Tecnologías de la información en las instituciones de seguridad social

Diplomado semipresencial

CENTRO INTERAMERICANO DE ESTUDIOS DE SEGURIDAD SOCIAL
CISS
IMSS

material de estudio

Tecnologías de la información en las instituciones de seguridad social
Diplomado semipresencial

Material de estudio

Centro Interamericano de Estudios de Seguridad Social

Órgano de docencia, capacitación e investigación de la Conferencia Interamericana de Seguridad Social

Ciudad de México, mayo de 2000.

Editor: Centro Interamericano de Estudios de Seguridad Social
Calle San Ramón s/n esq. San Jerónimo,
San Jerónimo Lídice,
C.P. 10100 México, D. F. Tel. 5595-0011
Registro 3079

ISBN: 968-6748-19-9

Índice

	Página
¿En qué consiste y cómo debo usar mi material didáctico?	5
¿Cómo está conformado el Diplomado?	7
Módulo 1. Evolución de la informática, por Víctor Quintero González.	9
Tema 1. Sistemas de información.	11
Tema 2. Redes y Telecomunicaciones.	29
Tema 3. Las bases de datos y los manejadores de bases de datos.	53
Ejercicios y actividades de evaluación.	68
Módulo 2. Seguridad informática, por Miguel Angel Alvarado Sandoval.	69
Tema 1. Políticas, normas, procedimientos y programas de seguridad informática.	71
Tema 2. Seguridad física del *hardware* y del *software*.	95
Tema 3. Seguridad en las redes y telecomunicaciones.	111
Ejercicios y actividades de evaluación.	122
Módulo 3. Auditoría de informática, por Sara Isabel Ayala Rodiles.	123
Tema 1. Reingeniería en las organizaciones.	125
Tema 2. Auditoría a sistemas en desarrollo.	139
Tema 3. Auditoría a sistemas en operación.	155
Ejercicios y actividades de evaluación.	189

Página

Módulo 4. Impacto organizacional de la tecnología de la información, por Ricardo Loranca González. 191

Tema 1. Reingeniería en las organizaciones. 193

Tema 2. Rediseño de los procesos para su automatización. 215

Tema 3. El desarrollo organizacional en el cambio. 227

Ejercicios y actividades de evaluación. 235

Formato para envío de actividades de evaluación. 237

¿En qué consiste y cómo debo usar mi material didáctico?

El material didáctico está conformado por ***una guía didáctica y el material de estudio*** de cada uno de los módulos del Diplomado, a excepción del quinto módulo, que se desarrollará en la fase presencial.

Guía didáctica

La Guía Didáctica tiene el propósito de ofrecer a usted una orientación general sobre los procedimientos para realizar el Diplomado y recomendaciones para aprovecharlo mejor. En este sentido, ***es importante que lea toda la guía didáctica antes de pasar al material de estudio y que incluso la revise antes de iniciar un nuevo módulo***.

La Guía Didáctica contiene los apartados siguientes:

Planteamiento del Diplomado: En esta parte se señalan la justificación, propósito, objetivos y perfil de egreso, lo que le permitirá delimitar las finalidades del Diplomado y tener un punto de referencia para que usted evalúe si está cubriendo las expectativas de aprendizaje. También incluye un esquema en el que se indican el orden de los módulos, de forma que usted pueda llevar un seguimiento de éstos y distinguir la relación interna de cada una de las partes del Diplomado. Para ello también se señalan las palabras clave de cada módulo.

Metodología: Señala los medios de comunicación por los que usted puede mantener el contacto con este Centro y conocer las responsabilidades de su tutor. En el apartado *¿Qué se espera de mí como participante de un diplomado semipresencial?* se señalan algunas recomendaciones para un mejor aprovechamiento del curso.

Una lista de los ejercicios que debe resolver y enviar al CIESS, así como las características del proyecto final que debe exponer en la fase presencial para acreditar el Diplomado, se ofrecen en el título *¿Qué actividades debo realizar y cómo se evaluará mi desempeño?* ***Aquí se indican las fechas límite para entregar cada ejercicio***. En el material de estudio, al final de cada módulo, también se indican estas actividades. De igual manera se señala el procedimiento y las características de la acreditación que el CIESS otorgará por su aprobación a este Diplomado.

Equipo docente: En esta sección se hace una presentación de los coordinadores y tutores.

Glosario: Ofrece una lista de términos importantes para el estudio de los temas informáticos que se abordan en el Diplomado.

Material de Estudio

Este material está dividido de acuerdo con los cuatro módulos que conforman la fase a distancia. En él se señalan los temas seleccionados en función de los objetivos de aprendizaje ordenados de manera secuencial para que la asimilación se realice paulatina y progresivamente.

Para el logro de los objetivos de aprendizaje de cada módulo ***es importante que realice la lectura de los textos correspondientes antes de pasar a la resolución de los ejercicios*** y actividades señaladas para la evaluación. Al finalizar su actividad de evaluación, recuerde enviarla al CIESS oportunamente, de acuerdo con las fechas señaladas.

¿Cómo está conformado el Diplomado?

¿Cómo está conformado el Diplomado?

El programa del Diplomado semipresencial *Tecnologías de la información en las instituciones de seguridad social*, corresponde a un diplomado presencial de 240 horas. Integra en sus cuatro primeros módulos el análisis sobre la constante evolución de la tecnología de la información en las vertientes que a continuación se señalan: los sistemas de información, las redes de comunicaciones, las bases de datos, técnicas de seguridad informática, métodos de auditoría en informática y aspectos organizacionales influidos por el uso de la tecnología. El análisis de estos campos se orientan para la solución de los problemas informáticos y de tecnología en la seguridad social. En todos los casos se promueve la construcción de ejercicios analíticos y de aplicación, basados en la experiencia y área de desempeño del participante. Usted estudiará estos módulos bajo la modalidad a distancia.

El quinto módulo corresponde a la fase presencial y su estructura se integra por un conjunto dinámico de actividades académicas como la presentación de los trabajos desarrollados en la etapa a distancia, el intercambio de experiencias (éxitos y fracasos) en un entorno propiciado por talleres académicos, la participación de expertos en los temas abordados y las visitas guiadas.

MÓDULO I. EVOLUCIÓN DE LA INFORMÁTICA. En esta primera parte del diplomado estudiaremos el desarrollo de la informática en tres de sus principales campos: los sistemas de información, las redes de comunicación (especialmente se hace énfasis en redes locales) y las bases de datos. Se examinará la función de la informática y de las nuevas tecnologías de la información en el contexto de las instituciones de seguridad social.

MÓDULO II. SEGURIDAD INFORMÁTICA. La segunda parte se centra en los conceptos y categorías de la seguridad informática y su aplicación en la organización para garantizar la protección de la información contra riesgos y vulnerabilidades provocadas por los relajamientos del control. Se abordarán los campos de las políticas y normas de seguridad, los programas de protección, la seguridad física, la seguridad de *hardware* y del *software* y por último, los mecanismos de protección requeridos por las redes locales.

MÓDULO III. AUDITORÍA DE INFORMÁTICA. La tercera parte se compone de un análisis del campo de estudio integrado por dos especialidades: la auditoría y la informática. Los momentos "clave" de revisión, evaluación, las técnicas de auditoría y los mecanismos de control son aspectos fundamentales para que la función informática resulte satisfactoria a los usuarios. Se incluye el estudio acerca de qué y cómo revisar la adquisición de bienes informáticos y la contratación de servicios a un tercero (*outsourcing*).

MÓDULO IV. IMPACTO ORGANIZACIONAL DE LA TECNOLOGÍA DE LA INFORMACIÓN. Por último se analizará el origen de la reingeniería de los procesos organizacionales, la constitución de la llamada "cadena de valor" y el lugar que tiene la tecnología de la información en la cadena de valor. El factor humano en nuestros tiempos y sus posibilidades de crecimiento y autocontrol, es el tema de cierre de este módulo.

MÓDULO V. TECNOLOGÍAS DE LA INFORMACIÓN Y EVOLUCIÓN DE LA SEGURIDAD SOCIAL. El último módulo se realizará bajo la modalidad presencial en las instalaciones del CIESS (**no está incluido en el material de estudio**). La programación de las actividades estará orientada al intercambio y a la reflexión sobre los beneficios y la gestión que aproveche mejor la tecnología para el manejo de la información. El análisis conjunto de los alcances reales de su puesta en marcha en las instituciones prestadoras de servicios será también tema de este módulo, haciendo especial referencia al contexto de las instituciones de los participantes, así como el caso de España.

A través de la guía docente de especialistas y de las aportaciones grupales, se consolidará una perspectiva integral de los temas de administración, auditoría y seguridad aplicados a la tecnología de la información. La perspectiva de la fase presencial es construir las conclusiones que consoliden la producción académica del diplomado, de manera que se concrete un documento útil y actualizado para el estudio de la informática en las instituciones de seguridad social.

Módulo 1. Evolución de la informática

INTRODUCCIÓN

Sin duda, el movimiento mundial hacia la digitalización envuelve también a la esencia misma de las instituciones de seguridad social, pero a un ritmo diferente, más pausado, que en otros sectores económicos como la banca, el comercio, la industria y los servicios privados. Esta diferencia se asienta fundamentalmente en las fuertes inversiones que conlleva la adopción de tecnología de punta.

En el entorno competitivo y global de nuestra época, los sistemas de información entendidos como entidades formadas por elementos humanos, de *hardware* y de *software*, juegan un papel estratégico institucional; la historia nos muestra que hasta hace algunos años los sistemas de información estaban en manos de los técnicos y especialistas de cómputo, sin embargo, ahora que se han convertido en soluciones para la organización, todos los niveles de ésta deben estar involucrados en la planeación, desarrollo y evaluación de los sistemas de información.

El panorama evolutivo de la informatización en la seguridad social de América, también muestra desde hace quince años una constante adopción por parte de las instituciones de tecnologías para automatizar el procesamiento de datos, eliminar los enormes volúmenes de almacenamiento documental y brindar servicios más eficientes y de mejor calidad. Esto ha representado también una transformación de los procesos de operación y un impacto en la cultura organizacional.

Sin embargo, la aplicación de las nuevas tecnologías para mejorar la calidad en la prestación de los servicios, no es por sí misma un hecho que garantice el éxito de los planes. Entre otros factores, es imprescindible una adecuada gestión de los proyectos informáticos que comprenda cómo integrar los recursos de *hardware*, *software*, telecomunicaciones, metodologías, sistemas de información, usuarios, almacenamiento, y que incluya, de manera permanente, aspectos de seguridad, de control, auditoría y evaluación.

☞ OBJETIVO

- Estudiar los alcances y prospectivas de los sistemas de información, las redes de comunicaciones y las bases de datos, su utilidad y aplicaciones en el campo de la seguridad social.

PALABRAS CLAVE

Archivo
Arquitectura de la información
Base de datos
Dataware house
Imagen fisica
Red de valor agregado
Sistema de información
Imagen lógica
Medios de comunicación
Protocolo
Query
Red
Sistema experto
Topología

TEMAS

1. Sistemas de información
2. Redes y telecomunicaciones
3. Bases de datos

Autor de todos los temas: Víctor Daniel Quintero González.

Tema 1. Sistemas de información

Por Víctor Quintero González

Resumen

El desarrollo de la tecnología aplicada al manejo de la información, conocida también como tecnología de la información, es un fenómeno que envuelve sin excepción los ámbitos institucionales y personales y que obliga a realizar un permanente esfuerzo personal para estar al día de los avances, pero sobre todo, de cuáles son los mecanismos que permitirán aprovecharla de mejor manera.

El primer tema del módulo uno está destinado a realizar un estudio general sobre la importancia que revisten los sistemas de información para el cumplimiento de la misión y funciones de cualquier organización o empresa. Cómo definir un sistema de información, cómo clasificarlo y cuáles son las formas de gestionar adecuadamente su integración con el resto de los factores esenciales de un proyecto informático (los recursos humanos, los procesos, los productos y la tecnología), son aspectos que se analizan en esta parte del Diplomado.

La evolución y los retos que implica orientar esta tecnología a la misión de la seguridad social se abordan también en este tema rescatando referencias de algunos países con un alto nivel de desarrollo. Sin embargo, cualquier proyecto social que involucre el uso de la tecnología deberá considerar, primero y con especial énfasis, el contexto nacional con sus propias características sociales, económicas, políticas y culturales, así como el contexto institucional hacia el que se dirige.

Tema 1. Sistemas de información

Por Víctor Quintero González

Aspectos generales de los sistemas de información

Para partir de una base común que permita describir lo que son los sistemas, se revisarán algunos aspectos de la teoría general de sistemas cuyo enfoque permite estudiar y analizar los problemas considerando todos los elementos que pueden intervenir, visualizándolos como una formación completa e integral. Aunque existen muchas definiciones de lo que es un sistema, este vocablo se utiliza prácticamente en todas las ramas del saber y de las ciencias y se aplica en la agricultura, la industria, el comercio, en la vida civil, en la computación, la informática, etc.

Desde un punto de vista muy práctico, se puede definir un sistema como una colección de diferentes elementos que tienen algún tipo de relación entre sí, mediante la cual interactúan e intercambian productos e insumos y se coordinan para que, al funcionar, logren el objetivo común de todo el sistema.

Desde un punto de vista muy práctico, se puede definir un sistema como una colección de diferentes elementos que tienen algún tipo de relación entre sí, mediante la cual interactúan e intercambian productos e insumos y se coordinan para que, al funcionar, logren el objetivo común de todo el sistema.

En el plano de las organizaciones, cualquier sistema de información (SI) sobre el que se esté trabajando, sea manual, computarizado o mixto, interactuará con otros sistemas para formar parte de un sistema mayor, el cual a su vez será parte de un sistema institucional que con otros sistemas institucionales conformarán una organización social, misma que es también un sistema.

El modelo general de un sistema de información se compone de:

- Entradas o insumos (inputs) que son aceptados en el sistema.
- Salidas o productos (outputs) mismas que se producen a través de los procesos dentro del sistema.
- Almacenaje o memoria, en donde se archiva la información que el sistema necesita para su funcionamiento.
- Control, sobre el funcionamiento del sistema.
- Proceso, que efectúa transformaciones a las entradas.

La definición de sistema adoptada para este material y que es la base para los siguientes módulos, es que un SI es un conjunto de componentes relacionados entre sí que le permiten capturar los insumos, procesarlos, almacenarlos y distribuirlos, de tal manera que la salida o el producto de información permite soportar la toma de decisiones, coordinar gestiones y dar apoyo al análisis de problemas así como controlar las funciones operativas. El SI opera en un entorno que le suministra los datos de entrada e insumo y, a su vez, el SI modifica al entorno a través de la salida de información y la retroalimentación a la etapa de entrada, en un proceso interactivo y permanente.

El SI opera en un entorno que le suministra los datos de entrada e insumo y, a su vez, el SI modifica al entorno a través de la salida de información y la retroalimentación a la etapa de entrada.

En contraste con los SI informales como las conversaciones cotidianas, los SI formales tienen una estructura definida, aceptada y fija de los datos o insumos, de los procedimientos para captarlos, de los medios para almacenarlos, procesarlos, distribuirlos así como de la forma en que serán utilizados los productos de información arrojados.

Los SI pueden ser de tipo manual o bien estar basados en computadora. En este caso, los sistemas de información basados en computadora (SIBC) están soportados por la tecnología de la información (*hardware*, *software* y las comunicaciones) y es a través de ésta que almacenan, procesan y distribuyen los productos de información. Los SIBC anteriormente descritos no son equivalentes a las computadoras, a los programas o al *software*, ya que las computadoras y sus programas son los fundamentos técnicos o herramientas de este tipo de sistemas. La conformación general de un SIBC está definida por los siguientes elementos (Pressman, 1996):

- *Hardware*
- *Software*
- Procedimientos
- Documentación
- Bases de datos
- Personas (desarrolladores, usuarios finales)

En adelante y para fines de este material, el concepto de SIBC será equivalente al de SI.

Ciclo de vida de los sistemas de información

Frecuentemente se habla de la "crisis del *software*", la que se ha producido, en mayor medida, por los errores que en un alto porcentaje cometen los equipos de desarrollo del mismo. Dado que el *software* es un elemento lógico y no físico, su éxito se mide por la calidad y como entidad única, en vez de por muchas partes ensambladas o fabricadas. En el campo del desarrollo de los SI de la seguridad social, se encuentran también muchos conflictos ya sea porque se rebasa considerablemente el tiempo de entrega, porque el rendimiento no es lo que se esperaba, porque hay gran cantidad de defectos incluso cuando se emplearon los lenguajes y las técnicas más recientes del mercado, por la falta de una adecuada capacitación, o bien, porque el equipo responsable del desarrollo, interno o externo no supo interpretar adecuadamente las necesidades y expectativas de los usuarios solicitantes.

El gestor de sistemas o responsable del desarrollo de los sistemas debe comunicarse efectivamente con todos los componentes implicados en el desarrollo del *software* como clientes, realizadores del *software*, equipo de soporte, y otros. De lo contrario, cuando la comunicación se rompe o se comprenden mal las características especiales del *software*, se provoca que los problemas asociados con la "crisis del *software*" se acrecienten.

Existe poco entrenamiento formal en las nuevas técnicas de desarrollo de software.

Es común ver en los proyectos de desarrollo institucionales que cada individuo enfoca su tarea de "escribir programas" con la experiencia obtenida en trabajos o proyectos anteriores, es decir, existe poco entrenamiento formal en las nuevas técnicas de desarrollo de *software*, lo cual tampoco quiere decir que esto sea fácil, pues hay programadores que tienen muchos años utilizando un lenguaje estructurado de bajo nivel y es bastante complejo migrar su lógica de pensamiento y de programación a la lógica de los lenguajes orientados a objetos. Algunos programadores desarrollan un método ordenado y eficiente de desarrollo del *software* mediante prueba y error, pero muchos desarrollan malos hábitos que dan como resultado una pobre calidad y enormes problemas para el mantenimiento del *software*.

Sin embargo, el desafío que se vive desde la década de los noventa hasta nuestros días, - y que seguramente perdurará por un largo periodo - es mejorar la calidad del producto, aplicación o sistema y reducir el costo de tales soluciones.

En el contexto de la seguridad social, así como en cualquier otro campo, resulta fundamental reflexionar en cómo se desarrollan los SI considerando las estrategias empleadas para aprovechar las capacidades del *software* y del *hardware*, los planes y acciones que se realizan para el mantenimiento y la actualización de éstos y especialmente a partir de qué mecanismos se corrobora la utilidad y el logro de los objetivos planteados para los sistemas o aplicaciones implantados.

Diversos expertos en desarrollo de los sistemas y las experiencias recopiladas en las instituciones de seguridad socia, coinciden en señalar que uno de los problemas más importantes es el excesivo tiempo que se emplea, aunado a una mala planeación del trabajo.

Dado que todo "urge para ayer" y las listas de necesidades y peticiones de los usuarios aumenta día con día, es necesario trabajar con nuevas estrategias que, permitiendo acortar los tiempos de entrega del producto, no sacrifiquen la calidad del mismo.

Es necesario trabajar con nuevas estrategias que, permitiendo acortar los tiempos de entrega del producto, no sacrifiquen la calidad del mismo.

Las nuevas tecnologías y los nuevos productos informáticos no son en sí mismos la estrategia, como tampoco lo son las jornadas exhaustivas de programación, ni la omisión de las etapas clave para el desarrollo como planeación, recolección de requerimientos, análisis, diseño o documentación. Existen lineamientos y sugerencias clave para mejorar la gestión del desarrollo de sistemas, pero esto también requiere tiempo y esfuerzo pues no es fácil arrancar de un momento a otro los vicios y la inercia que se padecen desde hace años en este campo.

Cualquier punto de partida que tenga como objetivo mejorar la gestión del desarrollo de los SI, deberá considerar cinco líneas que guían esta actividad:

1. La referente al equipo de trabajo: el recurso humano con todas sus capacidades, experiencia y talentos creativos es el factor fundamental. Cómo motivarlo, cómo conformar equipos de trabajo eficientes, cómo seleccionar adecuadamente al personal para los diferentes tipos de proyectos, cómo distribuir las cargas de trabajo, resolver fricciones ante puntos de vista opuestos, cómo capacitar y actualizar a dicho personal, son premisas que los jefes y directivos de los departamentos informáticos o líderes de proyecto deberán tener presentes. Especial atención merece el proceso de comunicación con el usuario final del producto o el solicitante del desarrollo. El recurso humano, no obstante ser el más valioso, también es el más complejo e impredecible en su manejo. El ambiente laboral influye de manera significativa en la productividad informática por lo que el ruido excesivo, la iluminación inadecuada, la falta de privacidad, la interferencia con otras áreas son factores negativos para un buen desempeño del personal.

El ambiente laboral influye de manera significativa en la productividad informática.

