir un jardín o lugar en donde exista humedad, en caso contrario es necesario colocar un ducto que aflore a la superficie para poder humedecer el fondo.
- b) Hacer un pozo de 3 metros de profundidad y 70 centímetros de diámetro.
- c) En el fondo se debe colocar una capa de 40 cm. de carbón mineral sobre la cual descansará una varilla copperwel.

- d) Encima del carbón se deberá agregar una capa de sal mineral de 5 cm. y otra de pedacería de aluminio y cobre de 40 cm., cubriéndose después con tierra hasta la superficie.
- e) El tablero principal para el equipo del computador se debe proveer trifásico y con doble bus de tierra, (5 hilos), uno para el neutro eléctrico y otro para proveer tierra física a las maquinas.
- f) Como una medida de seguridad deberá instalarse en un lugar próximo a la puerta un control para cortar la energía a todo el equipo de cómputo en cualquier situación de emergencia, y deberá estar debidamente señalizado.
- g) El espacio próximo al control de interruptores debe permanecer libre de obstáculos para su fácil operación.
- h) Se deberá tener tantos circuitos como máquinas estén indicadas que deben llevar conector, esto es: La unidad central de proceso, impresoras, unidades de control de discos, cintas, comunicaciones, pantallas, etc. La protección de estos circuitos debe ser interruptor termo-magnético. Se deben tener circuitos extras para cubrir ampliaciones con las características de los circuitos trifásicos y monofásicos.

Todos los conductores eléctricos hacia el centro de carga de la sala deben instalarse bajo tubería metálica rígida y de diámetro adecuado, debidamente conectadas a tierra. Los circuitos a cada unidad deben estar en tubo metálico flexible, en la proximidad de la maquina que alimentarán, para evitar transferencia de energía radiante de los mismos, a los cables de señal del computador y por otra para evitar peligros de incendio.

Los circuitos de la unidad central de proceso, impresoras, unidades de control de discos, cintas, comunicaciones, se debe rematar con conectores tipo industrial a prueba de agua y explosión Rusell & Stollo equivalente.

Todos los interruptores deben estar debidamente rotulados para su rápida operación por parte del personal autorizado. Para las conexiones de los contactos polarizados 125 VCA 3 hilos, debe utilizarse el código de colores:

FASE: Negro, rojo o azul

NEUTRO: Blanco o gris

TIERRA FÍSICA: Verde

Al efectuar los cálculos de la instalación eléctrica al tablero del equipo, los conductores, reguladores de tensión, interruptores termo-magnéticos, etc., se deben calcular teniendo en cuenta la corriente de arranque de cada máquina, la cual generalmente es superior a la nominal. Dicha corriente de arranque debe poder ser manejada sin inconvenientes, por todos los elementos constitutivos de la instalación. Se debe considerar una expansión del 50% como mínimo.

Línea Eléctrica Independiente para Servicios

El uso de herramientas eléctricas para la limpieza o cualquier otro trabajo (aspiradora, taladro, pulidora, etc.) dentro del área de cómputo o en sus proximidades, implica las necesidades de que estas sean utilizadas conectándolas en una línea eléctrica que no sea utilizada por las

máquinas componentes del sistema, para evitar las perturbaciones electromagnéticas que pudieran producir, las cuales afectan el trabajo que realiza el computador.

Placa contra Transientes Eléctricos

En construcciones nuevas de locales para centros de cómputo, es necesario prever una placa de aluminio de 1 metro cuadrado, ahogada en concreto, debajo del piso falso y frente al tablero principal de distribución eléctrico a las diferentes máquinas del sistema.

Estas placas deberán unirse eléctricamente al tablero de distribución eléctrico, de modo que forme una capacidad contra el plano de tierra del piso falso. La línea de conexión entre la placa con transientes con el tablero de distribución, no debe exceder de 1.5 metros de largo.

Regulador de Voltaje

Es indispensable la instalación de un regulador de voltaje para asegurar que no existan variaciones mayores al $\pm 10\%$ sobre el valor nominal especificado, que dé alta confiabilidad, protección total de la carga y rechace el ruido eléctrico proveniente de la línea comercial contaminada por motores, hornos, etc., éste deberá soportar la corriente de arranque con baja caída de tensión y estar calculado para las necesidades del sistema y la ampliación futura que se estime necesaria.

La regulación debe ser rápida efectuando la corrección para cualquier variación de voltaje o de carga entre 1 y 6 ciclos.

Las variaciones que soportan los equipos son las siguientes:

Tolerancia de voltaje Tolerancia de frecuencia

115 volts +10% -10%

60 Hz. +-1/2 Hz.

208 volts

+6% -8%

Se requiere instalar un arrancador electromagnético con estación de botones, para proteger los equipos que no estén soportados por el UPS, de sobretensiones al momento de cortes de energía momentáneos y que estén únicamente con regulador de voltaje, el cual al momento de cualquier corte eléctrico, des-energizará los equipos y cuando regrese la corriente eléctrica, no entrará de lleno a los mismos si no hasta que una persona active el botón de arranque.

Fuente Ininterrumpida de Energía (UPS)

Para proteger de fallas de energía eléctrica comercial y evitar pérdida de información y tiempo en los procesos de cómputo de los equipos, se requiere de un UPS el cual abastezca eléctricamente como mínimo al equipo procesador, la impresora del sistema y la consola del sistema.