2. La línea que se orienta hacia el proceso del desarrollo: un primer punto es la necesidad de una planeación realista del ciclo de vida elegido, trátese de desarrollos por cascada pura, codificar y corregir, espiral, cascadas modificadas, *prototipado* evolutivo, entrega por etapas, entrega evolutiva, diseño por herramientas y por supuesto, el desarrollo externo (*oursourcing*). El uso adecuado de las diferentes metodologías de gestión de proyectos, de las metodologías técnicas, de la gestión de riesgos y de los estándares de la ingeniería del *software*

son asuntos que deberán ser atendidos formalmente para alcanzar resultados satisfactorios en el desarrollo de sistema. El control de calidad del producto entregado, la corrección de errores justo en el momento en que se detectan, darle el peso específico a las necesidades de los usuarios y clientes o interpretarlas adecuadamente, también son asuntos de capital importancia en el proceso de desarrollo.

3. Una tercera línea de atención es la referente a la tecnología: es importante seleccionar adecuadamente las herramientas de desarrollo y tener claramente definidas sus prestaciones y sus limitantes (lenguajes de bajo nivel, estructurados o de cuarta generación, herramientas CASE, programación orientada a objetos, sistemas administradores de bases de datos, etc.); conocer las ventajas del *hardware* con que se estará trabajando (velocidad y capacidad de procesamiento, compatibilidad, estabilidad del producto por cuestiones de mantenimiento), asimismo, tener presente las necesidades de comunicación remota y su correspondiente infraestructura. Cabe mencionar en este renglón el estudio de los nuevos desarrollos tecnológicos como los poderosos sistemas de almacenamiento y análisis de la información conocidos como *data warehouse*.

4. El estudio del propio producto por desarrollar: primero en cuanto a sus dimensiones, por ejemplo, las prestaciones esenciales o secundarias del producto o las que deberán entregarse en una primera iteración de un prototipo. En segundo lugar se deben considerar sus características técnicas en cuanto al consumo de recursos de cómputo, desempeño y confiabilidad. En tercer lugar, los aspectos de propiedad intelectual y derechos de uso sobre el producto desarrollado para una institución.

5. La línea que corresponde al análisis de la propia información que será emitida por el sistema o aplicación: quién la va a usar, cuáles y cómo son las fuentes de entrada, cómo se podrá reutilizar esta información en otros departamentos, cómo se verifica su integridad, su vigencia y su utilidad. Para que este análisis de la información sea verdaderamente objetivo, tendrá que efectuarse con auxilio de otros paradigmas, como son la auditoría a la informática y la seguridad informática, temas abordados con detalle en los siguientes módulos.

Para que este análisis de la información sea verdaderamente objetivo, tendrá que efectuarse con auxilio de otros paradigmas.

Los sistemas de información en las instituciones

La indiscutible transformación del entorno mundial en los últimos diez años, tiene como uno de sus ejes el grado de desarrollo de la tecnología para las comunicaciones mundiales, y ésta es una razón por la que los SI ahora desempeñan un papel diferente dentro de las organizaciones; ahora, en el desarrollo de los SI se involucra una proporción mayor de las funciones centrales y metas de la institución. Asimismo, su impacto dentro de las organizaciones es

En el desarrollo de los SI se involucra una proporción mayor de las funciones centrales y metas de la institución.

mucho mayor ya que están aparejados de cambios administrativos e institucionales.

Un de los enfoques contemporáneos de los SI, tiene como punto de vista la propia actividad del negocio o la misión de la institución. En este sentido, un SI "...es una solución de organización y administración basada en la tecnología de información, a un reto que surge del medio ambiente..." (Laudon; 1996: 11). Dicho en otras palabras, los SI pueden definirse como soluciones institucionales, ligadas entre sí de manera interdependiente, administradas por un departamento, coordinación o dirección y soportadas con herramientas tecnológicas que les permitan enfrentar los cambios y retos del entorno.

Existen diversas clasificaciones o tipos de sistemas, a continuación se describe uno de esos modelos de clasificación dentro de las organizaciones:

Sistemas de información para el nivel estratégico: para directores o administradores superiores o de nivel estratégico. Aquí encontramos los sistemas de soporte gerencial (SSG) para la toma de decisiones, los cuales dirigen las decisiones no estructuradas y crean un ambiente generalizado de computación y comunicación Es decir, no trabajan sobre una aplicación o programa específico. El diseño de los SSG les permite incorporar información externa como nuevas leyes o disposiciones fiscales, pero también obtienen su insumo de los sistemas de información para la administración y de los correspondientes al soporte a la toma de decisiones. Una de las peculiaridades de los SSG es su empleo de programas altamente eficientes para la presentación de gráficas, pudiendo ofrecer de manera inmediata información de muchas fuentes. De ahí que, más que utilizar aplicaciones o programas específicos, estén basados en una gran capacidad de procesamiento y de telecomunicaciones. Se caracterizan por sus facilidades en tiempo y esfuerzo para rastrear y comprimir información crítica de utilidad para los ejecutivos.

Como ejemplos de los SSG tenemos pronósticos de ventas o recaudación a cinco años, planes de operación a cinco años, pronósticos de presupuesto también a largo plazo, planeación de las utilidades y planeación de la mano de obra.

Sistemas de información para el nivel de la administración: para gerentes o administradores medios. Aquí se encuentran los sistemas de información para la administración (SIA, en inglés MIS) y los sistemas para el soporte a la toma de decisiones (SSD). "...Los primeros proporcionan a los administradores informes y, en algunos casos, acceso en línea a los registros ordinarios e históricos de la institución (...) sirven principalmente a las funciones de planeación, control y toma de decisiones al nivel de administración gerencial..." (Laudon 1996: 43).

Los SIA concentran información obtenida de los sistemas de información para el nivel operativo y la presentan en forma de resumen rutinario y de informes de excepción empleando modelos muy sencillos. Su capacidad de análisis es poca y se orientan comúnmente a aspectos internos de la institución u organización y no del entorno; la periodicidad de su emisión es muy regular (por ejemplo semanal, quincenal, mensual o semestral, pero no diaria) y dan respuesta a preguntas estructuradas y de rutina. El manejo de los reportes es flexible ya que permite al usuario estructurar sus propios reportes y combinar datos de diferentes archivos. Ejemplos de SIA son: administración de ventas, presupuestación anual, análisis financiero y análisis de inversiones.

Los SIA concentran información obtenida de los sistemas de información para el nivel operativo y la presentan en forma de resumen rutinario y de informes de excepción

Los SSD, a diferencia de los SIA, tienen sofisticadas herramientas de análisis y modelaje de información que permiten, emplear diversos modos para modelar y visualizar la información. Estos sistemas dependen de la información suministrada por sistemas para el apoyo operativo y por los SIA y se sirven también de la información suministrada por fuentes externas, como precios de venta, de renta, porcentajes inflacionarios, tasas de inversión, costos de los insumos, etc. A diferencia de los SIA, los SSD son de acción instantánea, interactivos, orientados hacia modelos y hacia acciones, en tanto, los SIA son ponderados y orientados hacia lotes de información. Ejemplos de SSD son el soporte para la diagramación de la producción, de los costos o inversiones y análisis territoriales con bases de datos geográficas.

Sistemas de información para la generación de conocimientos: para trabajadores del conocimiento y la información. En este nivel se encuentran los sistemas de trabajo del conocimiento (STC) y los sistemas de automatización en la oficina (SAO). Son trabajadores del conocimiento los profesionistas que tienen grados universitarios, de maestría o superiores, son miembros de una profesión reconocida y su trabajo consiste en crear nueva información, nuevos productos y nuevos conocimientos. Los STC se apoyan en infraestructura de alto desempeño como estaciones de trabajo de ingeniería, de mecánica o científicas. A través de la investigación formal y el uso de los STC se promueve que la nueva producción científica sea integrada adecuadamente a las empresas o instituciones.

Por su parte, los trabajadores de la información por lo regular tienen niveles académicos menos formales y, más que generar o crear nueva información, tienden a procesar, presentar y distribuir la información; se trata principalmente de secretarias, auxiliares, archivistas y administradores no gerenciales. Los SAO son las herramientas tecnológicas comercialmente distribuidas que permiten incrementar la productividad de los trabajadores de la información en el esquema de una oficina clásica, por lo que en esta categoría se encuentran los procesadores de palabras, hojas electrónicas, correos electrónicos internos y los sistemas de almacenamiento y recuperación de imágenes digitales de documentos.

Los SAO son las herramientas tecnológicas comercialmente distribuidas que permiten incrementar la productividad de los trabajadores de la información en el esquema de una oficina clásica.

Sistemas de información para el nivel operativo:. Aquí se encuentran los sistemas de procesamiento de operaciones (SPO). Estos sistemas realizan y registran las transacciones diarias de rutina necesarias para la operación de la institución. Las tareas, recursos y metas del nivel operativo están bastante definidos y son muy estructurados. Los SPO son los principales generadores de información para los otros tipos de sistemas, "...Como los SPO hacen el seguimiento de las relaciones con el medio ambiente, son el único lugar donde los administradores obtienen evaluaciones inmediatas del funcionamiento de la institución e información muy anterior del funcionamiento de la misma..." (Laudon 1996: 41). Ejemplos de estos sistemas tenemos: levantamiento, control y seguimiento de pedidos, control de equipos, control de movimiento de materiales e inventarios, nóminas, cuentas por pagar, cuentas por cobrar, administración del efectivo, control de impuestos, seguimiento de la capacitación, registro de empleados, etc.

Arquitectura de la información dentro de las instituciones es un concepto de vital importancia en el enfoque contemporáneo de desarrollo de SI. Este término se refiere al cómo ordenar, coordinar e integrar a la tecnología de información (incluidos los SI) con las funciones centrales de la institución: es la forma particular que una institución adopta respecto a su tecnología y es a través de esta forma en que logra alcanzar sus metas o funciones específicas. Planear la arquitectura de la información implica definir en qué medida la información y la capacidad de procesamiento quedarán centralizados o distribuidos a lo largo y ancho de la organización, cómo deberán ubicarse los recursos de *hardware*, de *software* y de telecomunicaciones, de tal manera que las necesidades de información institucionales, sin perder de vista los diferentes niveles de información, queden satisfactoriamente cubiertas.

A nivel de las oficinas de trabajo de cualquier institución, el poder de la nueva arquitectura está centrado en las microcomputadoras,

Actualmente, la posibilidad de conectar diversas plataformas de *hardware* es total y, gracias a las redes troncales de alta capacidad, se pueden conectar entre sí muchas redes locales compuestas a su vez por estaciones de trabajo, computadoras personales, servidores, minicomputadoras, macrocomputadoras y dispositivos de telecomunicación. El sistema troncal, puede estar conectado a muchas redes externas y por supuesto a internet. La proliferación de las microcomputadoras, las estaciones de trabajo de escritorio, el gran poder de las telecomunicaciones y la tendencia a la baja de los precios del *hardware* son factores de gran importancia que han promovido la nueva arquitectura de la información. A nivel de las oficinas de trabajo de cualquier institución, el poder de la nueva arquitectura está centrado en las microcomputadoras, ya que pueden actuar como servidores de archivos en redes, asumiendo una función que anteriormente era exclusiva de las macro y las minicomputadoras.

Otro concepto que se está tornando cada vez más común en el desarrollo de sistemas, es el de sistemas *data warehouse*. Éste se puede definir como un

mecanismo para entregar información de negocios integrada a la organización. Más que un producto, es un proceso definido en la organización para que la toma de decisiones esté basada en una única fuente de información detallada conforme se va generando en la operación. Técnicamente, un *data warehouse* es una colección integrada de información corporativa diseñada para la recuperación y el análisis en apoyo a los procesos de toma de decisiones.

Un sistema de data *ware house* incluye cuatro componentes:

- Un almacén o data *warehousing* donde está almacenada físicamente la información. Esto incluye dispositivos de almacenamiento, un servidor y un sistema de administración de bases de datos.
- Un módulo de adquisición de fuentes de datos, que es un software que copia los datos de sus fuentes originales, los limpia y los transfiere hacia otro *warehouse* (almacén).
- Un módulo de entrega al usuario final donde se pueden hacer preguntas y obtener respuestas. Incluye generadores de reportes, OLAP *(on line analytical processing;* procesamiento analítico en línea) y otras herramientas de solicitud de información.
- Un depósito *metadata*, que es una guía que permite al usuario encontrar más cosas en el data *warehouse.*

La extracción de los datos puede hacerse en muchas formas, desde simples reportes hasta una minería de datos avanzada. El usuario puede escribir sus aplicaciones o consultas personalizadas, crear reportes, gráficas, realizar análisis multidimensionales y navegar en el *data warehouse*.

Para el sector de la salud y de la seguridad social, el *data warehouse* tiene diversas aplicaciones. Por ejemplo, en el caso del abasto de medicamentos y bienes terapéuticos, la Dirección de Abastecimiento necesita conocer la existencia de tales productos en cada uno de los almacenes que están distribuidos en todo el país qué tipo de distribuidores tiene, cuáles son sus tiempos de entrega y si ha cumplido o no con su programa de entregas. Las áreas financieras en sus renglones de recaudación de cuotas obrero patronales, pago de subsidios, pago de pensiones y de prestaciones en general, son otro campo fértil para la

incorporación del *data warehouse,* con el cual se podría consolidar información crítica resultante de las auditorías, así como historiales especializados para evitar fraudes.

Ahora bien, para implantar un data warehouse es necesario tener preparados los sistemas básicos de operación y administración (contabilidad, inventarios, transacciones bancarias, cuentas conciliadas, etc.) porque éste se alimentará de ellos. El costo de desarrollarlo puede resultar en varios miles de dólares, aunque se prevé un alto crecimiento en su uso.

Para implantar un data warehouse es necesario tener preparados los sistemas básicos de operación y administración.

En los temas siguientes de este primer módulo, se estudiará con más detenimiento el aspecto técnico de esta nueva arquitectura de la información, por ahora se continúa con el estudio de cómo se ha incorporado la tecnología de la información a las prestaciones y servicios que brinda la seguridad social.

La incorporación de los medios electrónicos en la prestación de servicios

La seguridad social está experimentando, gracias a la tecnología de la información, un cambio en la manera como presta sus servicios y no sólo en sus aspectos internos como instituciones u organizaciones que modernizan su gestión. Las tecnologías (dispositivos, aplicaciones, sistemas, conectividad) producto de los avances científicos, se emplean para mejorar la calidad del servicio en rubros como la rapidez, la comodidad, la precisión, el acceso directo por el propio cliente, la rentabilidad y la adaptación al crecimiento de las solicitudes. Esta nueva tendencia en la prestación de servicios a través de los medios electrónicos se denomina "entrega de servicios electrónicos (ESE)". La ESE consiste básicamente en el uso de quioscos de multimedia, tarjetas inteligentes, uso de internet, intranet y extranet, reconocimiento vocal interactivo, telefonía inteligente y centros de llamadas, para atender las necesidades de los derechohabientes y beneficiarios de la seguridad social.

La ESE en la seguridad social y en muchos otros giros, se basa en las cinco líneas que soportan el desarrollo informático: las personas, los procesos, la tecnología, los productos y la información. Sin embargo,como ya se planteó anteriormente, es la infraestructura tecnológica de la información la que debe responder a las necesidades generadas por la actividad de una organización; ésta debe determinar el alcance y la forma de explotación de dicha tecnología.

Es la infraestructura tecnológica de la información la que debe responder a las necesidades generadas por la actividad de una organización.

Además de la modificación a la forma de prestar los servicios, la evolución de la tecnología también ha cambiado la fisonomía administrativa de las instituciones: se han generado nuevos puestos de trabajo, se impone la educación permanente de los funcionarios, han cambiado los procesos organizacionales y por supuesto, está surgiendo una nueva cultura informática.

Latinoamérica destaca por ser uno de los mercados más grandes del mundo que compra bienes y servicios de tecnología, incluso, diversas prestaciones o servicios del seguro social en la región se han impregnado de la filosofía de ESE. Como ejemplos, se pueden citar el pago de salarios de los empleados a través del depósito en una cuenta (lo que supone una conectividad electrónica con la banca); las declaraciones patronales vía diskette; la integración de la información entre diversas dependencias gubernamentales o instituciones afines y por supuesto, la información general en un sitio en internet.

Sin embargo, predomina la preocupación ante el desconocimiento de cómo usar adecuadamente la tecnología en el caso de obreros, campesinos, empleadas domésticas y la población económicamente activa que aún no conoce cómo usar una computadora o no tiene forma de acercarse a éstas. Es conocido el temor que los adultos experimentan para acercarse a las computadoras haciendo especial señalamiento en los adultos mayores, campesinos y población rural o urbana marginada, a quienes los beneficios de la tecnología informática (entre otros) no han llegado.

Otro inconveniente lo representan las dificultades de muchas instituciones para hacer inversiones importantes en el rubro de la tecnología y modernizar sus procesos y servicios, problema que se ha acrecentado por la falta de continuidad en los programas institucionales y por la falta de una cultura informática en los niveles que toman las decisiones. De igual modo, otro problema es la carencia de equipos de trabajo institucionales que orienten y gestionen efectivamente la incorporación de nuevas tecnologías en la organización, aun cuando se estén utilizando los servicios de consultoría y desarrollo de terceros, ya que nadie mejor que los propios funcionarios conocen las necesidades, problemas, expectativas y cultura organizacional, factores fundamentales para que la tecnología sea la que se adecue a la institución y no viceversa. También es necesario mencionar los obstáculos que significan la falta de continuidad en los programas de capacitación institucionales y la carencia de una estrategia educativa integral, dentro de una lista que podría crecer.

A riesgo de caer en un fatalismo, también habrá que reconocer los frutos alcanzados, ya que muchas instituciones están logrando avanzar en la incorporación y uso de la tecnología para evitar que los derechohabientes inviertan muchas horas al solicitar un servicio y para ahorrarles muchos trámites al solicitar información.

Algunas experiencias de países con un alto grado de desarrollo tecnológico, acerca de cómo han empleado la tecnología para brindar servicios más rápidos y la evolución de estos servicios, nos pueden ilustrar cómo la incorporación a la seguridad social de los avances tecnológicos es gradual y planeada.

La incorporación a la seguridad social de los avances tecnológicos es gradual y planeada.

En el caso de Canadá, específicamente del Ministerio de Desarrollo de Recursos Humanos (HRDC), un órgano del gobierno federal encargado de entregar servicios sociales como seguro de empleo, pensiones, créditos para estudiantes, etc., cuenta con aproximadamente 25,000 empleados ubicados en diez provincias; el universo de usuarios de estos servicios alcanza la cifra de 30 millones de ciudadanos (Rainville, 1999). La entrega de servicios se hace por los conductos tradicionales como son las oficinas, el correo y el teléfono, pero también ofrecen información y posibilidad de muchas gestiones a través de los quioscos multimedia y a través de internet.

La infraestructura tecnológica del HRDC actualmente comprende varias plataformas informáticas, computadoras personales, redes de área local, redes de área ancha, centros de llamada, sitios en internet e intranet, aplicaciones, bases de datos y quioscos multimedia. El alto grado de integración de su parque informático se ha conformado gracias a las continuas inversiones económicas y a una evolución estratégicamente planeada que dio inicio en los años sesenta.

Como respuesta a las crecientes solicitudes de los usuarios a lo largo de los años, se ha aumentado la complejidad de los programas de atención, se han introducido nuevas funciones informáticas, nuevos programas de aplicaciones y nuevos conductos para entregar los servicios. Dado que las aplicaciones constituyen el núcleo de la entrega de los servicios, se ha puesto especial énfasis en definir las reglas y procesos acordes al flujo de trabajo así como establecer los requisitos de la información. Actualmente las aplicaciones se diseñan en tres capas: la de presentación, que es el navegador instalado en la computadora personal; en segundo término, la capa de funcionalidad que contiene la lógica y las reglas de manipulación de datos y finalmente la capa de datos.

Dado que las aplicaciones constituyen el núcleo de la entrega de los servicios, se ha puesto especial énfasis en definir las reglas y procesos acordes al flujo de trabajo.

La difusión y el crecimiento de internet han generado una gran oportunidad de reparto de servicios gracias a la entrega de servicios electrónicos en "autoservicio" para los clientes: los servicios que quieren cuando quieren. Los dispositivos finales también han cambiado, pues en la actualidad son un teléfono o computadora personal configurada como quiosco y disponible para el público, o como unidad conectada a internet, ya sea a domicilio o en un lugar público. La atención a las necesidades de información de los usuarios también se efectúa gracias a los sistemas de respuesta vocal interactiva, a las centrales privadas de conmutación (PBX), a los sistemas de distribución automática de las llamadas y a la tecnología de datos como servidores y macrocomputadoras.

El desafío para ésta y otras muchas organizaciones consiste en mejorar la gestión de sus datos e información. Para ello, es esencial la racionalización de los procesos y la normalización de elementos tales como fabricantes, sistemas operativos y *software* de navegación. Puesto que en el curso de su vida los clientes accederán a diversos programas o servicios, es necesario garantizar la

unificación de los datos relativos a cada cliente en los diferentes programas, evitar al máximo la redundancia de datos, los diferentes procesos para la actualización, acceso y supresión de la información y otras incompatibilidades.

Es necesario garantizar la unificación de los datos relativos a cada cliente en los diferentes programas, evitar al máximo la redundancia de datos, los diferentes procesos para la actualización, acceso y supresión de la información y otras incompatibilidades.

El campo de la seguridad es un elemento crucial para la entrega de servicios electrónicos. Es compleja, costosa y debe evaluarse constantemente. Existen varios niveles de seguridad disponible, que van desde una simple contraseña a una seguridad elevada con cifrado de datos y firmas electrónicas, pero el asunto de la seguridad no sólo es de orden técnico, los directivos de cada programa de servicios también están involucrados en los aspectos de seguridad.

En Estados Unidos, la Administración de la Seguridad Social (Social Security Administration (SSA), brinda sus servicios anualmente a más de 150 millones de trabajadores, a 48 millones de beneficiarios, a seis millones de empleadores y a miles de organizaciones estatales, locales y privadas. No obstante que se trata de un considerable volumen de transacciones, la SSA estima un crecimiento mucho mayor en los próximos diez años, debido a que entonces llegarán a la jubilación los nacidos durante el *baby-boom* de los cincuenta (Adams, 1999). De acuerdo con este panorama, la SSA tendrá que encontrar mecanismos más eficientes para procesar y gestionar los altos volúmenes de información y proporcionar la cantidad de servicios que la población le demande.

Una forma de abordar este problema es aumentar el nivel de autoservicio automatizado a disposición del público. Una gran cantidad de usuarios están conscientes que al tener conexión electrónica a través de internet podrán acceder a los servicios de manera más cómoda, rápida y durante las 24 horas del día. Es previsible que el uso de internet continúe experimentando un rápido crecimiento y que la gente se acostumbre cada vez más a utilizarla para buscar información y llevar a cabo sus transacciones, por lo que, a través del trabajo conjunto entre diversas agencias gubernamentales, se estudian los mecanismos para garantizar adecuadamente la seguridad y la intimidad de la información que viaja en la red.

La información contenida en el sitio web de la SSA no contiene datos sensibles por lo que no es necesario adoptar medidas de alta seguridad, más bien se refiere a la información amplia y variada acerca de los programas y servicios que proporciona la seguridad social. A través del sitio web los visitantes pueden obtener publicaciones, formularios, informes de los programas y direcciones de las oficinas locales; también pueden bajar aplicaciones informáticas para calcular pagos de subsidios o solicitar empleo. El sitio se actualiza regularmente y las visitas crecen día con día de tal manera que la internet se está convirtiendo en un medio cada vez más común para acceder a la información sobre la seguridad social.

Uno de los retos de la SSA y de todas las instituciones que prestan servicios

vía electrónica es proporcionar un acceso cómodo y público a los servicios a través de internet y, al mismo tiempo, encontrar los criterios adecuados para garantizar la seguridad y la confidencialidad de la información personal almacenada en los registros.

La protección de la información para evitar accesos no autorizados y durante la transferencia a través de internet se consigue habitualmente mediante el cifrado o codificación; la SSA emplea una clave de cifrado de 40 bits que es la normal en la mayoría de los programas de navegación de internet. Aumentar a un nivel mayor de seguridad es lo deseable pero eliminaría a una parte muy grande de la base de clientes que no han actualizado sus versiones de programas de navegación. La amenaza latente de los hackers obliga a cualquier institución o empresa de comercio electrónico que tenga su red corporativa privada vinculada a internet, a establecer las medidas necesarias que eviten el acceso injustificado a ella, tal es el caso de los firewalls.

La amenaza latente de los hackers obliga a cualquier institución a establecer las medidas necesarias que eviten el acceso injustificado a ella, tal es el caso de los firewalls.

Aspectos de confidencialidad de la información y autentificación de usuarios que realizan transacciones electrónicas son vigilados con mecanismos como las firmas electrónicas, la autentificación basada en el conocimiento, los números de identificación personal y se estudia la incorporación de infraestructura de clave pública. El mecanismo de seguridad empleado depende del tipo de información por proteger.

Estas breves referencias nos ayudan a comprender la magnitud del impacto tecnológico. En los países con dependencia industrial y tecnológica de terceros el reto será aumentar la calidad de los servicios que aún se prestan sin contar con la infraestructura de vanguardia. También es conveniente considerar que ningún proyecto tecnológico tendrá éxito si se pretende hacer de golpe o de manera descontextualizada, es decir, extrapolar o imponer soluciones tecnológicas exitosas en otras latitudes no tendrá un buen resultado si no se realiza antes una seria planeación y una gestión adecuada del proyecto.

Bibliografía

Adams Cathy, (1999), *El reto de equilibrar la atención al cliente y el derecho a la intimidad en la Administración de la Seguridad Social de los Estados Unidos en la era electrónica,* artículo presentado en la 9a. Conferencia Internacional sobre Tecnologías de la Información en la Seguridad Social, de la Asociación Internacional de la Seguridad Social, Montreal.

Avison, D.E. & Fitzgerald G. (1994), *Information systems development: methodologies, techniques and tools.* London.

Laudon, C., Kenneth & Laudon, P., Jane (1996). *Administración de los sistemas de información. Organización y tecnología*; México, Prentice Hall Hispanoamericana.

Mc. Connell, Steve (1997), *Desarrollo y gestión de proyectos informáticos,* Madrid, McGraw-Hill Interamericana.

Pressman, S., Roger, (1993), *Ingeniería del software. Un enfoque práctico.* México, McGraw-Hill Interamericana.

Rainville Serge (1999), *Consideraciones sobre la infraestructura,* artículo presentado , artículo presentado en la 9a. Conferencia Internacional sobre Tecnologías de la Información en la Seguridad Social, de la Asociación Internacional de la Seguridad Social, Montreal.

Senn, A., James (1992*), Análisis y diseño de sistemas de información.* México: McGraw-Hill Interamericana.

Tema 2. Redes y telecomunicaciones

Por Víctor Quintero González

Resumen

Debido a la continua evolución de plataformas y tecnologías en nuestros días, la transferencia de información constituye una de las principales herramientas para la administración, control y distribución de los procesos tanto en las empresas públicas como privadas, ya que hace más eficiente la toma de decisiones en todos los niveles organizacionales. Por lo tanto, las redes computacionales como herramientas de actualidad conforman el entorno principal para que dichas propuestas se lleven a cabo satisfactoriamente, fortaleciendo los avances tecnológicos tanto en el proceso y distribución de la información, ciencia, investigación, así como en todos los niveles de nuestro ámbito social. En este documento analizaremos y revisaremos algunos de los conceptos más relevantes del concepto de red y sus tipos de transmisiones.

Tema 2. Redes y telecomunicaciones

Por Víctor Quintero González

Red

¿Qué es una red? Es un conjunto de computadoras y equipos conectados entre sí de tal forma que permitan transmitir, recibir, compartir y procesar información. Su objetivo principal es compartir los recursos tanto de *software* como de *hardware*, optimando tiempos de proceso y manejo de información.

Los principales elementos de una red son:

- Servidores
- Estaciones de trabajo
- Sistemas operativos de red
- Medio de comunicación
- Conectividad
- Protocolos
- Tarjetas de red
- *Software* de aplicación

Servidores

Computadora de gran capacidad capaz de compartir recursos específicos los cuales se definen previamente soportando las peticiones de las estaciones de trabajo utilizando la filosofía cliente-servidor, en donde el servidor sea capaz de dar el servicio solicitado. Existen dedicados, los cuales solamente administran los recursos de la red, y los no dedicados, que realizan la misma función además de servir como estación de trabajo.

Estaciones de trabajo

Se define como cada una de las computadoras conectadas en la red, con la capacidad de realizar sus propios procesos, solicitando y compartiendo sus recursos.

Sistemas operativos de red

Es el conjunto de programa y rutinas que interactúan entre el usuario y la computadora, las cuales apoyan las tareas del servidor, así como la administración y compartimiento de los recursos de la red. Después de cumplir todos los requerimientos de *hardware* para instalar una red, se necesita instalar un sistema operativo de red (network operating system, NOS), que administre y coordine todas las operaciones de dicha red. Los sistemas operativos de red tienen una gran variedad de formas y tamaños, debido a que cada organización que los emplea tiene diferentes necesidades. Algunos se comportan excelentemente en redes pequeñas, y otros se especializan en conectar muchas redes pequeñas en áreas bastante amplias.

Los servicios que el **NOS**[1] realiza son:

- Soporte para archivos: esto es, crear, almacenar y recuperar archivos, actividades esenciales en que el NOS se especializa proporcionando un método rápido y seguro.

- Comunicaciones: se refiere a todo lo que se envía a través del cable. La comunicación se realiza cuando, por ejemplo, alguien entra a la red, copia un archivo, envía correo electrónico o imprime.

- Servicios para el soporte de equipo: aquí se incluyen todos los servicios especiales como impresiones, respaldos en cinta, detección de virus en la red, etc.

- Compartir recursos:

  - Almacenamiento.
  - Programas.
  - Datos del sistema administrador.
  - Información procesada.
  - Sistemas de bloqueo.
  - Dispositivos periféricos(impresoras, unidades de almacenamiento, etc.)

- Seguridad: debe administrar el uso de los recursos de la red y otorgar niveles de acceso a los usuarios definiendo jerarquías para tal efecto.

---

[1] Network operating system (sistema operativo de red).

- Facilidades de comunicación: debe permitir establecer puentes entre redes (interconexión de redes locales, por ejemplo), a equipos *mainframes*, comunicaciones remotas, etc.

- Ayudas en línea.

Tipos de sistemas operativos

Servidores de discos.
Servidores de archivos.
Arquitectura cliente–servidor.
Arquitectura cliente–cliente (punto a punto)
Servidor de base de datos

Principales sistemas operativos de red

NOMBRE	MARCA
Lantastic	Artisoft
Lan Manager	SCO
Netware	Novell
Lan Manager	Microsoft
Windows for Work group v.3.11 *	Microsoft
Windows 95-2000*	Microsoft
Windows NT	Microsoft

* Se consideran sistemas operativos de red porque tiene las características de interconectividad entre las estaciones de trabajo, pero carecen de algunas otras como el manejo íntegro de la seguridad y tener propiamente un servidor.

Medio de comunicación

Son las interconexiones físicas entre los componentes de toda la red. Los principales medios de comunicación son:

Par trenzado (twisted pair) Cable tipo telefónico generalmente de cobre por el cual fluye la información. Dentro de este tipo de cable es posible encontrar variantes tales como cable sin blindaje (unshielded twisted pair UTP) y cable con blindaje (shielded twisted pair): éste consiste en una

capa de metal que protege al cable interior que es una malla tejida de hilos de metal. Este medio es el que presenta más bajo costo pero su desventaja es que es más vulnerable al ruido, por lo que no se recomienda adecuado para altas velocidades o largas distancias.

Las instituciones encargadas de realizar las recomendaciones indican que para el cable UTP se deberá contemplar una distancia de 100 a 150 m. como máximo y para el cable STP 300m. como máximo. Comercialmente existen cinco niveles o categorías de cable UTP. (Ver figura I).

REFERENCIA (Forma de Encontrarlo)	**APLICACIONES (Forma de Uso)**
▪ EIA/TIA Categoría 1	▪ Correo ▪ Voz Analógica ▪ Voz Digital
▪ EIA/TIA Categoría 2	▪ ISDN (Datos) 1.44 Mbps ▪ TI: 1.544 Mbps ▪ Voz Digital ▪ IBM 3270 ▪ IBM SYSTEM/3X ▪ AS/400
▪ EIA/TIA Categoría 3 ▪ NEMA 100-24-LL ▪ UL Nivel III	▪ 10 BASE T ▪ 4 Mbps Token Ring ▪ IBM 3270, 3X, AS/400 ▪ ISDN ▪ VOZ
▪ EIA/TIA Categoría 4	▪ 10 BASE T ▪ 16 Mbps Token Ring
▪ EIA/TA Categoría 5 ▪ NEMA 100-24-XF ▪ UL Nivel 5	▪ 10 BASE T ▪ 16 Mbps Token Ring ▪ 100 Mbps DDI

Figura I Niveles o categorías de cable UTP

Es importante resaltar que en la mayoría de las instalaciones de redes LAN[2] el medio de comunicación que se elige es el UTP. Por su costo, pero sobre todo por su facilidad para conformar instalaciones bajo la filosofía del cableado estructurado. Se puede observar en la tabla que existen diversos niveles de UTP pero aún hay quien utilizan estas categorías indistintamente sin conocer a detalle

En la mayoría de las instalaciones de redes LAN el medio de comunicación que se elige es el UTP.

[2] Local area network (redes de área local).Están separadas por distancias de hasta unos pocos kilómetros, y suelen usarse en oficinas o campus universitarios

de ellas, por lo que se recomienda conocer sus especificaciones para indicar la categoría adecuada por instalar.

Cable coaxial. Este medio consiste en un conductor central de cobre, rodeado por otro conductor, generalmente una malla de hilos de metal, separados entre sí por un medio aislante, este apantallamiento evita interferencias. El cable coaxial puede llegar a manejar un ancho de banda mayor al par trensado. Además de clasificarse por su tamaño físico, también se clasifica por su impedancia.[3] Existen varios tipos de cable coaxial usados en redes:

Cable Ethernet, que cumple con las especificaciones de este tipo de red de los cuales existen dos tipos:

- Thin Ethernet.- RG-58U, distancia máxima por segmento 300m. impedancia de 58.5 ohms[4].
- Thick Ethernet.- RG-11, distancia máxima por segmento 600m. impedancia de 58.5 ohms.

- Cable Arcnet, RG-62, distancia máxima de 600m impedancia de 73 ohms.

Fibra óptica. Los cables anteriores deben colocarse en lugares libres de problemas ambientales evidente; con el cable de fibra óptica no se tiene esa desventaja. Este medio presenta excelentes características tanto eléctricas como mecánicas pero aún su costo es elevado.

Las fibras ópticas son hilos delgados de vidrio con un alto nivel de pureza, que se procesan desde silicatos a grandes temperaturas para lograr un hilo fino y uniforme.

Las fibras ópticas son hilos delgados de vidrio con un alto nivel de pureza, que se procesan desde silicatos a grandes temperaturas para lograr un hilo fino y uniforme. Este medio proporciona la ventaja de poder conducir información en forma de luz a velocidades más altas que en el cobre y aun el oro.

Otra gran ventaja de este medio es que tiene un amplio ancho de banda[5], lo que nos permite transmitir información de diversa naturaleza, como voz, datos e imágenes con la misma facilidad.

---

[3] Resistencia aparente de un circuito dotado de capacidad y autoinducción al flujo de una corriente eléctrica alterna, equivalente a la resistencia efectiva cuando la corriente es continua.

[4] Unidad en el Sistema Internacional de Resistencia Eléctrica que se produce entre dos puntos de un conductor cuando una diferencia de potencial constante de un voltio, aplicada entre ellos, produce una corriente de un amperio.

[5] En comunicaciones, un indicador de la cantidad de datos que pueden transmitirse en determinado periodo de tiempo por un canal de transmisión.

Señales radioeléctricas. Este medio se basa en la transmisión vía ondas de radio u otro medios inalámbricos, haciendo uso de diversos equipos necesarios para la adecuada transmisión de la información. En este tipo de transmisión hace uso del aire como medio de transmisión aprovechando el fenómeno electromagnético de las antenas, tanto receptoras como transmisoras. Ejemplo de lo anterior serían las comunicaciones vía microondas, vía rayo láser, hasta llegar a la transmisión vía satélite.

Para la elección del medio de comunicación adecuado se debe considerar principalmente los siguientes aspectos:

- Cubrir el ancho de banda necesario.
- Cubrir las velocidades requeridas.
- Cubrir las distancias requeridas.
- Adaptación al entorno físico y geográfico.
- Minimizar posibilidades de fallas.
- Posibilidad de crecimiento y modularidad.
- Minimizar costos de instalación y de mantenimiento.

Conectividad

La manera de interconectar los distintos elementos de una red da un primer acercamiento a la estructura y comportamiento de la misma. Por lo general, para redes pequeñas, la longitud del cable no es limitante para su desempeño; pero si la red crece, tal vez llegue a necesitarse una mayor extensión de la longitud de cable o exceder la cantidad de nodos especificada. Existen varios dispositivos que extienden la longitud de la red, donde cada uno tiene un propósito especifico. Sin embargo, muchos dispositivos incorporan las características de otro tipo de dispositivos para aumentar la flexibilidad y el valor. Existen dispositivos de este tipo como:

- **Hubs o Concentradores**. Son un punto central de conexión para nodos de red en donde su principal función es la simplificación y centralización del cableado además de hacer más sencillos los cambios, movimientos y adiciones a la misma. Con la centralización de los cables se ahorra mucho tiempo en el seguimiento de éstos, ya que el concentrador se encuentra en un gabinete y ahí mismo es donde salen todos los cables por distribuir, lo que hace más segura a la red.

Con la centralización de los cables se ahorra mucho tiempo en el seguimiento de éstos.

- **Repetidores.** Es un dispositivo que permite extender la longitud de la red; amplifica y retransmite la señal dependiendo el tipo y sus características.

- **Puentes.** Es un dispositivo que tiene la función de comunicar dos redes empleando la misma tecnología o una similar, las cuales se encuentran separadas

por lo que aparentara ser una sola red. La principal ventaja de utilizar puentes para la interconexión de redes es que se logran canales de alta velocidad y su principal desventaja es que no se divide el tráfico entre las redes por conectar, sino que se incrementa.

- **Ruteadores.** Los ruteadores o *routers* son un dispositivo de nivel más alto que los puentes. Un ruteador no solo entiende qué es lo que se va a trasmitir, sino que además, sabe lo suficiente del destino del mismo. Esta información le sirve al ruteador para tomar decisiones sobre cómo y hacia dónde reorientar la información que recibe.

A la configuración geométrica resultante se le llama topología de la red. Para el estudio de la topología se deben considerar dos tipos:

- Física
- Lógica

La topología física se determina por la disposición de los elementos a la red.

La topología lógica la determina el protocolo[6] de comunicación operando en la red, sin importar la disposición física de los elementos.

Existen diferentes tipos de topologías físicas. Para poder analizarlas primero se debe considerar su topología lógica, y posteriormente entender cómo se estructura o conforma su topología física con base en los elementos de conectividad.

Los factores de análisis que se deben de considerar para la elección de la topología son:

- Protocolo de comunicación física.
- La flexibilidad de la red para añadir o eliminar nuevas estaciones de trabajo.
- La repercusión en el comportamiento de la red, considerando que se pueda tener una falla en una de las estaciones de trabajos o nodos.
- El flujo de información que pueda transitar sobre la red sin que existan problemas asociados a retardos en la comunicación debido a una carga excesiva de transporte de información.
- Versatilidad en el diseño del cableado.
- Posibilidades de crecimiento.

---

[6] Conjunto de reglas que gobiernan las acciones de comunicación.

De acuerdo con lo anterior los más comunes tipos de topologías son:

- Estrella.
- Bus.
- Anillo.
- Múltiple (combinada o compuesta).

Topología tipo estrella. Antes que nada cabe mencionar que la topología lógica que ocupa es *pollin* o poleo. Aquí el elemento principal es el servidor y los periféricos a su alrededor; pregunta continuamente a las unidades acerca de sus requerimientos de transmisión y procesamiento, atiende el correspondiente y al terminar pregunta a otra.