El uso de una fuente interrumpida de energía evita fallas en los sistemas de cómputo entregando una tensión:

- a) De amplitud y frecuencia controlada.
- b) Sin picos ni ciclos faltantes.
- c) En fase y redundante con la línea externa, independiente del comportamiento de la red comercial.

El UPS en condiciones normales de energía comercial funciona como un regulador de voltaje, y en una baja o corte de energía, entra la carga de las baterías (Battery Backup) de un modo sincronizado que le es transparente al funcionamiento de los equipos.

Una vez restablecida la energía, las baterías se recargan automáticamente.

Estática

Una de las fallas más difíciles de detectar en los equipos es ocasionada por la electricidad estática producida por la fricción entre dos materiales diferentes y la consiguiente descarga de este potencial. Los materiales que son más propensos a producir estática son aquellos que están hechos de resina, plásticos y fibras sintéticas.

El simple hecho de arrastrar una silla sobre el piso nos ocasionará que tanto la silla como la porción del piso sobre el que se arrastró queden cargadas de electricidad estática. Si aquella silla o esta persona son aproximadas a una mesa metálica conectadas a tierra como los equipos de cómputo, ocasionará que se produzca una descarga que puede ser o no sensible a una persona, pero sí será sensible a los equipos de cómputo.

Para reducir al mínimo la estática, se recomienda las siguientes medidas:

- a) Conectar a tierra física tanto el piso falso como todos los equipos existentes.
- b) El cable para la tierra física deberá ser recubierto y del mismo calibre que el de las fases y el neutro.
- c) La humedad relativa deberá estar entre 45% +/- 5% para que las cargas estáticas sean menos frecuentes.
- d) Se recomienda usar cera antiestática en el piso.
- e) Si existieran sillas con ruedas, se recomienda que estas sean metálicas.

Los fabricantes de los equipos de cómputo presentan en sus manuales los requerimientos ambientales para la operación de los mismos, aunque estos soportan variación de temperatura, los efectos recaen en sus componentes electrónicos cuando empiezan a degradarse y ocasionan fallas frecuentes que reduce la vida útil de los equipos.

Se requiere que el equipo de aire acondicionado para el centro de cómputo sea independiente por las características especiales como el ciclo de enfriamiento que deberá trabajar día y noche aún en invierno y las condiciones especiales de filtrado. La alimentación eléctrica para este equipo debe ser independiente por los arranques de sus compresores que no afecten como ruido eléctrico en los equipos de cómputo. La determinación de la capacidad del equipo necesario debe estar a cargo de personal competente o técnicos de alguna empresa especializada en aire acondicionado, los que efectuarán el balance térmico correspondiente como es:

1. Para Calor Sensible.

Se determinan ganancias por vidrio, paredes, particiones, techo, plafón falso, piso, personas, iluminación, ventilación, puertas abiertas, calor disipado por las máquinas, etc.

2. Para Calor Latente.

Se determina el número de personas y la ventilación.

La inyección de aire acondicionado debe pasar íntegramente a través de las máquinas y una vez que haya pasado, será necesario que se obtenga en el ambiente del salón una temperatura de $21^{\circ}\text{C} \pm 2^{\circ}\text{C}$ y una humedad relativa de

45% +/- 5%, así como también en la cinta teca. Es necesario que el equipo tenga controles automáticos que respondan rápidamente a variaciones de +/- 1°C y +/-5% de humedad relativa.

Estas características de diseño también han demostrado ser de un nivel de confort bueno y aceptado por la mayoría de las personas.

Se recomienda mantener las condiciones de temperatura y humedad las 24 horas del día y los 365 días del año, puesto que las cintas, disquetes, papel, etc., deben estar en las condiciones ambientales indicadas antes de ser utilizados.

Debe tenerse en cuenta que una instalación de aire acondicionado debe proveer como mínimo el 15% de aire de renovación por hora, por el número de personas que en forma permanente consumen oxígeno y expelen anhídrido carbónico, si no se considera, al cabo de un tiempo de operación comienzan a manifestarse malestares como dolor de cabeza, cansancio o agotamiento y disminuyen en el rendimiento del personal.

No deben usarse equipos de aire acondicionado de ventana que no regulen la humedad ni filtren el aire, porque los gases de la combustión de motores y polvo es aspirado y enviado al centro de cómputo.

El polvo y gases corrosivos pueden provocar daños en el equipo, una concentración alta de gases tales como dióxido de sulfuro, dióxido de nitrógeno, ozono, gases ácidos como el cloro, asociados con procesos industriales causan corrosión y fallas en los componentes electrónicos. Este tipo de problemas son usuales en las ciudades muy contaminadas, por lo que se debe tener en cuenta en el diseño del aire acondicionado instalar filtros dobles o de carbón activado de tal manera que forme un doble paso de filtro de aire, con objeto de evitar causarle daño a las

máquinas del sistema y degradaciones en sus componentes electrónicos. Todos los filtros que se usen no deberán contener materiales combustibles.

Para mantener constante la humedad relativa, es necesario que el equipo de aire acondicionado se le adicione un humidificador en el ducto de inyección principal.