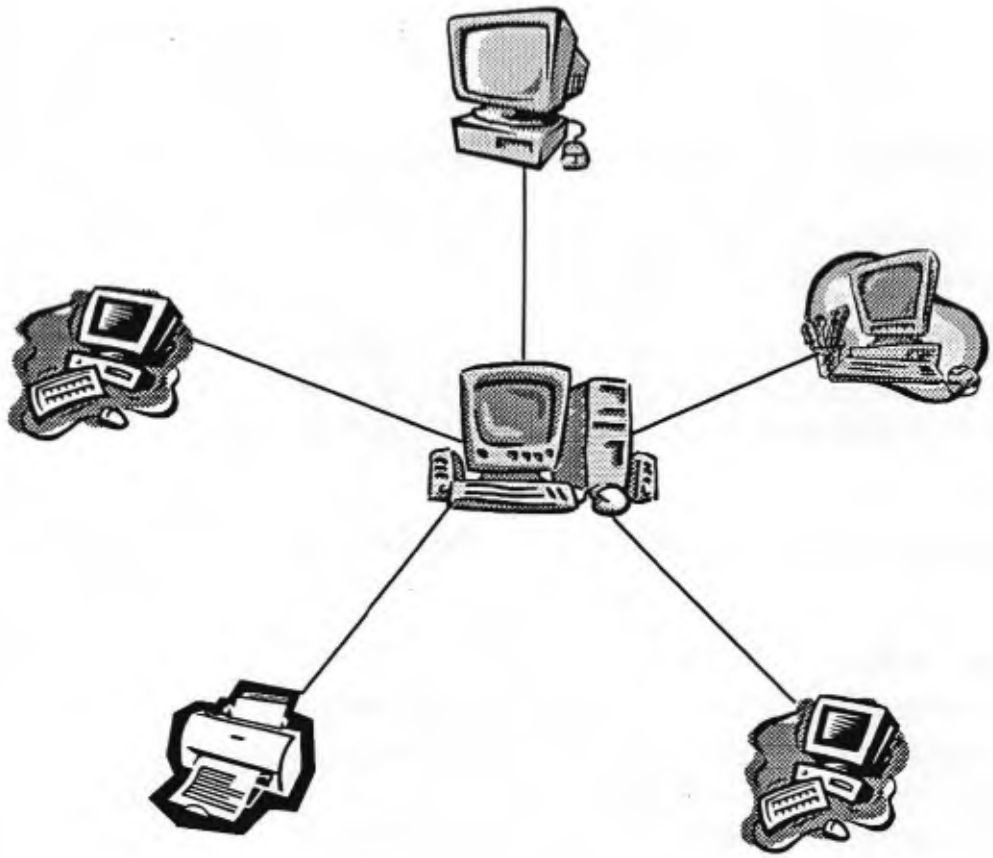

Figura 1

Configuración tipo estrella

Topología tipo bus. Se considera la más sencilla, pues todos los nodos están conectados a un único canal de comunicación incluyendo al servidor; la información va en ambos sentidos y mediante el protocolo lógico CSMA/CD[7] pregunta si la información ya se recibió, si no, espera un tiempo a que se desocupe el canal y transmite nuevamente.

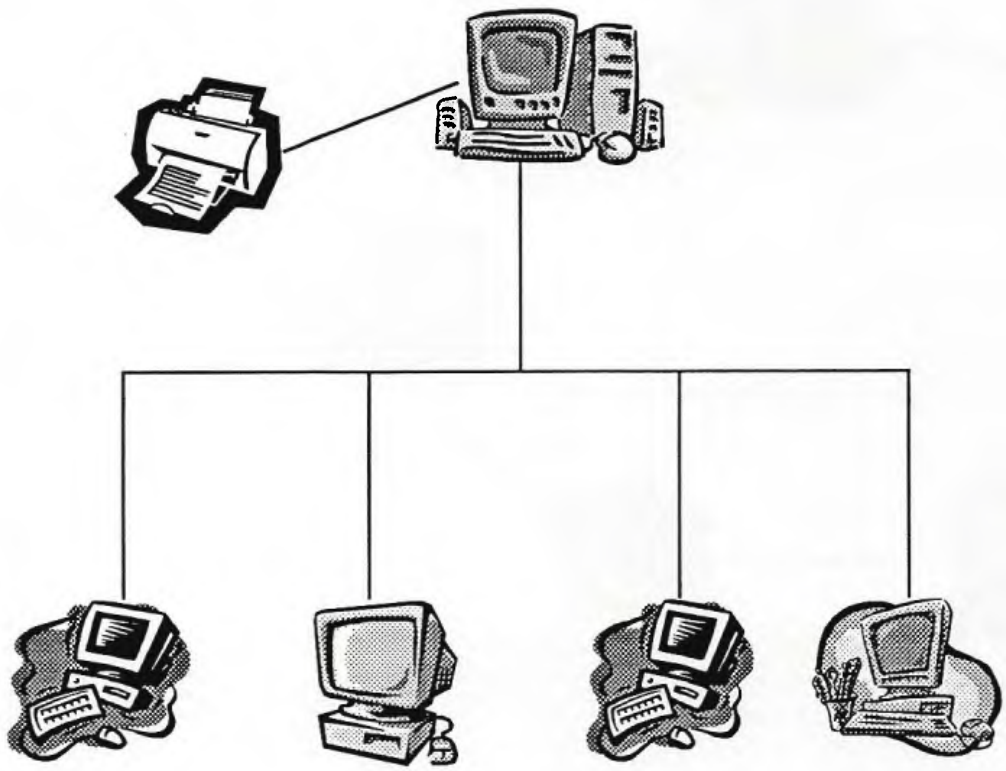

Figura 2

Configuración tipo bus

[7] (carrier sense múltiple access/ collision detection) sensor de acarreo de múltiple acceso/ detección de colisiones.

Topología de Anillo. En una configuración de anillo, los nodos de la red están colocados de manera circular formando un anillo, lo que permite que cada estación tenga conexión con otras dos estaciones. A simple vista, la topología física parecerá de estrella, mas la topología lógica sigue siendo de anillo. El protocolo lógico de comunicación es *ToKen Passing*.

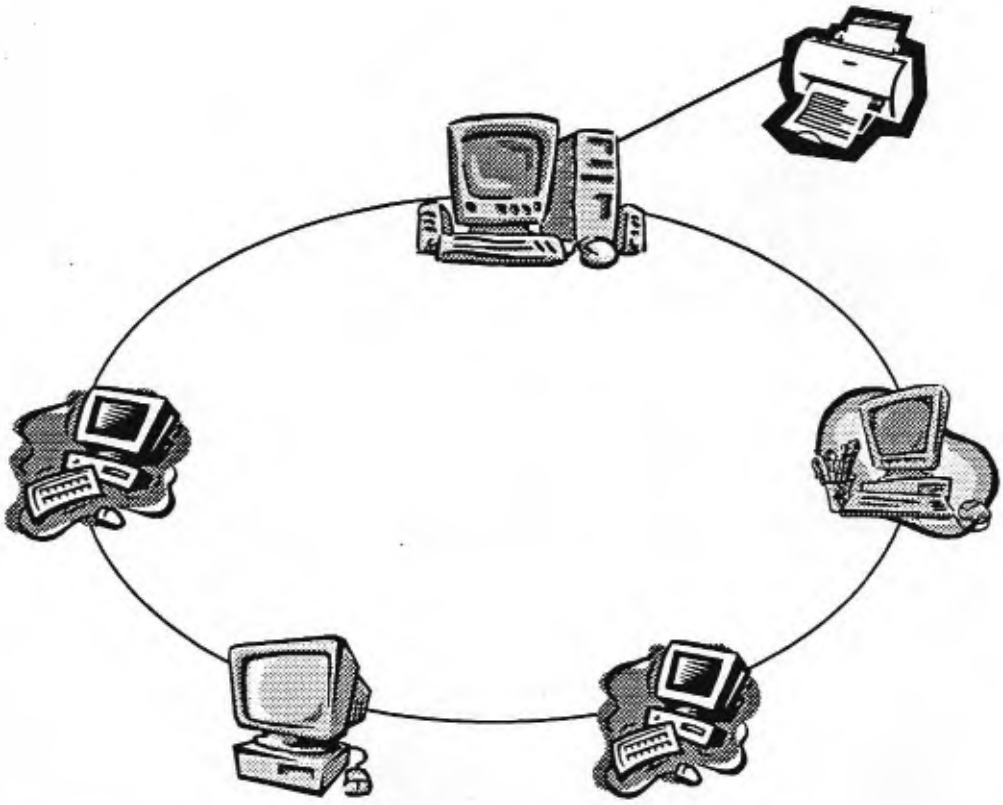

Figura 3
Configuración tipo anillo

Aquí la información va en un solo sentido por un solo canal; una señal(TOKEN) circula por la Red (formando 360°), pasa por cada estación y pregunta si hubo requerimiento, previa identificación de la estación de trabajo, hace la entrega, si no la vuelve a "guardar" y sigue el ciclo, llevando la instrucción de entregar hasta identificar al solicitante; todo lo anterior lo hace cerrando ciclos circulares.

La topología múltiple se enlaza mediante puentes y es una mezcla o combinación de las otras.

Protocolos

Se define como el conjunto de reglas y normas de comunicación como base fundamental en la red. Una pila de protocolos es un conjunto subdividido de protocolos que interactúan con el fin de propiciar la comunicación entre diversas aplicaciones, operando de manera conjunta a efecto de crear una plataforma consistente. A continuación se definen las características del protocolo TCP/IP:

Una pila de protocolos es un conjunto subdividido de protocolos que interactúan con el fin de propiciar la comunicación entre diversas aplicaciones, operando de manera conjunta a efecto de crear una plataforma consistente.

Arquitectura IP. El *software* de protocolo Inter-Red **(IP)**[8] opera tanto en *Hosts*[9] como en ruteadores IP. En general, el *software* IP permite a la computadora que lo ejecuta funcionar como un *host* IP, como un ruteador IP, o como ambos a la vez.

Acciones IP. Si el destino de la información no se encuentra en la red o fuera de ella. El IP decide el *ruteo* de la información mediante la detección de un destino remoto en una tabla de *ruteo.* El IP busca una entrada en la tabla de *ruteo* que corresponda al destino con la identidad del siguiente ruteador al cual será dirigido.

Arquitectura TCP. El TCP[10] se localiza en el *host.* La identidad de TCP en cada extremo de una conexión debe asegurar que los datos que se entreguen lleguen a su destino:

- Precisos.
- En secuencia.
- Completos.
- Sin datos duplicados.

TCP es un protocolo completamente bilateral, es decir, los dos extremos de la conexión pueden enviar y recibir información al mismo tiempo.

TCP/IP. Historia y generalidades

- 1969 Empieza el trabajo con ARPANET.[11]

---

[8] internet protocol (protocolo de internet).
[9] Se denomina *host* a un servidor central dependiendo sus características y ubicación.
[10] tcp transmision control protocol (protocolo de control de transmisión).
[11] arpa red que interconectaba a varias universidades y centros de investigación relacionados con el gobierno de los Estados Unidos.

- 1972 Primera demostración de ARPANET.
- 1976 Empieza la implantación de TCP/IP
- 1980 Se libera TCP/IP con Unix 4.1 de la Universidad de Berkley.
- 1982 TCP/IP reemplaza a NCP en ARPANET.
- 1983 Se publica TCP/IP con especificaciones militares estándares.
- Aceptado por los centros de investigación y desarrollo de todo el mundo.
- SUN[12] le da a TCP/IP un posicionamiento comercial.
- Los ambientes más técnicos adoptan TCP/IP.
- Predecesores del ISO[13].

Tarjetas de Red. Para que las estaciones de trabajo puedan comunicarse con el resto de la red, cada una debe tener instalada una tarjeta de interfaz de red (network interface card, nic), adaptadores de red o simplemente tarjetas de red.

Las principales funciones de las NIC son:

- Comunicaciones entre servidores y estaciones de trabajo.
- Formación de paquetes para el envío de información.
- Codificación y decodificación.
- Acceso a tipo de cable.
- Mensajes.

Software de Aplicación. Se refiere a todo el *software* que se utiliza en Red, desde la plataforma base, administración, seguridad y herramientas de apoyo.

Telecomunicaciones: análisis, comparación y normas, conceptos fundamentales

A lo largo de la historia, los medios de comunicación han ido avanzando en paralelo con la creciente capacidad de los pueblos para configurar su mundo físico y con su creciente grado de interdependencia. La revolución de las telecomunicaciones y de la transmisión de datos ha empujado al mundo hacia el concepto de "aldea global". Los efectos de estos nuevos medios de comunicación sobre la sociedad han sido muy estudiados. Hay quienes sostienen que los medios de comunicación tienden a reforzar los puntos de vista personales más que a modificarlos, y otros creen que, según quién los controle, pueden modificar decisivamente la opinión política de la audiencia. En cualquier caso, ha quedado

[12] sun microsystems (microsistemas SUN).Empresa dedicada a comercialización de tecnología informáticas.

[13] International Standar Organization (Organización Internacional de Estándares)

demostrado que los medios de comunicación influyen a largo plazo, de forma sutil pero decisiva, sobre los puntos de vista y el criterio de la audiencia.

Se pueden denominar telecomunicaciones a la transferencia de información, tanto a pequeña como a gran distancia.

Comunicaciones y conectividad en una red de computadoras. Es necesario mencionar en la parte de comunicaciones, además de lo antes referido, que dentro de los aspectos primordiales están los protocolos de comunicaciones que deben cumplir con los estándares establecidos, existiendo protocolos físicos y dentro de los más conocidos esta la norma v.24.RS232C, así como la comunicación en línea la cual puede ser del tipo síncrono o asíncrono.

De igual, manera se considera además de los concentradores ya mencionados, los *modems*[14], los cuales se utilizan considerando un ancho de banda establecido y el cual permite no solo la transmisión de datos, también incluye la transmisión de voz. Al igual que la terminal o estación de trabajo, el *modem* generará la sincronía, manejando también el protocolo físico (v.24.RS232C) y el acoplamiento con la red telefónica de acuerdo a los tipos de red: conmutada o privada. Se menciona que este dispositivo de comunicaciones es uno de los más empleados todavía en las redes de área local (LAN's).

Modelo de referencia ISO-OSI[15]

Las tecnologías que el hombre ha inventado para comunicarse siempre han seguido ciertas normas o reglas para su aceptación en un grupo social, que puede ir desde su pequeña comunidad hasta una gran sociedad. En la época moderna las normas que rigen a las comunidades deben de tener carácter universal. Hablando de comunicaciones digitales las normas o reglas universales están representadas por el modelo ISO-OSI.

El modelo OSI estructura en siete niveles o capas, el fenómeno global de la comunicación, es un marco hoy en día obligado y universalmente aceptado. Este modelo se ha convertido en una referencia obligada para todo lo relacionado con la intercomunicación de computadoras.

---

[14] Módem, equipo utilizado para la comunicación de computadoras a través de líneas analógicas de transmisión de datos. El módem convierte las señales digitales del emisor en otras analógicas susceptibles de ser enviadas por teléfono.

[15] ISO/OSI Internacional Standar Organization (Organización Internacional de Estándares) / Open System Interconection (Interconexión de Sistemas Abiertos)

Desde el punto de vista de ISO, un sistema abierto es el conjunto de una o más computadoras con su *software*, periféricos y terminales, capaces de procesar y transmitir información. Las características del modelo podrían resumirse de la siguiente forma:

- Cada nivel está representado por una identidad de nivel. Los niveles equivalentes en dos sistemas diferentes se comunican de acuerdo con unas reglas y convenios denominados protocolos de nivel o protocolos de pares.
- Cada nivel proporciona un conjunto definido de servicios al nivel superior y a su vez utiliza los servicios que le proporciona el nivel inmediato inferior.
- La comunicación se realiza a través de los niveles inferiores, siendo el protocolo de pares una abstracción lógica de relación entre las dos entidades comunicantes.

LOS SIETE NIVELES

NIVEL	DESCRIPCIÓN	FUNCIÓN
7	Aplicación	Provee servicios a los usuarios de la red: -Correo electrónico. -Transferencia de archivos. -Emulación de terminales.
6	Presentación	Realiza transformaciones en la información: -Conversión de código. -Compresión. -Encripción. -Conversión de formatos de archivo.
5	Sesión	Define el procedimiento para iniciar la comunicación entre dos procesos a nivel de presentación. Interfase entre el usuario (*software*) y de la red.
4	Transporte	Verifica que los paquetes lleguen en el orden requerido (secuencial).
3	Red	Agrupa en paquetes y define que camino toma cada paquete (*enrutamiento*).
2	Enlace de datos	Verifica errores de transmisión a nivel de *Frames*[16] y presenta al nivel tres una línea libre de errores
1	Físico	Define cómo será transmitida la información binaria: niveles de voltaje, modulación, velocidad de transmisión.

[16] Frame: trama o segmento

Características principales de las redes de área local

A nivel resumen se define que las características más importantes de las redes de área local son:

Área moderada. El espacio físico que abarca una red local suele estar limitado a un edificio o conjunto de estos, pudiendo variar la distancia máxima entre sus nodos desde una decena de metros hasta varios kilómetros.

Canal dedicado. El medio físico (canal) está exclusivamente dedicado a la comunicación que se produce entre las distintas estaciones de la red. Existen medios alámbricos e inalámbricos para establecer el canal de comunicación.

Baja tasa de errores. Debido a las características de especial dedicación del medio y las distancias relativamente cortas en que se produce la comunicación, los errores serán escasos y fácilmente corregibles.

Costo reducido. Uno de los principales objetivos que se toman en cuenta al planificar una red es que el costo de conexión entre los distintos sistemas informáticos sea notablemente inferior al precio del sistema informático propiamente dicho.

Modularidad. Las redes deberán ser muy flexibles tanto para la incorporación de nuevos elementos como para suprimirlos. La razón fundamental es que el entorno de la aplicación de las redes suele ser muy cambiante.

Posibilidad de interconexión de equipos heterogéneos. Con frecuencia, en una oficina o planta de fabricación, debido fundamentalmente a la rapidez con que se quedan obsoletos muchos equipos, éstos suelen proceder de distintos proveedores, siendo necesario que la red sea capaz de solucionar el problema de interconexión de todos ellos por lo que está directamente relacionada con la normalización.

Normalización

La normalización es la única vía que garantiza la compatibilidad de los equipos y la posibilidad de expandirse en un futuro evitando que queden obsoletos. Así se permite la independencia de los fabricantes, en el sentido de que si los productos están normalizados serán compatibles entre sí y en todo momento el comprador podrá valuar en distintas ofertas.

La normalización es la única vía que garantiza la compatibilidad de los equipos y la posibilidad de expandirse en un futuro evitando que queden obsoletos.

Además, con la normalización se cuenta con la garantía de soportar un conjunto de servicios bien conocidos basados en métodos y técnicas bien probadas. Y se cuenta también con la facilidad de la expansión, permitiendo añadir en un futuro nuevos equipos y nuevos protocolos a la configuración existente.

A continuación se citan algunos de los organismos encargados de la normalización:

ISO. Organización Internacional de Normalización, que presenta entre otras, el modelo de referencia OSI.

CCITT. Comité Consultivo Internacional Telegráfico y Telefónico, éste es un organismo de gran influencia en el entorno de las comunicaciones. Sus recomendaciones en cuanto a la conexión y cableado de interfaces son de aplicación común.

IEEE. Instituto de Ingenieros Eléctricos y Electrónicos, este organismo ha tenido un especial protagonismo en el tema de las redes. Las recomendaciones de la serie 802.1 a 802.6 prometen ser una norma muy estable para los niveles inferiores de las redes locales y han sido adoptadas por ANSI[17] también ECMA[18]. Ha puesto sus recomendaciones en consonancia con las de la IEEE.

En un principio, el modelo de referencia OSI fue concebido para normalizar las redes de área extendida en la que los niveles inferiores de la arquitectura quedan cubiertos por la red de conmutación de paquetes.

Al aplicar las consideraciones generales del modelo OSI a las redes locales, los niveles cuyas características resultan más peculiares son los locales, los niveles uno y dos (nivel físico y nivel de enlace). El organismo que ha conducido los estudios sobre normalización de estos niveles ha sido la IEEE y sus propuestas han sido aceptadas por los restantes organismos de normalización, ISO incluido.

Norma 801.1. Corresponde a un documento de contextualización de estas normas y su relación con el modelo ISO.

Norma 802.2. La recomendación 802.2 trata de una parte del nivel dos denominada control de enlace lógico, mientras que la otra parte de este nivel,

---

[17] ANSI. American National Standart Institute (Instituto de Estandar Nacional Americano).

[18] ECMA European Computer Manufacturers Association (Asociación Europea de Fabricantes de Computadoras).

más el nivel físico no se ha normalizado de una manera única, sino que han optado por generar diversas recomendaciones dependiendo del tipo de configuración y del método de acceso al medio. El nivel dos se subdivide en dos subniveles denominados control de enlace lógico y control de acceso al medio.

El primero de ellos es común para redes locales, mientras que el segundo es específico para cada una de las configuraciones.

Norma 802.3 CSMA/CD[19] Describe el subnivel de control de acceso al medio y el nivel físico, incluidas las distintas interfaces para redes locales con acceso al medio por el método de contienda en el que esta basado la red Ethernet. Cuenta con varios *adendum*, que ofrecen variantes en el medio de transmisión como 10BaseT. Un nuevo *adendum* define a *Fast Ethernet* de 100 Mbits/seg, usando el mismo protocolo de CSMA/CD.

Tipos más comunes de LAN 802.3 de banda base:

Nombre	Cable	Segmento máximo	Nodos/seg	Ventajas
10Base5	Coaxial grueso	500m	100	Bueno para Backbone
10Base2	Coaxial delgado	200m	30	Sistema más barato
10Base-T	Par trenzado	100m	1024	Fácil mante-nimiento
10Base-F	Fibra óptica	2000m	1024	Mejor entre edificios

Norma 802.4 Paso de Testigo en Bus. Regula el método de acceso por paso de testigo en bus (token passing bus), en sus dos versiones de banda bas y banda ancha, norma que ya ha sido aceptada por ISO. Esto fue usado en procesos automáticos de manufactura (MAP) para controlar robots en una línea de ensamble.

Norma 802.5 Paso de Testigo en Anillo. Este método de acceso fue de los primeros en ser usados en redes locales por su simplicidad desde el punto de vista lógico, debido a que existen múltiples versiones en cuanto a formato de tramas, existencia o no de prioridades, etc. No tiene topología definida ni tampoco medio de transmisión.

[19] CSMA/CD Carrier Sense Múltiple Access (Acceso Múltiple con Detección de Portadora). Lo que significa que puede detectar las colisiones.

Norma 802.6. Se refiere a Redes MAN[20], basada en la topología propuesta por la University of Western Australian, conocida como DQDB[21], la cual utiliza un bus dual de fibra óptica como medio de transmisión.

Normas 802.7 y 802.8. Son comités creados para apoyar y supervisar los desarrollos de tecnologías existentes que puedan migrar hacia fibra óptica o tecnologías en banda ancha (*broadband*), que utiliza señales analógicas y no digitales como los especificados anteriormente.

Norma 802.9. Se enfoca a arquitecturas e interfaces estándares, que permitan aplicaciones de escritorio con servicios integrados de voz, video y datos.

Norma 802.10. Este grupo desarrolla estándares concernientes a seguridad en una red de área local, que incluye mecanismos de seguridad en la transferencia de datos, administración de redes, administración de proceso de encriptación y procesos de seguridad compatibles con el modelo OSI.

Norma 802.11. Se refiere a las redes inalámbricas (Wireless LAN's) que especifica un sistema de red de área local por medio de radiofrecuencias.

Norma 802.12. Se prevé la posibilidad de que el Fast Ethernet, adendum de 802.3, se convierta en IEEE 802.12.

Norma 802.14. Es una propuesta no ratificada para Fast Ethernet pero que no utiliza CSMA/CD para la capa MAC. Por ahora a este proyecto se le denomina como 100Base-VG.

Internet

Denominada de manera común la red de redes. La internet ha alterado sin duda alguna y de manera permanente el paisaje de los negocios. Ha cambiado para siempre la forma en que las empresas interactúan entre sí, el modo en que la gente se comunica y la manera en que se distribuye la información de todo tipo. Se le usa para vender productos, proporcionar acceso a archivos, dar estadísticas y reportes actualizados instantáneamente, así como para enviar mensajes de correo electrónico de uno a otro extremo del mundo en segundos.

¿Qué significa en realidad estar en internet? Nuestra definición es que una máquina está en internet si opera con la pila de protocolos TCP/IP, tiene una dirección de IP y es capaz de enviar paquetes de IP a todas las demás máquinas de internet.

Una máquina está en internet si opera con la pila de protocolos TCP/IP, tiene una dirección de IP y es capaz de enviar paquetes de IP a todas las demás máquinas de internet.

[20] MAN metropolitan area network (redes de área metropolitana).
[21] DQDB distribuited queue dual bus (canal dual de cola distribuida).

Con el crecimiento exponencial, la antigua manera informal de operar la red ya no funciona. En enero de 1992 se integró la sociedad internet para promover el uso de ésta y quizá en algún momento hacerse cargo de su gestión. Tradicionalmente, internet ha tenido cuatro aplicaciones principales, que son las siguientes:

1. Correo electrónico.
2. Noticias.
3. Sesión remota.
4. Transferencia de archivos.

La world wide web

Se puede visualizar como un armazón arquitectónico para acceder a documentos vinculados distribuidos en miles de maquina de toda la internet; en cinco años, pasó de ser una manera de distribuir datos sobre física de alta energía a la aplicación que millones de personas piensan que es la internet. Su enorme popularidad se deriva del hecho que tiene una interfaz gráfica atractiva que es fácil de usar por los principiantes y proporciona un enorme cumulo de información sobre casi cualquier tema concebible.

La web (también conocida como www) se creó en 1989 en el CERN[22], en donde se tienen varios aceleradores en los que los científicos de los países europeos participantes llevan a cabo investigaciones sobre física de partículas. Estos equipos tienen media docena de países o más. La mayoría de los experimentos son altamente complejos y requieren de años de planeación experimentada y construcción de equipo. La web surgió de la necesidad de lograr que estos grupos de investigadores dispersos internacionalmente colaboraran usando un conjunto de informes, planos, dibujos, fotografías y otros documentos.

La propuesta inicial de una red (web) de documentos vinculados surgió del físico del CERN Tim Barners-Lee en marzo de 1989.El primer prototipo (basado en texto) estaba en operación 18 meses después. En diciembre de 1991 se hizo una demostración publica en la conferencia Hypertext '91 en San Antonio Texas. El desarrollo continuó durante el siguiente año culminando con la liberación de la primera interfaz gráfica, Mosaic, en febrero de 1993.

---

[22] CERN Centro Europeo de Investigación Nuclear

En 1994, el CERN y el MIT firmaron un acuerdo para establecer el World Wide Web Consortium[23], una organización dedicada al desarrollo de la web, la estandarización de protocolos y el fenómeno de operabilidad entre las instalaciones.

Los pasos que se ejecutan entre el clic del usuario y la presentación de las páginas web son las siguientes:

1. El visualizador determina el URL (viendo lo que se seleccionó).
2. El visualizador solicita la dirección IP.
3. El visualizador establece una conexión TCP.
4. A continuación, el visualizador emite un comando GET (extrae o baja) a un hypertext (archivo hipertexto).
5. El servidor www envía el archivo solicitado.
6. Se libera la conexión TCP.
7. El visualizador presenta todo el texto solicitado.
8. El visualizador trae y presenta todas las imágenes solicitadas.

La Internet ha llegado con gran fuerza y, en este mundo vertiginoso, eso plantea una pregunta importante: ¿Qué viene después?

Finalmente es importante mencionar las fases del diseño conceptual para una mejor elección de una red.

DISEÑO CONCEPTUAL
▪ Definir plataforma base. ▪ Elección de tipo de sistema operativo. ▪ Elección del sistema operativo y versión. ▪ Determinar número y tipo de servidores. ▪ Determinar configuración de servidores ▪ Determinar calendarios de instalación. ▪ Instalación. ▪ Determinar tipo de pruebas de aceptación. ▪ Efectuar pruebas de aceptación ▪ Puesta a punto de la red.

[23] La home page (página base) del consorcio puede encontrarse en http://www.w3.org

Bibliografía

Black Uyless. (1990), *Redes de computadoras. protocolos, normas e interfaces.* México, Macrobit Editores.

Enciclopedia Encarta 2000.

Facultad de Ingeniería de la UNAM. División de Educación Continua.(1995) *Diplomado en Redes.*México.

Jamsa Kris,Cope Ken (1998). *El mejor curso sobre TCP/IP* . México, McGraw-Hill.

Tanenbaum Andrew S (1998). *Redes de computadoras.* Prentice Hall. México.

Tema 3. Las bases de datos y los manejadores de bases de datos

Por Víctor Quintero González

Resumen

El acceso a los datos e información procesada en los ambientes corporativos es una de las tareas más urgentes de atender. Evitar la falta de información en los diferentes niveles directivos así como proporcionar información oportuna, en el momento adecuado y que sea veraz y de actualidad para la toma de decisiones, son los retos que los diseñadores de herramientas para el uso de tecnologías de la información deben considerar. Estas herramientas son desarrolladas para el manejo de grandes volúmenes de información y son las llamadas bases de datos. Las empresas no conciben hoy la planeación de sus actividades sin un adecuado soporte informático que permita la actualización, recuperación y consulta de datos. El material aquí contenido presenta una introducción al entorno de las bases de datos y las herramientas que se tienen para su análisis y desarrollo.

Tema 3. Las bases de datos y los manejadores de bases de datos

Por Víctor Quintero González

Bases de datos

En las épocas recientes y específicamente en el empleo y aprovechamiento de las tecnologías para el manejo de la información, se ha incrementado el uso de ambientes de desarrollo más poderosos, que permitan reducir los tiempos de elaboración de las aplicaciones y los costos asociados a éstas, así como los de mantenimiento. De igual forma, es importante que proporcionen mayor facilidad en el proceso de la información y en la interpretación de resultados.

Brevemente se menciona que una base de datos almacena y organiza información (por lo general bajo una descripción detallada) y permite incrementarla, manejarla, actualizarla y recuperarla rápidamente; y se define como un conjunto de archivos que contienen datos e información y se encuentran relacionados bajo una estructura definida.

Las bases de datos contienen información diversa y de diferentes tipos, como los siguientes:

Bases de datos	Tipos de información
Libros	Nombre de autor, nombre del título, ISBN, nombre de la editorial, precio del libro.
Inventarios	Código del producto, número de la parte, área de almacenamiento.
Control de activos	Nombre del bien, características, valor del bien, porcentaje de depreciación.
Medicina	Áreas de la medicina, tipos de enfermedades, tipos de pacientes, tipos de reacciones.
Beneficiarios	Año de nacimiento, clave de afiliación al seguro social, patrón actual, base de cotización.

Manejador de bases de datos

Es un conjunto de programas que interactúan entre los datos (archivos) y los usuarios. Ahora bien, es necesario establecer la distinción entre manejadores de bases de datos y las bases de datos: los primeros son los programas que controlan y actualizan a las segundas. No obstante, la mayoría de los usuarios se refieren a éstas en forma contraria o indistinta.

Podría esperarse que todos los manejadores de bases de datos fueran iguales, pero lo anterior desgraciadamente no es cierto. Cada DBMS[1] tiene características específicas y diferentes a las de los demás, lo que lo hace apropiado o no, para una cierta aplicación.

En un DBMS es necesario que se le diga cómo encontrar los datos que se requieren, no basta con que se le pida la información. Algunos vendedores de DBMS han añadido algunas extensiones muy útiles a su **SQL**[2] , como funciones sobre listas, matemáticas, estadística, etc; además de añadir tipos especiales de datos.

Características de los manejadores de bases de datos

Deben permitirle tanto al diseñador como al programador:

- Usar interfases nativas para interactuar con otros manejadores o lenguajes recientes.
- El acceso concurrente.
- Creación de ambientes gráficos.
- Creación de ayudas contextuales.
- Facilidad de compilar, corregir y actualizar las aplicaciones.
- Establecer criterios de acceso a los datos.
- Incluir validaciones de datos (independientes de las que el programador pueda establecer).

Para el usuario debe permitir en la parte de capacitación, proceso, actualización y recuperación de la información:

- Interfases sencillas.
- Posibilidad de menús.
- Procedimientos de consulta sencillos pero robustos.

---

[1] Data base management system (sistema manejador de base de datos)
[2] SQL. structured query languaje (lenguaje estructurado para consulta)

- Ayudas en línea.
- Reporteador básico.
- Generador de aplicaciones.
- Acceso a varios archivos simultáneamente.

En general, debe proporcionar independencia (al menos parcial) entre datos y programas. Esto es, que genere *modularidad* en la realización de aplicaciones, si cambian las rutinas o partes de código fuente no necesariamente deben cambiar las estructuras de los datos. De igual modo, debe proporcionar un lenguaje de interfase para el usuario que le permita realizar consulta y búsquedas con relativa facilidad (este lenguaje comúnmente llamado **QUERY** [3] o lenguaje de consulta).

El diccionario de datos permite definir las características de los datos y sus atributos una vez.

Cabe mencionar la importancia del diccionario de datos, el cual permite definir las características de los datos y sus atributos una vez, esto significa que si los datos son utilizados por varios usuarios, aplicaciones o archivos, no es necesario que se definan varias veces; por ejemplo, para el campo *código de cliente,* usado en varios archivos, es suficiente que sus características se definan y almacenen una vez, proporcionando un mejor control y la posibilidad de normalizar las estructuras de los datos. Esto es especialmente importante cuando diferentes programadores desarrollan módulos distintos del mismo sistema.

Herramientas o lenguajes de apoyo. Se utilizan para el manejo de la información en los sistemas de bases de datos. Dentro de estos se cuentan:

- Lenguaje de definición o descripción de datos (DDL), mediante el cual se crean las tablas y diccionarios de datos.
- Lenguaje de manipulación de datos (DML), con el cual se seleccionan los datos, se ordenan, se crean nuevas tablas.
- Lenguaje de consulta *(query language)*, el cual permite realizar consultas no planeadas; en ocasiones puede ser un subconjunto del lenguaje de manipulación de datos.

---

[3] QUERY, lenguaje de consulta estructurado, en informática, un *sublenguaje* utilizado en bases de datos para consultar, actualizar y manejar bases de datos relacionales. Se deriva de un proyecto de investigación de IBM, que creó el "lenguaje estructurado de consulta en inglés" (SEQUEL) en la década de los setenta. El SQL (structured query language) es un estándar aceptado en productos de bases de datos. A pesar de que no se trata de un lenguaje de programación como puedan serlo C o Pascal, puede utilizarse en el diseño de consultas interactivas y puede incluirse en una aplicación como un conjunto de instrucciones de manejo de datos. El SQL estándar cuenta también con elementos destinados a la definición, modificación, control y protección de los datos. Tanto los usuarios técnicos como los que no lo son pueden utilizar este lenguaje.

El Estandar SQL

Un programa servidor de base de datos es un motor que realiza matemáticas relacionales en grupos de datos. En un programa servidor de base de datos no es necesario que se le diga cómo encontrar los datos que se requieren, sino la importancia de saber pedir la información.

Cada programa servidor de SQL, se equipa con un manejador de transacciones que asegura que las tablas y los índices sean sincrónicos, aún después de una falla en el sistema o en el programa.

El problema se presenta cuando un programa termina de manera abrupta, lo que le puede provocar que una transacción particular no se hayan actualizado, o bien, que los datos dentro del **buffer**[4] puedan perderse. El manejador de transacciones detectará esta condición y automáticamente removerá todas las actualizaciones parciales, de esta manera las tablas e índices solo reflejarán transacciones terminadas normalmente.

Los servidores de SQL también protegen los datos contra la pérdida de los mismos, después de una falla en medio de archivo. Tienen *utilerías* para respaldos y restauración que crean y restauran copias de la base de datos. Al comprarlos vienen equipados con utilerías para recuperar datos a futuro, con procedimientos que recuperan todos los cambios que se completen entre el último respaldo y el punto en el que falle el medio de almacenamiento. Todos los programas servidores SQL soportan una completa integridad por medio de la combinación de un único índice y el atributo de la columna no nula.

Todos los programas servidores SQL soportan una completa integridad por medio de la combinación de un único índice y el atributo de la columna no nula.

Lenguaje de consulta estructurado *(structured query language*: SQL), es más que un simple lenguaje de consulta, permite la definición y el manejo de datos. Sus principales características son:

- Incluye las operaciones que permiten el enfoque relacional (select, join, project, etc.).
- Permite recursividad en los *query's*.
- Permite interfases a otros lenguajes*(embedded SQL)*.
- Permite restricciones de acceso e instrucciones de seguridad.

---

[4] **Buffer** o **memoria intermedia es**, en informática, depósito de datos intermedio, es decir, una parte reservada de la memoria en la que los datos son mantenidos temporalmente hasta tener una oportunidad de completar su transferencia hacia o desde un dispositivo de almacenamiento u otra ubicación en la memoria. Algunos dispositivos, como las impresoras o como los adaptadores que las soportan, suelen tener sus propios buffers.

- Sin embargo, su característica primordial es que se considera un estándar aprobado por la ANSI desde1986.

De igual forma, las aplicaciones con bases de datos se pueden ir sofisticando y por lo tanto se hace necesario tener herramientas que simplifiquen esto; una de las tareas más importantes es la recuperación de datos en caso de fallas y al mismo tiempo asegurar la integridad y consistencia de la información. Es decir, la información consistente debe ser el reflejo del mundo real y en caso de fallas en el proceso de la misma no debe quedarse incompleta.

Para asegurar la consistencia de la información existe el concepto de transacción; es un bloque atómico (indivisible) de procesamiento (actualizaciones) de archivos. La transacción solamente puede estar terminada o no terminada, si algo pasó en el lapso entre el inicio y la terminación de la misma, ésta debe ser eliminada; ello se realiza mediante una bitácora donde están la referencia inicial y el movimiento de afectación del registro, si algo pasa se revisa la bitácora y se regresan los archivos a su estado inicial.

Diseño de bases de datos

En el diseño de bases de datos es necesario considerar los siguientes aspectos:

- **No trabaje sin una especificación**. Normalmente se antepone la falta de tiempo y recursos, pero en todo desarrollo o proyecto se necesita un arranque, un proceso y un producto claramente definidos. Se debe asegurar que se tiene una idea clara de lo que se está haciendo, de su entorno y del por qué se necesita hacer.
- **Defina un modelo**. Es necesario definir el modelo y/o estructura de datos antes de empezar.
- **Apóyese en algunas referencias previas** similares al desarrollo que está por iniciar.
- **Considere al usuario**. Cuando empiece a programar tenga en cuenta al usuario, no trabaje sin él, pues de otro modo estará en riesgo de regresar al inicio.
- **Normalice**. Siempre y en la medida de lo posible, depure la definición de sus datos hasta el máximo, así evitará duplicidad y optimará el desarrollo del código correspondiente, así como su mantenimiento.
- **Limite el desarrollo**. Defina los alcances del diseño y mantenga éstos hasta lo posible. Recuerde qué ajustes grandes a los datos pueden resultar en la siguiente versión.
- **Documente el trabajo**. A pesar de considerarse aburrido, es de vital importancia la documentación, ya que en ésta reside el antecedente para futuras actualizaciones. No olvide que la mayoría de los diseños se pierden cuando no se ha documentado apropiadamente.

La mayoría de los diseños se pierden cuando no se ha documentado apropiadamente.

Entre las principales consideraciones que se deben tener al diseñar bases de datos están las siguientes:

- Independencia de los datos.
- No redundancia de datos.
- Flexibilidad de acceso.
- Integridad de la información.
- Seguridad en la consulta y actualización de datos.
- Eficiencia en el diseño.
- Fácil administración de la base de datos.

De las herramientas que se han empleado al paso del tiempo para la generación de bases de datos, se tienen principalmente las llamadas estructuras de datos (listas, colas, árboles, etc.), con las cuales se pueden establecer las características principales de los procedimientos para el manejo interno de la información. Es importante mencionar en este punto que un buen diseño de estas estructuras optimará las posibilidades inherentes a las formas de acceder y manejar la información.

Los modos de acceder a la información de las bases de datos, normalmente caen en alguna de las siguientes formas:

- De acceso secuencial
- Acceso secuencial indexado
- Acceso directo (HASH), entre otros

Las bases de datos o DB (del inglés *data-base*) se desarrollaron a inicios de los sesenta y en los ochenta aparecieron los DBMS *(data base management systems)* y posteriormente aparecieron los llamados de cuarta generación. Actualmente hay una gran variedad de productos como *oracle, sybase, informix, progress, db2, access,* etc. Algunas bases de datos están siendo desarrolladas por expertos utilizando herramientas como java y bases de datos orientadas a objetos.

Modelos de bases de datos

Entre los diferentes modelos que existen, los más referidos son tres:

- jerárquico
- de red
- relacional

En el modelo jerárquico las relaciones son básicamente definidas de padre-hijo, como se muestra:

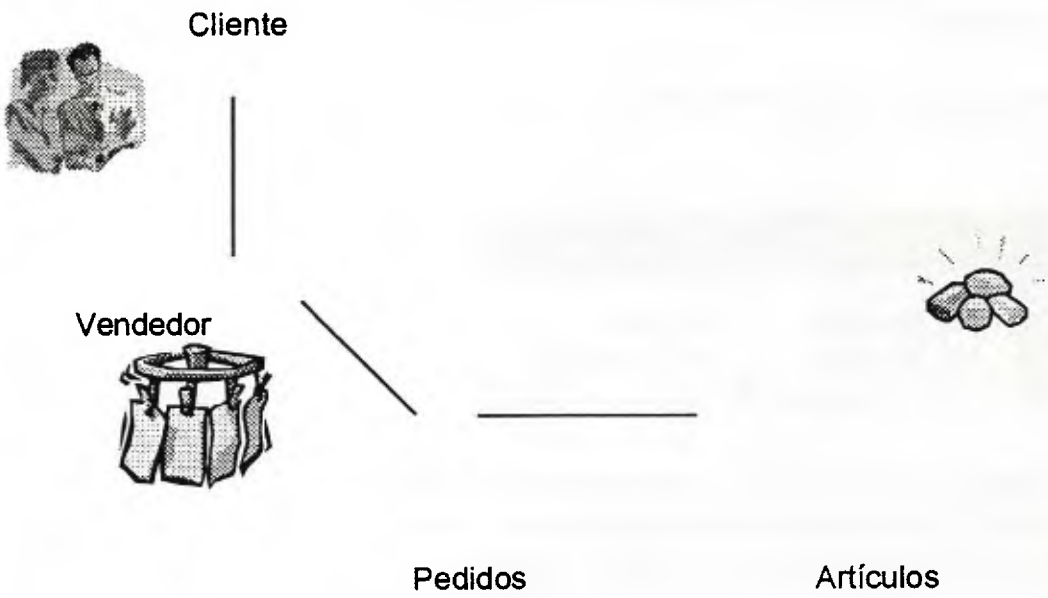

FIGURA 1

En el modelo de red se presenta el siguiente ejemplo:

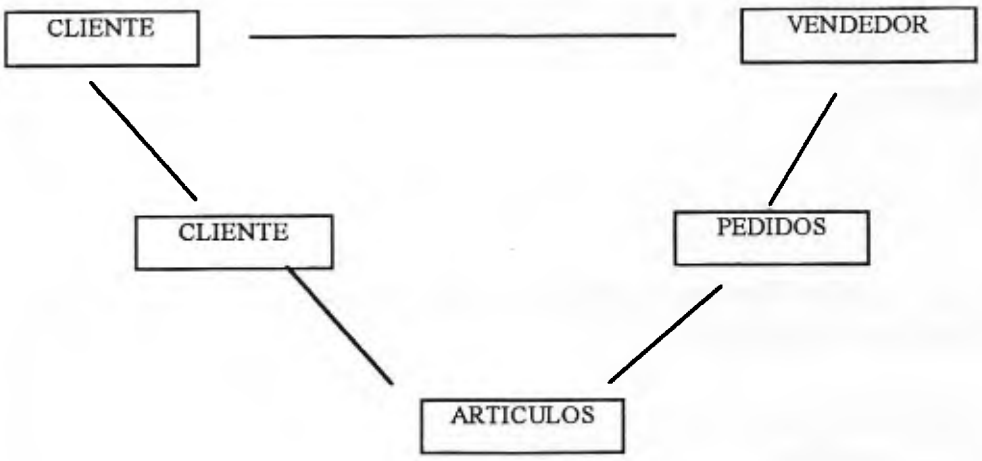

FIGURA 2

Aquí se aprecia que las relaciones no necesariamente son padre-hijo, se ve que también pueden existir variantes, por ejemplo de cliente a vendedor y de cliente a artículos, el mismo vendedor puede referir la base de datos de artículos. Lo anterior, respectivamente mediante las acciones de consulta y pedidos, donde éste último puede ser otra tabla.