Un higrómetro de pared en el ambiente de la sala debe controlar al humidificador para el arranque y parada del compresor únicamente. Las unidades manejadoras de aire deberán trabajar en forma continua. El termostato y el higrómetro deberán responder a variaciones de 1°C y 5% de humedad relativa. Una alta humedad relativa puede causar alimentación de papel impropio, accionamiento indebido de los detectores de humo e incendio, falta de confort para el operador y condensación sobre ventanas y paredes cuando las temperaturas exteriores son inferiores a las del centro de cómputo. Una baja humedad relativa crea la facilidad para que con el movimiento de personas, sillas rodantes, papel y mobiliarios generen la electricidad estática. El mejor método de distribución de aire para el centro de cómputo es el de usar el piso falso para la salida de aire y el plafón falso para el retorno mismo. Debe preverse una renovación de aire mayor al 15 %.

Iluminación y Acústica

Iluminación

Es muy importante contar con buena iluminación en toda el área, que facilite la operación de los equipos y para el mantenimiento de los mismos. Si es posible, se deben instalar todas las estaciones de trabajo alineadas en paralelo, de tal forma que las lámparas en el techo queden directas a los costados de las pantallas. Para evitar la fatiga de la vista es necesario instalar lámparas fluorescentes blancas compatibles con la luz del día y pintar la oficina con colores tenues y el techo blanco para activar la reflexión.

Debe evitarse que lleguen los rayos directos del sol, para observar con claridad las distintas luces y señales de la consola y tableros indicadores de los equipos. Los circuitos de iluminación no se deben tomar del mismo tablero eléctrico que para alimentar los equipos de cómputo. El nivel de iluminación corresponde a 40 watts por metro cuadrado de superficie de salón, usando lámparas fluorescentes.

Acústica

El total del nivel de ruido en el centro de cómputo, es acumulado por todos los ruidos del salón es afectado por los arranques físicos de los motores de los equipos y los movimientos en la operación. Para proveer una mayor eficiencia y una operación confortable, se recomienda aplicar material acústico en paredes y techos del salón, como son texturas a base de tirol o recubrimientos de enjarres.

Piso Falso

El piso falso de la facilidad de distribuir el aire acondicionado de una manera más eficiente para el enfriamiento de los equipos, ocultar el cableado de instalación eléctrica y distribuir el cableado de sentido; al a las necesidades requeridas así como sus cambios de posición y mantenimientos. Se pueden mencionar algunas de las ventajas al usar el piso falso:

- a) Permite un espacio entre el piso real y el piso falso, que se puede usar como cámara plena para el aire acondicionado, facilita la distribución y salida del mismo donde se requiera.
- b) Proveer una superficie uniforme y plana que cubra todos los cables de señal de interconexión, cajas, cables y boas de alimentación de energía eléctrica, líneas telefónicas y de comunicaciones, etc.
- c) Permite cambios de distribución de los equipos o ampliaciones de los mismos con el mínimo de costo y tiempo.

- d) Es construido por paneles antiestáticos por una densa barrera termo acústica, envuelto con lámina electro galvanizada, proporcionando solidez para un soporte de cargas óptimo resistente a la humedad y al fuego.
- e) La base guarda uniformidad estructural para soportar cargas distribuidas en un área mínima de 40cm cuadrados.
- f) Los pisos falsos metálicos, presentan la facilidad de ser conectados a tierra en diferentes puntos, lo cual ayuda a descargar la estática que se produce en las superficies.

El piso falso debe ser de módulos intercambiables de 61x61 cm. Y pueden ser contruidos de acero, aluminio, hierro, etc. En el caso de los pisos de madera, la parte inferior de las losas deberá quedar recubierta con la termina metálica, de tal forma que al descansar sobre los pedestales la placa haga contacto físico y forme un plano de tierra elevado, que facilite la descarga electrostática. Esto implica que los pedestales deberán ser conecta dos a tierra, lo cual se comprobará previamente a la instalación de sistema.

La carga de algunos equipos en sus puntos de apoyo puede ser de hasta 455 kg. (1000 lbs.), por lo que le piso falso debe ser capaz de soportar cargas concentradas de 455 kg. En cualquier punto con una máxima deflexión de 2mm.

Si el espacio entre el piso real y el piso falso se usa como cámara plena, es necesario que tanto el firme del piso como el de las paredes que limitan la cámara no desprendan polvo en absoluto y sean tratadas deberá estar sellada lo más herméticamente posible, para evitar fugas de aire o para evitar que entre polvo y basura. Es necesario un escalón o rampa de acceso al centro de cómputo para igualar los niveles de piso, por seguridad el escalón o rampa deberá ser del

mismo material del piso falso y estar recubierta con hule estriado perpendicular a la dirección de circulación o acceso, y en caso de la rampa tener una elevación menor de 12°.

Ductos y Cableado de Señal

En un centro de cómputo donde existe gran variedad de cables necesarios para el funcionamiento y comunicación de los procesadores con sus equipos periféricos, tanto por seguridad como por cuidar los acabados en la decoración interior, los ductos son un factor de gran importancia para ocultar los cables de señal.

Aún contando con piso falso en el centro de cómputo se deben distribuirlos cables a través de canaletas o ductos especiales para cables reducen los costos de instalación dando una apariencia ordenada y facilidad para el mantenimiento. Existen varios tipos de ductos son:

PVC, el cual es igual para la canalización aparente, METALICOS, NORYL,

POLYCARBONATO, etc., (los últimos dos soportan temperaturas arriba de los 125°C).

El sistema modular de cableado de comunicación permite conducir cables para voz, datos, video, fibra óptica y electricidad en canales independientes y cuenta con toda la gama de conectores RJ-11, RJ-45, F. TWINAX. BNC. TOKEN-RING. RCA, etc., tanto en PLUG, JACK, ADAPTADOR O RECEPTACULO. Nunca deberá conducir señal y electricidad por la misma tubería o ducto.

Cable Coaxial:

El tipo de cable para la conducción de señal de datos coaxial o twinaxial provee un alto rango de inmunidad a las interferencia electromagnéticas y de radiofrecuencia, lo cual es de suma

importancia contaminados o zonas con interferencias, también alcanza distancias más grandes para la transmisión de señal en comparación con el cable de par trenzado (twisted pair).

Cable Par Trenzado (Twisted Pair):

Hoy en día el sistema de cableado estructurado ha dado las facilidades de convertir un departamento, área o edificio en inteligente, donde cada oficina cuente con los servicios de señal que necesite utilizando el cableado de par trenzado (twisted pair).

Este cableado estructurado consiste en un sistema de distribuidores donde en uno le llega las señales de voz, datos o video de los equipos o procesadores y el otro distribuidor es la concentración de todos los cables que llegan de las oficinas y en este se realiza el patcheo de la señal o servicio requeridos.

Cable de Fibra Óptica:

La fibra óptica es el medio de transmisión de hoy y del futuro, es de alto grado de inmunidad a las interferencias electromagnéticas y cumple con el ancho de banda requerido para las aplicaciones de alta velocidad de datos. La fibra óptica es últimamente aplicada como medio de transmisión entre los pisos de un edificio como BACKBONE.

Seguridad

La seguridad es un factor de suma importancia al planear la instalación física de un centro de cómputo. Esta consideración se refleja en la elección de las normas a considerar para la ubicación del procesador, materiales utilizados para su construcción, equipo de detectores y protección contra incendios, sistema de aire acondicionado, instalación eléctrica, sistema de control de acceso y el entrenamiento al personal u operadores.

2. Situación del Área del Procesador

- a) El área de los procesadores no debe situarse encima, debajo o adyacente a áreas donde se procesen, fabriquen o almacenen materiales inflamables, explosivos, gases tóxicos, sustancias radiactivas, etc.
- b) No debe existir material combustible en el techo, paredes o piso y debe ser resistente al fuego (mínimo una hora).
- c) Todas las canalizaciones, ductos y materiales aislantes, deben ser no combustibles y que desprendan poco polvo.

3. Almacenamiento de Información

- a) Cualquier información almacenada en el centro de proceso, como listados, diskettes, cintas, etc..., debe estar guardados en gavetas metálicas o resistentes al fuego.
- b) La sintética deberá estar construida con un rango de resistencia al fuego de por lo menos dos horas y debe ser utilizada sólo para este fin.
- c) Se deberá contar con un lugar seguro e independiente del centro de proceso para custodiar los dispositivos magnéticos de respaldo, ya sea en bóvedas o en cajas fuertes, de preferencia en otro edificio.

4. Equipos Contra Incendios

- a) La mejor prevención contra incendios consiste en emplear materiales no combustibles o en su defecto, tratarlos con pinturas, impregnaciones u otros que impidan o retarden su inflamación.
- b) Debe instalarse un sistema de detección de humo e incendio distribuido por toda el área, tanto debajo del piso falso, en las salidas de aire acondicionado, en el falso plafón como

las visibles en el techo. Este sistema de detección debe activar una alarma, la que avisara al personal para efectuar el plan de contingencia ya establecido.

- c) Deben emplearse suficientes extintores portátiles de bióxido de carbono. Este es el agente recomendado para el equipo eléctrico (fuego clase "C"). La ubicación de los extinguidores debe estar marcada en el techo y ser accesible a las personas que trabajan en el área. Además, deben poder ser retirados con facilidad en caso de necesidad. Estos extintores deben ser inspeccionados una vez por año como mínimo y las instrucciones para su uso deben ser colocadas al lado de los mismos e incluidas en el programa de seguridad.
- d) Es aconsejable colocar una boca de agua con manguera a una distancia efectiva del centro de proceso, como agente extintor secundario para escritores, sillas, muebles, etc. (fuego clase "A").

5. Luces de Emergencia

Se recomienda el uso de luces de emergencia alimentadas del UPS (Uninterruptible Power Supply) o con baterías, que automáticamente se encienden ante una falta de energía eléctrica comercial.

6. Seguridad del Personal

- a) El centro de cómputo debe estar construido y amueblado de manera que no se presenten lugares de peligro para el personal, como son: puertas enteras de vidrio sin indicadores en el mismo, lámparas de vidrio sin una protección adecuada, etc.
- b) Las salidas deben estar claramente marcadas y los pasillos del salón que los conducen, deben permanecer sin obstrucciones.