En el modelo relacional se tiene el siguiente ejemplo:

CLIENTE	NOMBRE	VENDEDOR
pedidos **artículos**	No. de pedido No. de artículo	Vendedor No. de pedido

Se aprecia que las tablas se refieren entre sí mediante campos comunes en sus registros. Por ejemplo, se tiene que la tabla cliente incluye al vendedor, al igual que en pedidos y en artículos se incluye el número de pedido.

Creación de una base de datos

A continuación se ofrece un ejemplo breve de cómo se crea una base de datos. Inicialmente se tendría información aislada en diferentes campos, en este caso serían el número de cliente y el nombre del cliente.

No. de cliente: 001 Nombre del cliente: Juan Pérez

Con ellos se forma un registro:

001	Juan Pérez

De aquí tenemos que varios registros forman un archivo, por ejemplo, el archivo "clientes" estaría constituido como sigue:

Clientes

001	Juan Pérez
070	José Ruiz
143	César Simón
300	Julián Pérez

Y varios archivos relacionados entre sí forman una base de datos.

Archivo clientes

001	Juan Pérez
070	José Ruiz
143	César Simón
300	Julián Pérez

Archivo pedidos

001	020
070	021
070	022
070	029

Se ve la relación entre el archivo de clientes y otro archivo, pedidos en este caso, cuyo enlace es el número de cliente.

Al trabajar en el desarrollo de una base de datos, se deben considerar los siguientes aspectos:

En forma general:

- Necesidades contra buenos deseos (realidad).
- Filosofía de la empresa.
- Cambios y necesidades futuras.
- Las fuentes de obtención de información.
- Qué información se consultará en línea (terminales).
- Qué información se consultará vía documentos (reportes).
- Frecuencia con que se accederá a la información.

Con respecto a los archivos:

- Cómo se relacionarán los campos(datos) y con respecto a qué se definirá la longitud de cada uno.
- Definición de los archivos y su contenido.
- Estructura para el manejo de los archivos.
- Niveles de acceso a la información.
- Cuantas bases de datos se relacionarán con la que se está diseñando.

Es necesario involucrar al usuario desde el nivel operativo hasta el directivo, pues la parte de definición de requerimientos y necesidades se considera la fase que debe ser más creativa y una de las que más tiempo consumirá.

A continuación se presenta un diagrama que ilustra las fases generales del desarrollo de una base de datos.

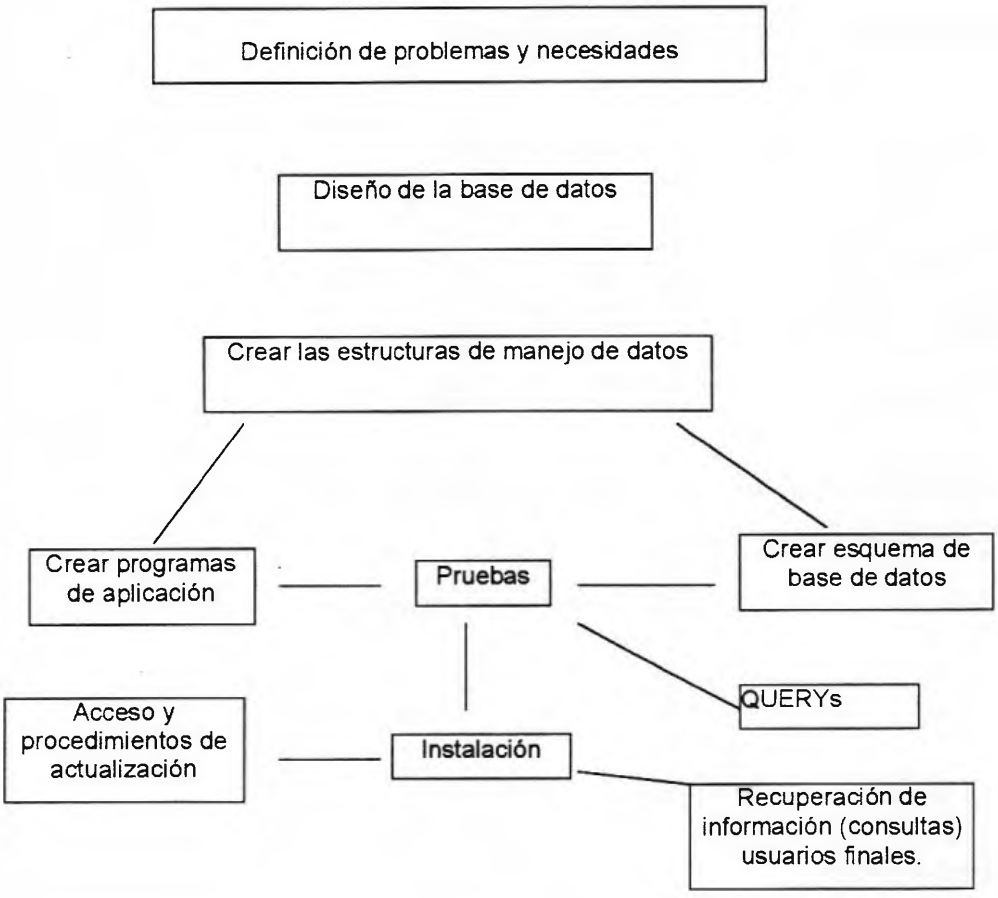

FIGURA 3

Implantación de bases de datos

Es posible construir sistemas de manejo de bases de datos con una amplia gama de generalidad. Una clasificación de estos enfoques en tres niveles distinguen los sistemas que apoyan a una sola aplicación, a varias aplicaciones del mismo tipo o a múltiples tipos de aplicaciones. Se han desarrollado algunos sistemas a través de estos tres niveles; otros se han diseñado para resolver problemas en un nivel específico.

Sistemas de bases de datos de una sola aplicación. Una organización establece una operación de base de datos utilizando las facilidades disponibles de sistema de archivo y diseña programas de aplicación, los cuales realizan una interfase a la base de datos usando un paquete mantenido, éste a su vez implanta el grado necesario de descripción de datos y de estructura.

Sistemas de bases de datos para varias aplicaciones del mismo tipo. Un grupo de usuarios trabajando en cierto tipo de áreas de aplicación reconoce la existencia de necesidades comunes. Por ello se diseña un sistema que cubra sus necesidades, esto es la diferencia principal a los de una sola aplicación.

Sistemas de bases de datos de tipo de aplicación múltiple. En donde se desarrolla un sistema que optima la base de datos cubriendo sus necesidades generales.

Ambiente moderno de bases de datos. La tecnología de las bases de datos puede eliminar de un tajo muchos de los problemas creados por la organización tradicional de archivos. Una definición más rigurosa de base de datos dice que es una colección de datos organizada para dar servicio eficientemente a muchas aplicaciones al centralizar los datos y minimizar aquellos que son redundantes. En lugar de separar los datos en diferentes archivos para cada aplicación, los datos son almacenados en una sola ubicación: una sola base de datos de personal (por ejemplo) sirve a muchas aplicaciones.

En lugar de separar los datos en diferentes archivos para cada aplicación, los datos son almacenados en una sola ubicación: una sola base de datos de personal (por ejemplo) sirve a muchas aplicaciones.

Sistemas de administración de bases de datos (SABD[5]). Es sencillamente el software que permite que una institución centralice sus datos, los administre eficientemente y proporcione acceso a los datos almacenados mediante programas de aplicación. Cuando los programas de aplicación llaman a un elemento de datos, el SABD encuentra ese elemento en la base de datos y lo presenta a un programa de aplicación. Usando los archivos de datos tradicionales, el programador tendría que definir los datos y luego decirle a la computadora dónde se encuentran. Un SABD elimina la mayoría de los argumentos para las definiciones de los datos que se encuentran en los programas tradicionales.

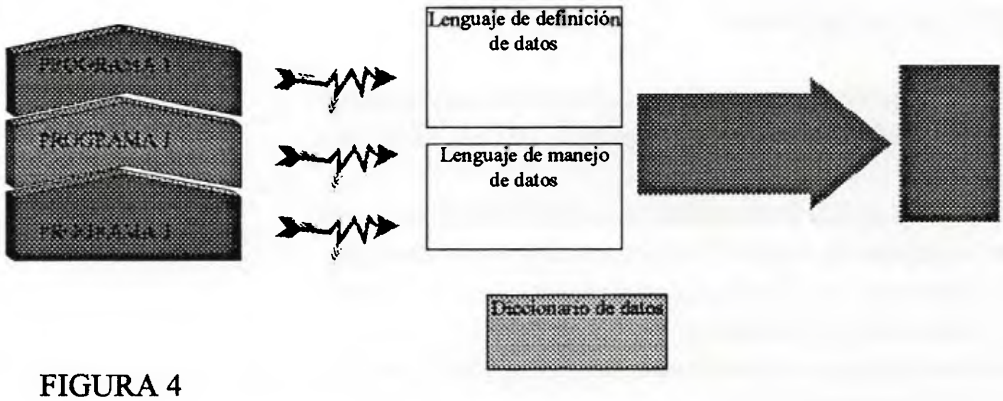

FIGURA 4

[5] SABD Sistemas de administración de bases de datos. *Software* especial para crear y mantener una base de datos y permitir las aplicaciones individuales de negocios para extraer los datos que necesitan sin tener que crear archivos por separados o definiciones de datos en sus programas de computadoras.

El sistema de administración de bases de datos tiene tres elementos:

- Un lenguaje de definición de datos
- Un lenguaje de manejo de datos
- Un diccionario de datos

Un lenguaje de definición de datos es el lenguaje formal empleado por los programadores para especificar el contenido y la estructura de la base de datos. Éste define cada elemento de datos como aparece en la base de datos antes de que este elemento sea traducido en las formas requeridas por los programas de aplicación.

Un lenguaje de definición de datos es el lenguaje formal empleado por los programadores para especificar el contenido y la estructura de la base de datos.

La mayoría de los SABD tienen un lenguaje especial llamado lenguaje de manejo de datos, que se usa en conjunción con algún lenguaje de programación de tercera o cuarta generación para manejar los datos en la base de datos. Este lenguaje contiene comandos que permiten a los usuarios finales y a los especialistas en programación extraer los datos en la base de datos para satisfacer solicitudes de información y/o para desarrollar aplicaciones.

El tercer elemento de un SABD es el diccionario de datos. Es un archivo automatizado o manual que almacena definiciones de los elementos de datos y características de los mismos, como su uso, representación física, propiedad (quién en la institución es el responsable de dar mantenimiento a los datos), autorización y seguridad.

Ventajas de los sistemas de administración de bases de datos

Las ventajas de un SABD son las siguientes:

- La complejidad del ambiente de sistemas de información de las instituciones puede reducirse mediante la administración centralizada de los datos, los accesos, el uso y la seguridad.
- La redundancia e inconsistencia en los datos puede reducirse al eliminar todos los archivos aislados en los cuales se repiten los mismos elementos de datos.
- Las confusiones en los datos pueden eliminarse al proporcionar un control central de la creación y definición de los datos.
- La dependencia en los datos del programa puede reducirse al separar la imagen física de los datos de su ordenamiento físico.
- El desarrollo de programa y los costos de mantenimiento pueden reducirse de manera radical.
- La flexibilidad de los sistemas de información pueden verse enormemente estimulada al permitir consultas rápidas y baratas dentro del gran volumen de información.
- El acceso y la disponibilidad de la información pueden incrementarse.

Bibliografía

Byrne Jeffry., (1997). *Microsoft access 97 visual.* México Prentice Hall. Hispanoamericana.

Deitel & Deitel., (1999) *C++ cómo programar*. México Pearson Prentice Hall.

Deitel M. Harvey., (1987). *Introducción a los sistemas operativos*. México Addison-Wesley Iberoamericana.

Gio Wiederhold (1997) *Diseño de bases de datos*. México Mc.Graw Hill.

McManus P. Jeffrey Madrid (1999) *Bases de datos con visual basic* Madrid, Sams Prentice Hall.

Rinehart Martin. (1998) *Desarrollo de bases de datos en java*. Madrid Osborne Mc. Graw-Hill.

EJERCICIOS Y ACTIVIDADES DE EVALUACIÓN

PRIMERA ACTIVIDAD
(Ejercicio individual)

A) A partir del enfoque de sistemas hacia lo general y lo particular, haga un ensayo sobre los siguientes puntos:

1. Su institución como entidad prestadora de servicios.
2. Su área de trabajo como parte de la organización.
3. La función informática dentro de su institución.

Extensión máxima: dos páginas.

B) Describa una propuesta general de desarrollo de un sistema de información o aplicación de usuario, utilizando alguna de las metodologías descritas en el contenido de este módulo, incluyendo las siguientes características:

1. Componentes de bases de datos, *hardware*, *software* y telecomunicaciones.
2. Utilizar alguno(s) de los niveles de sistemas de información dentro de la organización.

Extensión máxima: tres páginas.

C) Describa una propuesta general para el establecimiento de una red local en su ámbito de trabajo, ya sea como implantación de una nueva o como mejoramiento de la existente, utilizando el diseño conceptual como base e incluyendo las siguientes características: componentes principales, descripción específica de las bases de datos y telecomunicaciones necesarias.

Extensión máxima: tres páginas.

Módulo 2. Seguridad informática

INTRODUCCIÓN

La seguridad informática es una materia de relevancia ya que es requerida para garantizar la protección de la información contra riesgos y vulnerabilidades provocadas por los relajamientos de control presentes en el manejo de la información.

Los temas seleccionados para este material cubren aspectos fundamentales de la seguridad informática para fortalecer las medidas de protección de la información de las empresas.

Iniciamos con las políticas y normas ya que son el fundamento y el soporte de toda la actividad de protección, destacamos cómo deben realizarse, qué deben cubrir, qué son, por qué son importantes, qué niveles de seguridad existen de acuerdo al modelo americano, se dan ejemplos y se detalla el contenido de las políticas, entre otros aspectos. Como parte del primer tema también se resaltan los elementos críticos y de éxito para el establecimiento de un programa de protección de información, no sin antes comentar parte de los principales controles administrativos en el centro de cómputo.

Se destacan los aspectos relevantes de la seguridad física, la seguridad del *hardware* y del *Software*. En el primero se hace énfasis del control de acceso físico y lógico, los planes de recuperación ante contingencias y del segundo tema sobresale el tipo de mantenimiento requerido para proteger al *hardware* y *software* de acuerdo con los programas y tipos de mantenimientos.

Finalmente se presentan mecanismos de protección requeridos por las redes locales, destacando la seguridad física, lógica, *encripción* y protección contra virus, así como las redes de comunicaciones haciendo énfasis en el control físico y lógico, con base en el modelo OSI.

☞ OBJETIVO

- Estudiar los principios y fundamentos de la seguridad informática y su aplicación para disminuir los riesgos en el manejo de la información, la informática y las telecomunicaciones.

PALABRAS CLAVE

Análisis de riesgos
Atributos de seguridad
Claves de acceso
Control de acceso
Criptografía
Criticidad
Datos sensibles
Plan de contingencia
Riesgo
Seguridad física
Seguridad informática
Sistemas de seguridad

TEMAS

1. Políticas, normas, procedimientos y programas de seguridad informática
2. Seguridad física del hardware y del software
3. Seguridad en las redes y telecomunicaciones

Autor de todos los temas: Miguel Ángel Alvarado Sandoval.

Tema 1. Políticas, normas, procedimientos y programas de seguridad informática

Por Miguel Ángel Alvarado Sandoval

Resumen

El administrador de protección de información puede incrementar la efectividad del programa de *monitoreo* y reforzamiento a través de:

El aseguramiento de las políticas y procedimientos que están siendo *monitoreados* y reforzados.

Recordar que el *monitoreo* y reforzamiento sirve a varios propósitos proactivos y reactivos, siendo el más importante el proceso del medio ambiente. Todos los otros propósitos deben estar subordinados al objetivo primario.

Entender los objetivos del proceso para *monitorear,* reforzar y mejorar.

Asegurar que el programa de *monitoreo* y reforzamiento cubra a la empresa, su gente, su medio ambiente de negocio, y su tecnología.

Reconocer que el costo-efectivo es la medición primaria de un buen programa de mejora.

Plantear expectativas realistas del apoyo de la gerencia.

Verificar la credibilidad y mandato del programa de mejora, y si es necesario, actualizarlo antes de llevarlo a un entorno público.

Reconociendo que el *monitoreo* y el apoyo del reforzamiento es un rol de los especialistas de protección de información. La mejora actual es responsabilidad de la gerencia de línea.

Reconocer que hay otro personal involucrado: diseñadores, desarrolladores, proveedores, auditoría y operaciones.

Conocer qué está siendo *monitoreado*: el comportamiento del usuario, las fallas del sistema, los problemas administrativos, los planes de continuidad y sus características, los aspectos de diseño y desarrollo y ataques externos.

Utilizar el concepto de un problema de negocio en común cuando sea posible. El manejo de violaciones del administrador de protección de información puede hacer fracasar el programa. De nuevo, el administrador está tratando de mejorar el proceso y comportamiento, pero no a través del castigo.

Reconocer que los programas de capacitación y concienciación son fundamentales para una mejora efectiva.

Utilizar el crecimiento interno cuando sea necesario. Las funciones de tecnología están disponibles para *monitorear* y fortalecer las actividades. Pero auditoría, contabilidad, *monitoreo* y reporte no son lo más fuerte, completo y lo más maduro de las funciones de seguridad en sistemas distribuidos.

El *monitoreo* y reforzamiento de los requerimientos de protección de información son formas de aseguramiento de calidad del negocio donde las metas son mejora, confiabilidad y protección de los procesos. La justificación para el *monitoreo* y el reforzamiento de las actividades es una mejora del proceso del negocio. La tecnología y sobre todo la gente son los componentes más importantes para el éxito del programa.

Tema 1. Políticas, normas, procedimientos y programas de seguridad informática

Por Miguel Ángel Alvarado Sandoval

Introducción

Las políticas son el cimiento primario para cada esfuerzo hecho sobre la seguridad, auditoría y control. Para tener éxito el profesionista debe contar con un conjunto de políticas que soporten tanto al nivel directivo como al nivel administrativo. Las políticas se utilizan como referencia de una gran variedad de actividades, tales como: ejecución de auditorías, realización de análisis de riesgo, establecimiento de privilegios de acceso a los usuarios, conducir investigaciones sobre ilícitos y acciones disciplinarias para el personal que comete desviaciones a la norma.

Ya que las políticas tienen un impacto profundo en todos los esfuerzos de seguridad, auditoría y control, es muy importante que las políticas sean claras, suficientes y que den respuesta al medio ambiente informático en cuestión. Ya sea que la política exista o no, es recomendable que el profesionista responsable revise a las mismas de manera periódica, para evaluar si las políticas deben ser modificadas o aumentadas.

Hay quienes comentan que la seguridad, auditoría y control es un problema de personas, mientras que otros argumentan que es un problema de tecnología; ambos tienen razón. Pero antes que cualquier acción pueda hacerse respecto a seguridad, auditoría y control, la alta gerencia debe involucrarse. Por lo tanto la seguridad, auditoría y control es fundamentalmente un problema de administración.