- c) Las áreas de servicios recomendadas para todos los sistemas y equipos auxiliares deben ser siempre respetadas

7. Seguridad Contra Inundaciones

- a) Si el centro de cómputo en la planta baja o en el sótano, es importante que se considere y elimine cualquier posibilidad de inundación.
- b) Eleve 20cm. su piso normal y verifique que en el área y sus alrededores haya buen sistema de drenaje y que este funcione adecuadamente.
- c) Coloque una protección adicional en las puertas a fin de evitar que se introduzca en el agua, en caso de que ésta subiera arriba de los 20cm o hasta el nivel del piso falso

8. Seguridad para el Acceso al Centro de Cómputo

- a) El centro de cómputo debe tener una sola entrada para controlar el acceso a la instalación. Las puertas adicionales para salida de emergencia sólo podrán ser abiertas desde adentro y deberán estar siempre cerradas. Estas puertas de acceso único, permitirá tener un mejor control del paso al centro de cómputo, tanto del personal como visitantes.
- b) Dependiendo de factores tales como el edificio en donde está instalado el centro de cómputo albergue otras funciones, es primordial el hecho de evitar el libre acceso a áreas restringidas. La identificación de las personas deberá ser total, antes de permitirles el paso hacia áreas más críticas
- c) Excepto para el personal de servicio, no se debe permitir que cualquier visitante tenga acceso al centro de cómputo o sus alrededores. Si esto es requerido o necesario, dicho visitante deberá ser acompañado por el personal responsable autorizado o de vigilancia durante su permanencia en área. Tanto el personal de servicio como los visitantes deberán

ser llamados para revisión de cualquier objeto de mano que pretendan introducir al área restringida como: maletas, bolsas, portafolios, bultos, etc.

- d) El acceso puede ser mejor controlado por medio de cerraduras electromecánicas operadas a control remoto, previa identificación de la persona. Existen cerraduras eléctricas que se pueden abrir con tarjetas magnéticas programables o tableros de control con password (clave de acceso), cuya clave puede ser cambiada periódicamente y es posible registrar automáticamente las entradas, intentos de violación e inferir cuando se está haciendo mal uso de una clave confidencial.
- e) También existe dispositivos de monitoreo a base de cámaras de T.V. en circuito cerrado, de modo que una persona de vigilancia pueda estar checando simultáneamente todas aquellas áreas que son de fácil acceso desde el exterior del edificio y poder notificar oportunamente al vigilante más cercano sobre lo que considera sospechoso y que es necesario interceptar. Una comunicación directa entre todos los puntos de vigilancia mencionados y el puesto de monitoreo, es indispensable.
- f) La vigilancia personal es de los mejores medios de seguridad por lo que el personal deberá ser instruido para que vigile a cualquier persona que no conozca y que se encuentre dentro de la instalación y que en adición sepa que no está autorizada para permanecer ahí. Cuando menos una persona de cada turno deberá ser asignada como responsable de la seguridad interna.

9. Mantenimiento Preventivo

Es muy importante saber las condiciones de operación de los equipos y prevenir riesgos y efectos de problemas que puedan afectar la operación de los mismos, por lo que se recomienda que periódicamente se elaboren los calendarios y se realice el

mantenimiento preventivo oportunamente. Se recomienda contar con una póliza de mantenimiento de servicio de algún proveedor o con personal altamente capacitado para la realización del mantenimiento preventivo.

- a) Se deberá revisar las especificaciones en el manual de operación de cada equipo.
- b) Para los procesadores de datos se deberán checar: los errores del disco duro, cambiar los filtros de aire o en su defecto lavarlos, revisar la configuración del rack, limpiar las cabezas lectoras de las unidades de cintas diskette y cartucho, revisar cables flojos, remover y aspirar el polvo que pueda tener, revisar puertas abiertas, etc.
- c) Para las impresoras y demás periféricos revisar las bandas, engranes rodillos, tractores, motores, etc., se deberán cambiar partes muy gastadas.
- d) Para el piso falso y plafones, se deberán mantener aspirados y limpios sobre todo si se usan como cámara plena de aire acondicionado para que no suelte polvo para los equipos.
- e) El aire acondicionado por sus condiciones de uso que es exclusivo para el centro de cómputo y su funcionamiento es de las 24:00 hrs. del día todo el año, se requiere de un mantenimiento preventivo del compresor filtros de aire de la manejadora, etc.
- f) Los detectores de humo e incendio probarlos para que activen el sistema de alarmas y estén en condiciones de operación para cuando se requiera
- g) La instalación eléctrica, UPS y reguladores, checar que proporcionen los voltajes correctos, cables flojos o de falso contacto, interruptores, etc.

PROPUESTA

DESCRIPCIÓN DEL OBJETO DE ESTUDIO:

La Facultad de Contaduría y Ciencias Administrativas ubicada en Ciudad Universitaria consta con 5 edificios para el alumnado; en el edificio denominado A-2 se encuentra la dirección, control escolar y demás unidades administrativas, dentro de este edificio se encuentra también el centro de cómputo de dicha facultad el cual es nuestro objeto de estudio principal.

- La misión: Formar profesionales e investigadores en contaduría, administración e informática con: Excelente calidad, profunda y verdadera vocación humanista, elevados valores morales y comprometidos con las demandas del entorno económico y social, al cual nos debemos.
- La visión: Ser la mejor facultad en las ciencias contables, administrativas e informáticas, con trascendencia de orden mundial, en permanente búsqueda de modelos y sistemas innovadores.

OBJETIVO GENERAL:

Desarrollar un Sistema de Redes Internas que regule los procesos operativos de la Facultad y coadyuve en el desarrollo de habilidades informáticas, tanto del personal docente como del alumnado.

OBJETIVOS ESPECÍFICOS:

- Desarrollar Sistemas de Información que controlen el uso y aprovechamiento de los laboratorios, así como de las computadoras y la infraestructura informática de la Facultad.
- Instalación de redes internas que faciliten el desarrollo, manejo y control de procesos operativos, estadísticos y de registro de datos sistematizados para el control integral de la operatividad de la Facultad.
- Establecer programas de Capacitación para el Personal Docente, a través de modelos informáticos que faciliten los procesos de enseñanza, aprendizaje y el registro de sus resultados.

DESCRIPCIÓN DE FUNCIONES:

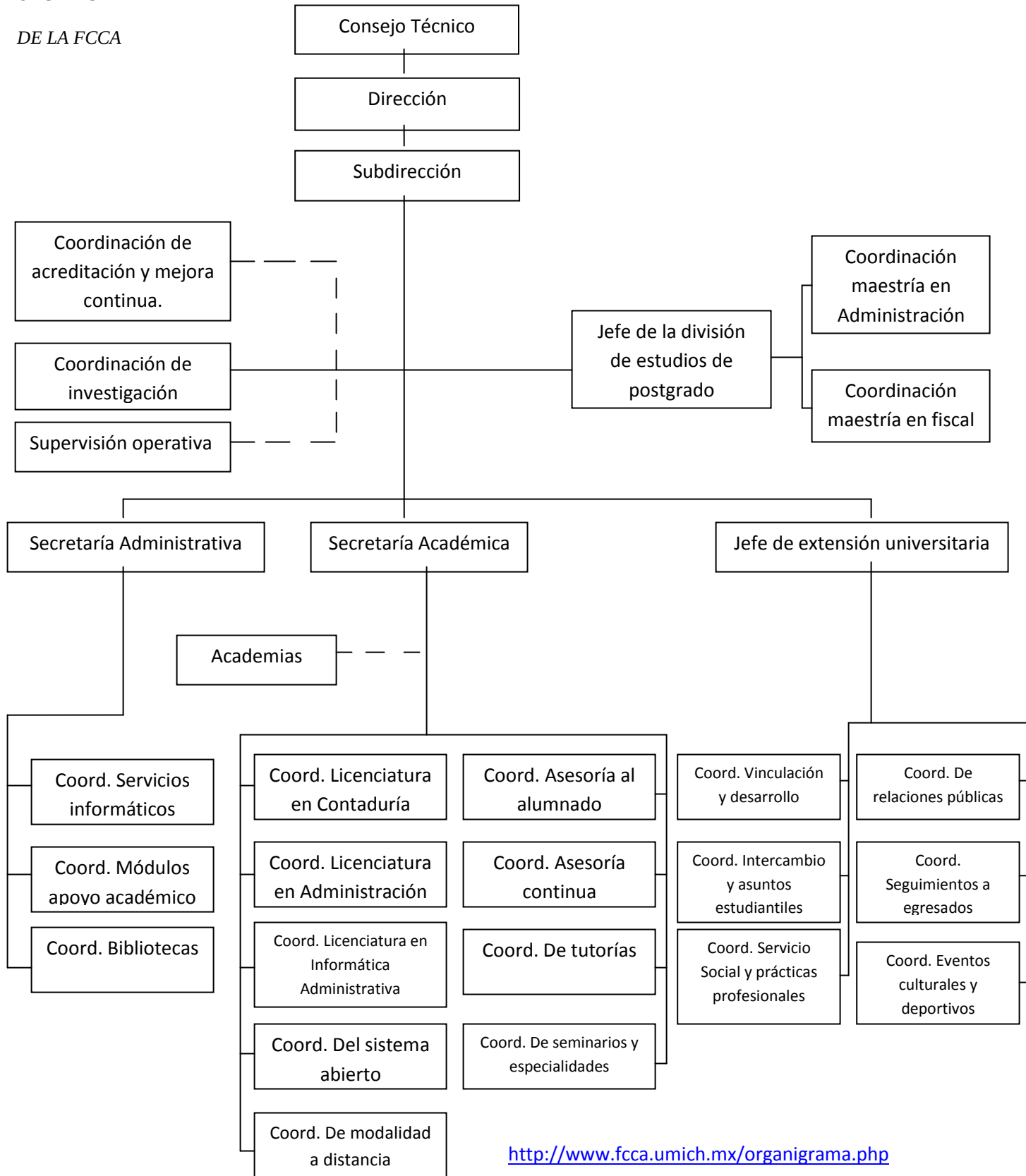
- ✓ Operar y coordinar el aprovechamiento de la infraestructura informática, para el registro de los procesos administrativos, financieros y estadísticos de la Facultad.