De manera más precisa, el éxito en la seguridad, auditoría y control radican en el involucramiento de la alta gerencia. Sin su apoyo, habrá atención y presupuesto insuficientes dedicados a la seguridad, auditoría y control.

Una de las formas de éxito para contar con el apoyo de la alta gerencia, concienciarlos e involucrarlos en seguridad, auditoría y control es preparar políticas, las cuales por supuesto deben ser autorizadas y aprobadas por la alta gerencia. De hecho, el involucramiento inicial de la alta gerencia en la seguridad, auditoría y control en muchas ocasiones es provocado a través del esfuerzo del desarrollo de políticas.

Independientemente del tamaño de la organización, su industria, o del grado en que se ocupen las computadoras, la seguridad, auditoría y control es una materia importante que debe ser atendida a través de políticas explícitas.

¿Qué son las políticas de seguridad, auditoría y control?

Distinción entre guía y estándar. Las políticas son instrucciones administrativas que indican como debe correr una organización. Son declaraciones de alto nivel que ofrecen una guía a aquellos que toman decisiones presentes y futuras. Algunas personas prefieren pensar que las políticas son requerimientos generales. Aunque varían considerablemente de organización a organización, las políticas comúnmente incluyen enunciados generales de metas, objetivos, comportamientos, ética y responsabilidades. Tales políticas son frecuentemente acompañadas de medios generales llamados procedimientos.

Las políticas comúnmente incluyen enunciados generales de metas, objetivos, comportamientos, ética y responsabilidades.

Las políticas son mandatorias (se requiere aprobación especial cuando un trabajador desea tomar un curso de acción diferente), son distintas pero similares a las guías, las cuales son opcionales y recomendadas.

Las políticas son declaraciones de un nivel mayor que los estándares, aunque ambos tipos de instrucciones administrativas requieren cumplimiento. Las políticas ofrecen declaraciones generales, mientras que los estándares hacen mención a tecnologías, metodologías, procedimientos de implantación y otros factores de detalle. Hablando de manera general, la intención de las políticas es que duren muchos años, mientras que la intención de los estándares es que duran por pocos años.

Los estándares hacen mención a tecnologías, metodologías, procedimientos de implantación y otros factores de detalle.

Los estándares requieren ser cambiados con una mayor frecuencia que las políticas ya que los procedimientos manuales, las estructuras organizacionales, los procesos del negocio y las tecnologías de los sistemas de información mencionadas en los estándares cambian muy rápido.

> Por ejemplo, un estándar de seguridad en comunicaciones podría especificar que todos los sistemas nuevos o modificados deben cumplir con el estándar X.509 (que involucra la autenticación de un canal de comunicaciones seguro a través de criptografía de llave pública) emitido por ISO (International Standar Organization).

Distinción entre procedimientos y controles

Las políticas son distintas y se consideran de un mayor nivel que los procedimientos (algunas veces llamados procedimientos operativos). Los procedimientos son pasos operacionales específicos que los trabajadores deben realizar para alcanzar una cierta meta. Por ejemplo, en muchos centros de cómputo

hay procedimientos específicos para ejecutar respaldos de servidores y discos duros. Una política describe únicamente los medios generales para acatar un problema o situación específica; no debe volverse detallado, ya que se convertiría en procedimiento.

Las políticas también son diferentes de los controles (también conocidos como medidas de seguridad). El diccionario Webster define el control como un dispositivo o mecanismo utilizado para regular o guiar la operación de una máquina, aparato o sistema. Un ejemplo de un control sería la encripción de datos sensitivos almacenados en disquetes. En muchos casos, las políticas ofrecen objetivos amplios que se alcanzan a través de controles. Frecuentemente, las medidas de control son dictadas directamente por la política.

En general, las políticas determinan las áreas en donde la alta gerencia debe orientar su atención.

En general, las políticas determinan las áreas en donde la alta gerencia debe orientar su atención.

¿Por qué son importantes las políticas?

Aseguran la implantación apropiada de controles. Con la esperanza de manejar la seguridad, auditoría y control de manera expedita, la alta gerencia en muchas organizaciones simplemente compra uno o varios productos de seguridad y auditoría. En estos casos, la alta gerencia piensa que los nuevos productos ya sean *hardware, software* o servicios, es todo lo que necesitaran. Tan pronto como los productos son instalados, la alta gerencia se decepciona al saber que la espera en resultados no se ha materializado.

En muchos casos, esta decepción se fundamenta en el hecho de que la alta gerencia falló en establecer una infraestructura organizacional para las funciones de seguridad y auditoría.

En muchos casos, esta decepción se fundamenta en el hecho de que la alta gerencia falló en establecer una infraestructura organizacional para las funciones de seguridad y auditoría.

Para establecer una infraestructura de soporte organizacional cada organización necesita documentar políticas, guías, estándares, procedimientos, responsabilidades organizacionales, procedimientos de refuerzo de medidas de seguridad, un comité directivo, un proceso de determinación de riesgos y un proceso de planeación de la seguridad y auditoría.

Las políticas y una determinación inicial de riesgos son los puntos de inicio para establecer una infraestructura organizacional apropiada.

Guiando la selección del producto y el proceso de desarrollo. La mayoría de las organizaciones tienen recursos para diseñar e implantar políticas de la nada. Frecuentemente escogen controles proporcionados por proveedores, y de ahí se intenta adecuar estos controles con políticas, procedimientos y estándares.

Este proceso de integración es realizado sin el suficiente entendimiento de los objetivos y metas de seguridad y auditoría de la organización.

Como resultado, los productos de seguridad y auditoría seleccionados e implantados pueden no responder a las necesidades de la organización.

Las políticas que contienen los objetivos de seguridad y auditoría pueden ofrecer el entendimiento y guía adicional que los empleados requieren para actuar como la gerencia lo ha establecido.

Las políticas que contienen los objetivos de seguridad y auditoría pueden ofrecer el entendimiento y guía adicional que los empleados requieren para actuar como la gerencia lo ha establecido.

Tales políticas pueden ser el camino para asegurarse que el personal está seleccionado, desarrollando e implementando sistemas de manera apropiada.

Demostrar soporte gerencia. Algunas personas (particularmente usuarios y staff de sistemas) con frecuencia dicen: "Cuando la gerencia me lo diga, haré algo acerca de la seguridad y la auditoría". Esta actitud no es sorprendente cuando uno percibe que la mayoría de las personas no prestan atención a los riesgos que enfrentan, lo que significa que no se han tomado de manera seria el tiempo para analizar estos riesgos.

Además, al carecer de experiencia, la mayoría de la gente es incapaz de evaluar la necesidad de contar con ciertas medidas de control.

> Las políticas son una forma clara y definitiva de la gerencia para demostrar que 1) la seguridad y auditoría son importantes y 2) los empleados deben poner atención a la seguridad y auditoría.

Las políticas pueden cumplir estos objetivos que de otra manera provocarían que la gente protegiera de manera insuficiente sus recursos de información.

Un ejemplo encontrado de manera frecuente involucra a la gerencia media que repetidamente rehúsa asignar dinero a la seguridad y auditoría a su presupuesto.

Si las políticas dictadas con el soporte gerencial son avaladas por la alta gerencia, entonces la gerencia media no será capaz de continuar ignorando la seguridad y auditoría.

Las políticas son una forma directa y económica en la cual la alta gerencia puede definir un comportamiento apropiado, demostrar su interés, y especificar que comportamiento es aceptable o no.

Evadiendo responsabilidad. La ley está demostrando que el personal, particularmente los miembros de gerencia, pueden ser considerados como responsables de atender de manera inadecuada la materia de seguridad y auditoría. La base para esta responsabilidad puede ser negligencia, relajamiento de la responsabilidad, falla en el uso de las medidas de seguridad encontradas en otras organizaciones o en la misma industria, falla en ejercer la práctica profesional, o falla en la conducta después de que un evento comprometedor ha ocurrido.

La preparación y promulgación de políticas relevantes es una manera importante para que la alta gerencia demuestre que está interesada y está tomando acciones para implantar la seguridad y auditoría.

Requisitos para establecer políticas:

Contar con un presupuesto y personal.

Establecer un canal de comunicación con la alta gerencia.
Demostrar progreso significativo con una inversión mínima.

Establecer el esfuerzo de conformar la seguridad, auditoría con credibilidad y visibilidad.

Retomar actitudes positivas y cambiar perspectivas.

Demostrar el apoyo de la alta gerencia.

Evitar disputas sobre políticas internas.

Permitir el rápido desarrollo de nuevos sistemas.

Coordinar actividades de varios grupos.

Ejecutar economías de escala.

Evitar problemas por reinventar la rueda.

Establecer puntos de referencia para auditorías futuras.

Guiar en la selección e implantación de productos de seguridad y auditoría.

Asegurar la aplicación de controles de manera consistente.

Arreglar obligaciones contractuales requeridas por aspectos legales.

Establecer las bases para acciones disciplinarias.

Mantener la protección de los secretos comerciales para los activos de información.

Evitar faltas de responsabilidad por dolo o negligencia.

Documentar el cumplimiento con leyes y regulaciones.

Demostrar procesos de control de calidad (cumplimiento con ISO 9000).

Alcanzar la consistencia y seguridad completa.

Uno de los problemas significativos en el campo de la seguridad y auditoría involucra esfuerzos aislados y fragmentados. Frecuentemente un departamento apoyará los esfuerzos de seguridad y auditoría, mientras otros departamentos dentro de la organización se resistirán. En la medida que estos departamentos compartan recursos tales como redes de área local, los departamentos resistentes pondrán en riesgo la seguridad del departamento que apoya.

Aunque no es factible ni deseable familiarizar a todas las personas en la organización con las complejidades de seguridad y auditoría, es importante que implanten un nivel mínimo de protección.

En términos de alto nivel, las políticas pueden ser utilizadas para definir un nivel mínimo de protección *(baseline)*.

El "libro naranja" es un estándar que indica el nivel de seguridad.

Niveles de Seguridad. El departamento de Defensa de los Estados Unidos definió unos niveles de seguridad para los equipos de cómputo que se recogen en el denominado "libro naranja". Éste es un estándar que indica el nivel de seguridad, denominados A1, B3, B2, B1, C2, C, D siendo el D de menor seguridad y A1 de mayor.

Nivel D:

Estos sistemas tienen exigencias de seguridad mínimos, no se les exige nada en particular para ser considerados de clase D.

Nivel C1:

Para que un sistema sea considerado C1 tiene que permitir la separación entre datos y usuarios, debe permitirse a un usuario limitar el acceso a

determinados datos, y los usuarios tienen que identificarse y validarse para ser admitidos en el sistema.

Nivel C2:

Para que un sistema sea de tipo C2 los usuarios tienen que poder permitir o negar el acceso a datos a usuarios en concreto, debe de llevar una auditoría de acceso, e intentos fallidos de acceso a objetos (ficheros, etc.) y también especifica que los procesos no dejen residuos (datos dejados en registros, memoria de discos por un proceso al "morir").

Nivel B1:

A un sistema de nivel B1 se le exige control de acceso obligatorio, cada objeto del sistema (usuario o dato) se le asigna una etiqueta, con un nivel de seguridad jerárquico (alto secreto, secreto, reservado, etc.).

Nivel B2:

Un sistema del nivel B2 debe tener un modelo teórico de seguridad verificable, ha de existir un usuario con los privilegios necesarios para implementar las políticas de control, y este usuario tiene que ser distinto del administrador del sistema encargado del funcionamiento general del sistema. Los canales de entrada y salida de datos tienen que estar restringidos, para evitar fugas de datos o introducción de estos.

Nivel B3:

En el nivel B3 tiene que existir un argumento convincente de que el sistema es seguro, ha de poderse definir la protección para cada objeto (usuario o dato), objetos permitidos y no permitidos así como el nivel de acceso permitido a cada cual. Tiene que existir un "monitor de referencia" que reciba las peticiones de acceso de cada usuario y las permita o las niegue según las políticas de acceso que se hayan definido. El sistema debe ser muy resistente a la penetración de intrusos, así como tener una auditoría que permita detectar posibles violaciones de la seguridad.

Nivel A1:

Los sistemas de nivel A1 deben cumplir los mismos requerimientos que los de nivel B3, pero debe ser comprobado formalmente el modelo de seguridad definido en el nivel B3.

Muestra de políticas de la Asociación de Seguridad en Sistemas de Información (ISSA)

Política corporativa de seguridad en información

Propósito y alcance

El propósito de la política es establecer responsabilidades y roles de custodia para la protección de la información corporativa.

Política
La información es vital para la organización, activo que requiere protección proporcionado con este valor. Se tomaran medidas de protección al activo contra accidente o modificaciones no autorizadas, flagrancia o destrucción.

Responsabilidades

La administración es responsable de identificar, definir y otorgar el acceso al activo de información y protección a la información en caso de haber sido asignado al área administrativa de control.

La administración de seguridad de información es responsable de establecer, implantar y dar mantenimiento a la protección de la información.

Conformidad

Estas políticas y todos los estándares de soporte, procedimientos y lineamientos dentro del soporte de esta política servirá de estándar sea aplicado por la administración.

Política de seguridad en datos

Propósito

Establece una política base que la corporación usa, protege y preserva en el cómputo basado en los sistemas de información.

Alcance

Las políticas son aplicadas en toda la unidad de operación de la corporación y todo el procesamiento de la información por el mainframe, computadoras, minicomputadoras y microcomputadoras.

Política

Los recursos de cómputo y datos asociados del corporativo, son un activo vital para la campaña que requiere de protección apropiada.

Responsabilidades

Dentro de la función de seguridad de información se establecen e implantan las políticas, y estándares, procedimientos y los lineamientos necesarios que aseguren la seguridad del activo de la información. Proporciona soporte necesario a:

- *Administración*
- *Propietaria*
- *Custodia*
- *Usuaria*

Contenido del manual de políticas y normas de seguridad

- Responsabilidades en el manejo de la información
- Clasificación de la información
- Control de los medios de información
- Internet
- Respaldo y contingencias
- Reportes de desviaciones
- Notificación inmediata de virus
- Fallas de *software*
- Seguridad física
- Seguridad en comunicaciones

- Seguridad de servidores
- Seguridad en estaciones de trabajo
- Administración de usuarios
- Protección contra virus

Controles administrativos y el programa de protección de información

Los datos son uno de los recursos más valiosos de las organizaciones y, aunque son intangibles, necesitan ser controlados y auditados con el mismo

> La responsabilidad de los datos es compartida conjuntamente por alguna función determinada (el propietario de la información) y el departamento de cómputo (custodio de la información).

cuidado que los demás inventarios de la organización, se debe tener presente:

Un problema de dependencia que se debe considerar es el que se origina por la duplicidad de los datos y consiste en poder determinar los propietarios o usuarios posibles (principalmente en el caso de redes y banco de datos) y la responsabilidad de su actualización y consistencia.

Los datos deberán tener una clasificación estándar y un mecanismo de identificación que permita detectar duplicidad y redundancia dentro de una aplicación y de todas las aplicaciones en general.

Los datos deberán tener una clasificación estándar y un mecanismo de identificación que permita detectar duplicidad y redundancia dentro de una aplicación.

Se deben relacionar los elementos de los datos con las bases de datos en donde están almacenados, así como los reportes y grupos de procesos donde son generados.

Control de los datos fuente y manejo cifras de control

La mayoría de los delitos por computadora son cometidos por modificaciones de datos fuente al suprimir, adicionar omitir o alterar datos, así como por duplicar procesos.

Esto es de suma importancia en caso de equipos de cómputo que cuentan

con sistemas en línea, en los que los usuarios son los responsables de la captura y modificación de la información, así como de tener un adecuado control de señalamiento de responsables de los datos, con claves de acceso de acuerdo a niveles.

El primer nivel es el que puede hacer consultas. El segundo nivel es aquel que puede hacer captura, modificaciones y consultas y el tercer nivel es el que puede hacer todos los anteriores, y además, realizar bajas.

El primer nivel es el que puede hacer consultas. El segundo nivel es aquel que puede hacer captura, modificaciones y consultas y el tercer nivel es el que puede hacer todos los anteriores, y además, realizar bajas.

Control de operación

La eficiencia y el costo de la operación de un sistema de cómputo se ven fuertemente afectados por la calidad e integridad de la documentación requerida para el proceso en la computadora.

En la operación del *mainframe* el manejo de bitácoras, el control de procesos, el control de salidas de información, la actualización de los datos en los procesos *batch*, el respaldo de la información, el *monitoreo* de la disponibilidad del servicio y la atención de procesos y de situaciones de contingencias son acciones que todo personal de operación debe realizar de manera oportuna y eficiente.

Control de medios de almacenamiento

Los dispositivos de almacenamiento representan, para cualquier centro de cómputo, dispositivos que contienen archivos extremadamente importantes cuya pérdida parcial o total podría tener repercusiones muy serias, no solo en la unidad de informática, sino en la dependencia a la cual se presta servicio.

Una Dirección de informática bien administrada debe tener perfectamente protegidos estos dispositivos de almacenamiento, además de mantener registros sistemáticos de la utilización de los mismos y tener control con los programas de limpieza (borrado de información), principalmente en el caso de las cintas, además de tener perfectamente identificados los carretes para reducir la posibilidad de utilización errónea o destrucción de la información.

Un manejo adecuado de estos dispositivos permitirá una operación más eficiente y segura, mejorando los tiempos de procesos.

Control de mantenimiento

Como se sabe, existen básicamente tres tipos de contrato de mantenimiento:

el contrato de mantenimiento total, que incluye mantenimiento correctivo y preventivo, el cual a su vez puede dividirse en aquel que incluye las partes dentro del contrato y el que no las incluye. El contrato que incluye refacciones es similar a un seguro, ya que en caso de descompostura el proveedor debe proporcionar las partes sin costo alguno.

Este tipo de contrato es normalmente más caro, pero se deja al proveedor la responsabilidad total del mantenimiento a excepción de daños por negligencia en la utilización del equipo. (Este tipo de mantenimiento normalmente se emplea en equipos grandes).

El segundo tipo de mantenimiento "es por llamada": en caso de descompostura se le llama al proveedor y éste cobra de acuerdo a una tarifa y al tiempo que se requiera para repararlo (casi todos los proveedores incluyen, en la cotización de compostura, el tiempo de traslado de su oficina adonde se encuentre el equipo y viceversa). Este tipo de mantenimiento no incluye refacciones.

El tercer tipo de mantenimiento es el que se conoce como "en banco", y es aquel en el cual el cliente lleva a las oficinas del proveedor el equipo, y éste hace una cotización de acuerdo con el tiempo necesario para su compostura más las refacciones (este tipo de mantenimiento puede ser el adecuado para computadoras personales).

Al evaluar el mantenimiento se debe analizar primero cuál de los tipos es el que más nos conviene y, en segundo lugar, pedir los contratos y revisar con detalle que las cláusulas estén perfectamente definidas, eliminando toda subjetividad y con penalización en caso de incumplimiento, para evitar contratos que sean parciales.

Para poder exigir el cumplimiento del contrato se debe tener un estricto control sobre las fallas, frecuencia y el tiempo de reparación.

Para poder exigir el cumplimiento del contrato se debe tener un estricto control sobre las fallas, frecuencia y el tiempo de reparación.

Programa de protección de información

El primer requerimiento para establecer un programa de protección de información es que el programa en sí debe existir y estar fortalecido. De igual modo, un programa de *monitoreo* de protección de información debe iniciar con un claro entendimiento de las métricas a ser utilizadas y el significado y la utilidad de la información que ellas ofrecen.

Ambos conceptos son obvios; pero desafortunadamente, tiempo, esfuerzo y carreras son mal gastadas tratando de desarrollar políticas y procedimientos de trabajo equivocados en negocios particulares o medios ambientes institucionales.

Esto es especialmente verdad con políticas que han sido tomadas de literatura genérica o prestadas de otras empresas en lugar de ser hechas a la medida y probadas contra las necesidades, cultura y características de una organización específica.

El *monitoreo* sirve a varios propósitos. El más básico es la detección de eventos no deseados y el resultado de sus reacciones. Esto realmente tiene que ver con el reforzamiento de la seguridad. El otro propósito se liga con la *retroalimentación*, modificación y mejora de todo el sistema de protección.

¿Está el sistema comportándose de acuerdo con lo esperado? ¿Qué ajustes deben ser hechos? Por ejemplo, ¿Una alta tasa en rechazos significa que la seguridad es pobre o sensitiva?

Los problemas se agravan en ambientes híbridos y distribuidos, donde más y más políticas de protección de la empresa, primero construidas para un ambiente *mainframe*, están ahora siendo dirigidas a cientos de usuarios finales y gerentes de negocios, y no solo hacia personal operativo. Los medios ambientes operativos y de negocios son muy diferentes a las operaciones de staff de cómputo.