- ✓ Coordinar, con las áreas académicas y administrativas, el uso racional y óptimo de la infraestructura informática de redes, laboratorios y servicios; así como diseñar programas paralelos del mantenimiento.
- ✓ Contribuir en la preparación y diseño de material académico, de difusión masiva, cultural y artística así como sugerir los mecanismos de reproducción mas apropiados.
- ✓ Mantener actualizada la página de Internet de la Facultad.
- ✓ Ofrecer apoyo informático y procurar el desarrollo de programas específicos, para el manejo de la información que genera cada una de las áreas que conforman la estructura de la Facultad.
- ✓ Diseñar programas de mantenimiento preventivo y correctivo de los equipos informáticos, salas audiovisuales y redes distribuidas en la Facultad.
- ✓ Crear y mantener actualizado el inventario de equipo informático, su estado físico y operativo, revisando en forma permanente los resguardos y las asignaciones de equipos a las diferentes áreas de la Facultad.

Este centro de cómputo cuenta en total con 487 computadoras a su administración, 7 servidores, todos con sus respectivos switches y no break.

La FCCA esta dividida en diversos departamentos, dentro de los cuales el centro de cómputo lleva el nombre de “Coordinación de servicios informáticos”, todos los departamentos se muestran a continuación en el organigrama:

ORGANIGRAMA
DE LA FCCA



<http://www.fcca.umich.mx/organigrama.php>

De acuerdo con la información obtenida de los equipos con los que cuenta este centro de cómputo, las funciones y objetivos que tiene y las observaciones realizadas dentro del mismo y dentro de los laboratorios donde se encuentra el resto de los equipos, se sugiere la siguiente evaluación de los riesgos con un total de 3 preguntas por riesgo:

RIESGOS	PREGUNTAS	¿CUENTA CON LO NECESARIO?	
Incendio	¿Existen extintores suficientes para cada área? ¿Los extintores están dentro de la fecha establecida de uso? ¿Existen los señalamientos necesarios en caso de ocurrir un incendio?	Sí Sí Sí	
Humo de incendio cercano	¿Las instalaciones se encuentran en áreas ventiladas? ¿Los equipos están cubiertos contra polvo? ¿Se cuenta con aire acondicionado en todas las áreas?	Sí No No	
Falta o falla eléctrica	¿Se cuenta con energía de emergencia? ¿Se cuenta con respaldos de información y laptops para trabajo alternativo?	No Sí	
Accesos no autorizados	¿Se tiene un buen control de las personas que entran al centro de cómputo? ¿Se cuenta con claves de acceso a los equipos informáticos? ¿Se cuenta con cámaras de circuito cerrado dentro y fuera de las instalaciones?	No Sí No	
Terremotos	¿Todos los equipos se encuentran fijos para así evitar caídas? ¿Se cuenta con un plan de contingencias específico?	Sí No	
Interferencia electromagnética	¿Los equipos del centro de cómputo se encuentran conectados adecuadamente? ¿Las conexiones dentro del centro de cómputo son hechas con material que disminuya la posibilidad	Sí Sí	

	de interferencia?		
Rayos (descarga eléctrica)	¿Se cuenta en los edificios con pararrayos? ¿Se cuenta con suficientes “no-break” para cada equipo? ¿Se cuenta con reguladores de energía?	No Sí Sí	
Falla en el cableado	¿Se tiene un tratamiento preventivo y/o correctivo en las instalaciones eléctricas?	Sí	
Robo de información	¿Son confiables las personas que laboran en el centro de cómputo?	Sí	
Mal manejo de la información	¿Son confiables las personas que laboran en el centro de cómputo? ¿Las personas que trabajan en el centro de cómputo están lo suficientemente capacitadas?	Sí Sí	

Dichas preguntas fueron previamente contestadas por la persona encargada del centro de cómputo de la FCCA. Habiendo obtenido las respuestas se dio paso a realizar la inspección física de las instalaciones para corroborar lo obtenido del cuestionario y poder llegar a notar probablemente algún otro detalle del mismo centro de cómputo.

Propuesta

Una vez realizada la inspección física del centro de cómputo se pudo corroborar que las respuestas obtenidas en el cuestionario mostrado anteriormente coinciden con las condiciones físicas en las que se encuentra dicho centro de cómputo, sin embargo hay ciertos puntos que son cruciales para el buen desempeño de un centro de cómputo (como se ha venido tratando a lo largo de este trabajo) y que éste no cumple sea parcial o totalmente. En base a esto se realiza la siguiente propuesta para la mejora del centro de cómputo:

Considerando los objetivos que se tienen plasmados en el centro de cómputo, los procesos que realiza para alcanzar dichos objetivos y la importancia que tiene este centro de cómputo dentro de la FCCA se toma como base para la creación de la propuesta el documento llamado: “Administración de centros de cómputo” realizado por el L.A.E. Arturo Pérez Arévalo, el cuál habla del cómo debe ser, tanto la estructura como el desarrollo en el trabajo, dentro de un centro de cómputo para su óptimo aprovechamiento (descrito en el capítulo 4), también se basa en el manual INEI de cableado estructurado 2009 [p. 7-12, 39-65] para la conectividad en el centro de cómputo.

Así pues como primer punto de la propuesta se maneja el hecho de que las personas que laboran en el centro de cómputo elaboren un manual específico en caso de contingencia, dado que no está por demás escatimar los posibles fenómenos que puedan llegar a perjudicar la información e infraestructura y más cuando se trata de información vital para el andar de una organización. Éste manual debe de cubrir aspectos tales como los factores internos y externos a los que se encuentra expuesta la organización, así como los riesgos físicos, humanos y de equipos técnicos.

De igual manera para la elaboración de dicho manual se deben de tener en cuenta los problemas más frecuentes que suceden dentro de un centro de cómputo, tomando en cuenta de igual manera problemas lógicos (software) y físicos (hardware), desde la manera de adquirirlos e implementarlos. Por ende se debe de tener contemplado el tipo y las especificaciones correctas tanto de hardware como de software que de acuerdo a las actividades llevadas a cabo en el centro de cómputo lograrán el mejor desempeño posible de sus tareas. Todo esto descrito de igual manera en el capítulo 4 de éste trabajo.

Otros puntos importantes a considerarse durante la elaboración del manual son los que en las preguntas del cuestionario obtuvieron respuesta negativa, a continuación se presentan:

- Los equipos informáticos no cuentan con protección alguna contra polvo, de manera que están expuestos a fallas ocasionadas por la acumulación del mismo, debe también, dentro de éste punto, tomarse en cuenta de que los equipos aún teniendo o no protección contra polvo deben de tener un mantenimiento de ésta índole pues aún estando cubiertos llegan a impregnarse.
- Dentro del centro de cómputo o laboratorios no se cuenta con aire acondicionado, el cuál es de suma importancia para mantener la temperatura ideal de los equipos informáticos, para poder evitar un sobrecalentamiento y llegar a su inutilidad.
- Aún contando con dispositivos y laptops para el respaldo de la información, no se cuenta con una fuente de energía alterna o de emergencia, pues en caso de alguna falla o una falta en el servicio de electricidad se pueda seguir trabajando en operaciones que sean vitales para el centro de cómputo y la organización en general.
- Dentro de los aspectos de seguridad tenemos en primer lugar el hecho de que no se tiene un control de la gente que ingresa al centro de cómputo, esto puede ocasionar desde riesgos físicos para los equipos (daños), robo de información o incluso un riesgo para los mismos trabajadores del centro de cómputo. Debe tenerse un control más estricto en el hecho de saber ¿quién? Y ¿para qué? Ingresa al centro de cómputo.
- Una muy buena manera de tener un control de las personas tanto que entran a la organización como al centro de cómputo es el hecho de contar con un sistema de cámaras de circuito cerrado, de tal manera que se tenga también un espacio y un encargado del control de éstas cámaras, ya que en caso de algún incidente se puede ver en ese momento o bien, se puede tener un archivo de los acontecimientos diarios grabados. Esto se sugiero no solamente alrededor del centro de cómputo, si no desde las entradas a la FCCA.

- En el caso de un espacio que se tiene destinado para el trabajo con aparatos electrónicos, como lo es, el centro de cómputo es muy importante estar precavidos contra las posibles descargas eléctricas que pueden ser originadas de distintas maneras, una de ellas y en muchos casos las más fuertes son las descargas ocasionadas por un rayo, en caso de lluvia, es una muy buena opción el contar con pararrayos en la parte más alta de la organización y en el edificio donde están ubicados los aparatos electrónicos, más si éste se encuentra cercano a fuentes de atracción como lo son los árboles.
- Otro punto vital para la seguridad en una organización, es el contar con personas encargadas del control en las entradas (guardias de seguridad), aparte de esto se debe de tomar en cuenta que tan seguras son los accesos a la organización, a cada edificio y a cada salón o laboratorio, ya que es muy pobre la seguridad en cuanto a chapas de cada puerta y reja. Esto ocasiona que con frecuencia se tengan robos dentro de la organización.

BIBLIOGRAFÍA

- (Tecnologías de la Información y de la Comunicación. Alfaomega Grupo Editor 2005 pág. 75)
- Administración de Centros de Cómputo/ Ricardo Hernández Jiménez /Trillas. 1997 pág. 340
- (Manual INEI de Cableado Estructurado 2009 [p. 7-12, 39-65]
- (Dembowski, Klaus 2000). Hardware : información sobre la totalidad del hardware, de rápido acceso. Barcelona: Marcombo. pp. 956)
- (JACOBSON, Ivar; BOOCH, Grady; RUMBAUGH, James (2000). El Proceso Unificado de Desarrollo de Software. Pearson Addison-Wesley.)
- (Sommerville, Ian (2005). Ingeniería del software (7ma. edición). Madrid: Pearson Educacion S.A.)
- (Maturana, J. (2009):¿Cómo interactúa el hardware con el software? Extraído de http://www.jorgematurana.cl/dv/P09/pct/PCT0906a_Como_interactuan_HW_y_SW.pdf)
- (Manuel Aranda Ogayar “Estrategias genéricas competitivas” <http://ciberconta.unizar.es/cv/manuelaranda.HTM>)
- [Web1] (Extraído de “Riesgos Informáticos” 2011 <http://www.basc-costarica.com/documentos/riesgosinformatica.pdf>)
- <http://elprofejorge.blogdiario.com/img/acc.pdf>
- <http://www.fcca.umich.mx/descargas/apuntes/Academia%20de%20Informatica/INTRODUCCION%20-%20ADM.%20CENTROS%20DE%20COMPUTO%20PEREZ%20AREVALO.pdf>