La naturaleza situacional de la protección de información

La métrica generalizada de una buena práctica de seguridad es de extrema importancia, hecho difícil de definir. En suma, el movimiento hacia la adopción de estándares generales y cuerpos comunes del conocimiento debe ser aplaudida. Sin embargo, algo importante por recordar es que la protección de la información —continuidad, integridad y confidencialidad— es un proceso situacional y subjetivo.

El movimiento hacia la adopción de estándares generales y cuerpos comunes del conocimiento debe ser aplaudida.

Se debe tener cuidado con el concepto de mejores prácticas y no confiar demasiado en él. Lo que es importante para una empresa puede no serlo para otra. El criterio de clasificación de los modelos de políticas (si los hay) están generalmente estructurados con base en a la confidencialidad.

Sin embargo, si el nivel de importancia de muchas empresas se enfoca a la prueba de confidencialidad de datos, en muchos casos la confidencialidad viene atrás de continuidad e integridad.

En el establecimiento de las prioridades de seguridad, la cultura, historia y naturaleza de la organización son tan importantes como la tecnología, aplicaciones y contenidos de información.

Estableciendo el interés de la gerencia

¿Qué es importante para la administración del negocio cuando ellos revisan las políticas y procedimientos de protección de información? El costo beneficio es aún un criterio de selección dominante, independientemente de qué controles de seguridad se requieren. Lo fundamental es que si no se venden los beneficios de la seguridad, la misma no se implanta.

El costo beneficio es aún un criterio de selección dominante, independientemente de qué controles de seguridad se requieren.

Por lo tanto, el primer paso para implantar programa de *monitoreo* y reforzamiento es revisar el conjunto de políticas y procedimientos que aseguran la aplicación en los procesos de negocio, medio ambiente, cultura y tecnología. ¿Cubren las mismas expectativas de la gerencia?, ¿Trabajan en los ambientes requeridos?

Las provisiones y requerimientos deben jugar un rol importante en los miembros de la organización que son los responsables de llevarlos a cabo. El nivel de conocimiento, experiencias y prioridades de los individuos involucrados debe revisarse para determinar si ellos pueden realizar las responsabilidades de protección que les han sido asignadas.

Con la implantación y reforzamiento del programa viene la hora de la verdad. Hasta ahora, el objetivo de la administración ha sido ligar tecnologías especificas aprobadas y establecer procedimientos de libros. Ahora, los recursos están siendo dedicados, los procesos están cambiando, y el comportamiento está siendo afectado. La implantación del programa puede ser traumática.

Mantener el soporte de la gerencia

Cuando la gerencia aprueba el programa de protección de información, es su deseo y objetivo que el mismo se lleve a cabo, no el de otros departamentos tales como el de auditoría, negocio, sistemas, etc. Los administradores de seguridad no deben sucumbir a las presiones de estos departamentos o de otras funciones staff.

Los departamentos piensen cómo la gerencia puede asegurar que los requerimientos de la administración se incorporen en el programa, y que los controles y la seguridad soporten los objetivos del negocio.

Lo mejor es que los departamentos piensen cómo la gerencia puede asegurar que los requerimientos de la administración se incorporen en el programa, y que los controles y la seguridad soporten los objetivos del negocio.

No importan las reacciones del nivel operativo o de gerencia media, los administradores de la protección de la información tienen el derecho y la obligación para insistir en los deseos y objetivos de la gerencia, para que la protección de información se realice. No obstante lo anterior, los administradores deben ser sensibles a lo que es razonable y factible.

Se debe medir el nivel de apoyo de la gerencia: si el conflicto sobre recursos y prioridades aparece cuando se esté implantando el programa de protección de información, y si la administración siente que tiene todos los elementos de su parte durante el conflicto, debe continuar con el programa , si no, debe replantear, ganar soporte o revender el programa de protección de información para que el mismo se establezca con éxito.

Establecer la motivación detrás del programa de protección de información

También con mucha frecuencia, los programas de protección de información son diseñados en respuesta a incidentes específicos o a una auditoría muy pobre. Ciertamente, los incidentes requieren remedios y las auditorías respuestas; pero un programa de seguridad diseñado exclusivamente, o aun de manera primaria para responder a reportes de auditoría, es un enfoque equivocado.

Si el programa de protección de información ataca de manera adecuada todas las necesidades de la organización, los comentarios de auditoría pueden ser atendidos. Si el programa no cubre las expectativas de ciertas áreas, aquellas áreas deben ser fortalecidas antes de que el programa se lleve a cabo.

***Monitoreando* y reforzando los objetivos y responsabilidades**

Comunicando los objetivos y obteniendo consenso. Las señales mezcladas son una acción fatal en la mayoría de los programas que fallan. Es esencial comunicar clara y exactamente las actividades de establecimiento del programa requeridas o autorizadas y lograr consensos Si la política y los objetivos de soporte de la gerencia tienen una orientación conservadora, los hechos deben ser comunicados a las áreas de tecnología y de negocio afectadas.

Revisar políticas y procedimientos actuales

Muchas políticas de protección de información son deficientes al describir las responsabilidades de monitoreo y reforzamiento del programa. Los administradores de protección de información deben identificar los requerimientos y consecuencias de la implantación de un programa efectivo de monitoreo y reforzamiento, y eventualmente proponer modificaciones si corresponden a las políticas, procedimientos, estándares y guías.

Los administradores de protección de información deben identificar los requerimientos y consecuencias de la implantación de un programa efectivo de monitoreo y reforzamiento.

Clarificar el rol del administrador de protección de información

Tal vez la situación más difícil que los administradores de protección de información pueden encontrar es la responsabilidad de establecer el programa sin la autoridad. En el análisis final, el establecimiento y mejora es una responsabilidad de la línea de la gerencia.

El rol del administrador es soportar el proceso de la administración, pero no actuar de manera unilateral. Los administradores deben revisar la estructura de políticas y procedimientos y asegurar que no quedan situaciones de seguridad sin atender.

Aún existe confusión respecto a quién es responsable de *monitorear* y quién es responsable de establecerlo. *Monitoreo*, en el sentido genérico, es un rol del administrador de protección de información. Apoyar en el establecimiento del programa, también es un rol del administrador. Esto es especialmente importante en ambientes distribuidos donde el proceso del negocio, no el tecnológico, es la infraestructura primaria en la protección de información.

Otro personal involucrado

De manera clara, la línea de gerencia está también involucrada en el establecimiento y *monitoreo* de un programa de protección de información, pero la gerencia y el administrador no están solos. Probablemente la función más importante que el administrador puede realizar es ayudar a comunicar los deberes y responsabilidades en materia de seguridad. Entre tales candidatos están:

- Los desarrolladores y diseñadores
- Los proveedores
- Auditoría
- Operadores del site

Violaciones de seguridad y anomalías que deben ser monitoreadas

A continuación se presenta una lista como ejemplo de una variedad de áreas donde una empresa puede dar seguimiento. No todas las organizaciones *monitorean* estas áreas. De hecho, existe desacuerdo sobre su importancia relativa. Una vez más, la efectividad del costo, recursos disponibles y factibilidad

son factores determinantes. Una muestra de temas que pueden ser fuente de violaciones y anomalías de seguridad incluyen:

Temas relacionados con el usuario.

Problemas de *passwords*.

Incidentes de virus.

Protección física de dispositivos, medios e impresos.

Enlaces *dial in –dial out* no autorizados.

Software no autorizado o sin licencia.

Peticiones de accesos no autorizados por procesos o usuarios autenticados.

Uso no apropiado de la red de comunicaciones o falla de uso de protecciones tales como la Encripción.

Liga o conexión a dispositivos no autorizados o inseguros.

Uso de *hardware* y *software* para fines diferentes a los del negocio.

Uso fuera de la oficina de los recursos del sistema.

Temas relacionados con fallas en el sistema o comportamiento no esperado.

Tiempos perdidos o bloqueos inesperados, incluyendo problemas de sincronización del server y fallas en sistemas de *password* de única vez.

Virus.

Aspectos de asignación y mantenimiento de *passwords*.

Aspectos de administración de la autorización.

Fallas y problemas de respaldos.

Problemas administrativos.

Problemas de corrección, completes y status de pruebas de planes de continuidad.

Aspectos de diseño, desarrollo y liberación de sistemas.

Ataques externos con sus advertencias y alertas.

El programa de concienciación de seguridad como una herramienta de reforzamiento

Los administradores de protección de información no deben subestimar el valor de un programa de concienciación en seguridad. Tal programa puede iniciar con una audiencia cooperativa y receptiva, asegurando que todos están trabajando como las mismas metas y objetivos buscando la misma prioridad. Sin embargo, para ser verdaderamente efectivos, el programa debe tener las siguientes características:

- Ser desarrollado desde la alta dirección.
- Ajustarse a las necesidades de la empresa.
- Ser consistente con los resultados y objetivos deseados del programa de protección de información.

Enfocándose a las actividades de reforzamiento y *monitoreo*

Al establecer el programa de reforzamiento, medición y *monitoreo*, es importante para los administradores de protección de información establecer el enfoque de la estructura de administración de la seguridad. Las tres opciones fundamentales son:

Al establecer el programa de reforzamiento, medición y monitoreo, es importante aplicar el enfoque de la estructura de administración de la seguridad.

Centrado en tecnología: el enfoque centrado en la tecnología monitoreado y reforzado por plataforma aún es válido en muchos centros de cómputo y procesadores independientes.

Centrado en la función del negocio (organización): el *monitoreo* y reforzamiento por función del negocio es una vista de seguridad que está emergiendo. Frecuentemente, por ejemplo, hay similitud entre las redes de área local y las funciones de negocio.

Centrado en procesos del negocio: el *monitoreo* y reforzamiento por procesos de negocio es adonde las organizaciones deben dirigirse. Un proceso de negocio tal como marketing o finanzas puede y probablemente trascenderá sobre uno o varios centros de tecnología y trascenderá también sobre una o varias funciones de negocio.

El híbrido: la situación de protección actual en muchas empresas es híbrida. En una situación híbrida, hay elementos de tecnología, funciones de negocio y procesos de negocio enfocados en diferentes niveles. Los administradores de protección de información deben tratar de clarificar esta situación si pueden. Mientras más consistente el punto de vista, más coherente y significativo el *monitoreo*.

Mientras más consistente el punto de vista, más coherente y significativo el monitoreo.

Soporte automatizado para el *monitoreo*

¿Qué se incluye en un programa de monitoreo efectivo? tecnología, obviamente. La detección, alerta, auditoría, contabilidad, reporte y análisis de funciones asociadas con redes de sistemas operativos, manejadores de bases de datos, aplicaciones, y seguridad y varios subsistemas de administración del sistema de *monitoreo* ofrecerán información básica sobre seguridad y en algunos casos información avanzada.

Sin embargo, especialistas de seguridad con experiencia en *mainframes* estarán tentados en llevar este enfoque del *monitoreo* en sistemas distribuidos, pero el modelo del proceso es diferente. Por lo tanto, el establecimiento, naturaleza y apariencia de las funciones de *monitoreo* deben diferir.

El administrador de protección de información debe estar familiarizado con el modelo de seguridad del Open *Software* Fundation/Distributing Computing Environment (OSF/DCE). Aunque el modelo fue diseñado sobre UNIX, Microsoft y Novell soportan ciertas funciones de seguridad del modelo.

Alarmas en ambientes distribuidos

El especialista de seguridad que se enfrenta con el *monitoreo* del ambiente distribuido (cliente/servidor, *peer to peer, store and foreward* y configuraciones lógicas similares) debe tomar interés especial en la estructuración de alarmas. La mayoría de los controles de acceso y los procesos de identificación, autenticación y autorización activarán una alarma en el evento de un comportamiento anormal.

La pregunta especial en ambientes distribuidos es: ¿Dónde debe ir la alarma?, Si, por ejemplo, la alarma es localizada en un *server* específico o puntos finales. De igual modo, la pregunta del tiempo también es importante. ¿La alarma es inmediata e interactivamente dirigida a un punto en donde recibirá atención y respuesta directa?, ¿Es registrada o olvidada?, ¿Es registrada en cualquier parte excepto el punto de origen?

Los administradores de protección de información deben especificar de manera cuidadosa sobre aceptar *defaults* de tecnologías en esta área, ya que las alarmas podrían no suministrar el nivel de soporte esperado.

Monitoreo y reforzamiento en medio ambientes especiales

Mucha de la doctrina sobre *monitoreo* y reforzamiento está basada en supuestos implícitos sobre la propiedad que la empresa tiene de los activos, control físico sobre el proceso, y el control de la administración sobre los participantes. Sin embargo, medios ambientes especiales tales como casa, viaje, e interempresas usualmente contradicen una o varios de estos supuestos.

No hay respuesta simple para *monitorear* estos medios ambientes, ya que esto difiere en forma significativa de una empresa a otra. Algunas de las variables por considerar son:

> ¿Quién es el dueño del procesador y su contenido?
> ¿Dónde está localizado el proceso?

El reforzamiento de las restricciones de telecomunicaciones puede ser soportado utilizando tecnologías de rastreo, limitando modos y trayectorias de acceso, y aun haciendo financieramente atractivo pagar servicios de comunicaciones seguros administrados por terceros.

Bibliografía

Alvarado Miguel Ángel, (1997) *Políticas de control de acceso a centros de cómputo,* (s/ed), México.

Arias Cuadros Sergio (1999) *Seguridad en centro de cómputo,* Dirección de Servicios de Cómputo, México.

Burch- Grudnitski (1998), *Diseño de Sistemas de Información,* Editorial: Megabyte, México.

Ministerio de Finanzas Públicas de Guatemala (1999), *Auditoría a Sistemas,* Guatemala.

Zella G. Ruthberg y Harold f. Tipton (1996), *Handbook of information security management,* Editors Auerbach, Nueva York.

Tema 2. Seguridad física del hardware y del software

Por Miguel Ángel Alvarado Sandoval

Resumen

Un aspecto muy importante en al seguridad física son los controles y mecanismos de seguridad dentro y alrededor del centro de cómputo para salvaguardar el hardware y software. Ello implica la instauración de medidas preventivas, detectivas y correctivas. Asimismo, es fundamental abarcar lo referente a sistemas de controles de acceso, sistemas de detección, tipos de control de acceso y normas de control en todo horario.

Del mismo modo, ante lo inevitable de considerar que cierto margen de riesgo estará siempre presente, se deben tomar precauciones ante las posibles contingencias, contando con un plan de recuperación de desastres. En éste, es necesario el establecimiento de procedimientos de respaldo en caso de desastre.

Tema 2. Seguridad física del hardware y del software

Por Miguel Ángel Alvarado Sandoval

Seguridad física de las instalaciones del centro de cómputo

La seguridad física se refiere a los controles y mecanismos de seguridad dentro y alrededor del centro de cómputo, así como a los medios de acceso remoto al equipo de cómputo, que se implantan para proteger el *hardware* y medios de almacenamiento de datos.

Este tipo de seguridad está enfocada a cubrir las amenazas ocasionadas, tanto por el hombre como por la naturaleza, al medio físico en que se encuentra ubicado el centro de cómputo.

Las principales amenazas que se consideran en la seguridad física son:

- Desastres naturales, incendios accidentales tormentas, inundaciones.
- Amenazas hechas por el hombre:
- Disturbios, sabotajes internos y externos deliberados.

Para afrontar este tipo de amenazas es necesario implantar medidas de protección preventivas, detectivas y correctivas, como las siguientes: considerar el tipo de materiales que se emplearon para la construcción física del centro; los procedimientos administrativos para prevenir el fuego; detectores de humo y calor; sistemas de extinción usando agua; sistemas de extinción; entrenamiento del personal para llevar a cabo ciertas acciones en caso de incendios; temblores e instalar personal de vigilancia en los accesos al centro de cómputo, por ejemplo.

Un punto importante es el control de acceso al centro de cómputo. Actualmente las instituciones dependen en gran medida de las computadoras, por lo que éstas y la información que en ellas se procesa debe ser protegida

contra toda clase de riesgos que afecten la continuidad de la operación y la confidencialidad de la información.

Sistemas de controles de acceso

Para hacer una selección correcta del sistema de control de acceso debemos tomar en cuenta las siguientes consideraciones:

Margen de error: determinar el porcentaje de error tolerable del sistema, es decir, hasta cuántas veces se aceptará que el sistema niegue el acceso a una persona autorizada, o lo permita a una que no cubre esta condición.

Protección en caso de fallas en el suministro de energía eléctrica: establecer el modo en que el sistema seguirá funcionando en caso de falla o interrupción de energía eléctrica.

Resistencia de manipulación: determinar hasta qué punto el sistema resistirá las manipulaciones o sabotajes.

Mantenimiento: considerar las facilidades para mantener el sistema en buen estado.

Flexibilidad: determinar hasta dónde podrá crecer el sistema en relación con el crecimiento de la institución.

Sencillez en su operación: evaluar el rendimiento que ofrece el sistema desde su instalación y puesta en marcha, hasta su aceptación y uso correcto.

Cantidad y frecuencia de acceso: considerar la cantidad de tráfico de entrada y salida del centro de cómputo.

Sistemas de detección

En cada uno de los accesos principales se debe considerar el sistema de esclusas equipado con detectores de:

- Metales
- Explosivos
- Material magnético
- Intrusos a través de sistemas infrarrojos

Además, es importante llevar un registro del personal autorizado por área de trabajo y horarios, principalmente de visitas a lugares como el centro de cómputo, comunicaciones, planta de emergencia, subestación, banco de baterías, y control de energía, por ejemplo.

Tipos de control de acceso

En las entradas principales e internas debe existir un sistema electrónico de control de acceso, con guardias las 24 horas del día.

En las entradas principales e internas debe existir un sistema electrónico de control de acceso.

El sistema de control de acceso podría ser desde un dispositivo simple hasta uno complejo. Dentro de esta gama encontramos:

Sistemas digitales: son dispositivos numéricos, en los que se solicita, a la persona que desee el acceso al centro de cómputo, teclear el código correcto. Se restringe el acceso por lo que la persona sabe.

Sistemas por medios magnéticos: se apoya en el uso de tarjetas magnéticas, de las cuales hay una gran variedad. Se restringe el acceso por lo que la persona tiene.

Sistemas biométricos: es importante considerar los medios de control de acceso biométricos. En ellos se restringe el acceso por lo que la persona es, de manera que es necesario verificar la voz, la retina del ojo, la huella digital o la palma de la mano, por ejemplo.

Sistemas de control para prevención de intrusión: en lugares donde debe encontrarse personal únicamente en determinados horarios, se deben considerar los detectores de perturbaciones (movimientos, ruidos, vibraciones); estos lugares son los siguientes:

- Areas perimetrales
- Salidas de emergencia
- Azotea
- Cuarto de baterías
- Cuarto de equipo de extinción de incendios
- Subestación

- Almacén
- Cuarto de aire acondicionado
- Estación satelital

Normas de control de acceso para distintas horas del día o la noche

Los controles de acceso deberán variar de acuerdo con las distintas horas del día. Es importante asegurar que los controles durante la noche sean tan estrictos como durante el día. Asimismo, deberán existir controles durante los descansos o cambios de turno y hacerse una revisión de personas que trabajan en horas o días no laborales.

Consideraciones generales

- Delimitar al centro de cómputo como área restringida para personal no autorizado.
- Controlar la entrada de personal autorizado con gafetes o algún otro medio de identificación, que señale además el área del centro de cómputo a la que puede tener acceso.
- Contar con puertas blindadas bajo el sistema de doble puerta o esclusa (trampa humana); Esto significa que al pasar la primera puerta, ésta se cierra y la siguiente no se abre hasta que el guardia identifique plenamente a la persona.
- Contar con un procedimiento por seguir en caso de que el personal que transporta medios de acceso los extravíe o los olvide.
- Contar con procedimientos de entrada y salida de suministros, dispositivos magnéticos, equipos e información procesada.
- Es importante considerar que los medios de control de acceso no impidan la fácil evacuación del centro de cómputo en caso de urgencia.
- No permitir alimentos o bebidas.
- No introducir material sin uso especifico (armas blancas o de fuego, gases inflamables, imanes, etc.)
- Negar acceso el personal que no cuente con los medios de identificación vigentes.

- No fumar dentro del centro de cómputo
- El personal debe ser responsable de la seguridad, los empleados deben estar motivados y entrenados para evaluar, decidir y actuar rápidamente y con buen juicio.
- El acceso debe ser limitado sobre la base "*need to know*".

Precauciones antes de la contingencia

Los conductos de aire acondicionado deben esta limpios, ya que son una de las principales causas de polvo. Se habrá de contar con detectores de humo que indiquen la posible presencia de fuego.

En las instalaciones de alto riesgo se debe tener equipo de fuente permanente, tanto en la computadora como en la red y los equipos de teleproceso.

En cuanto a las extintores, se debe revisar la cantidad de extintores que se ocupa, su capacidad, fácil acceso, peso y tipo de producto que utilizan. Es muy frecuente que se tengan los extintores, pero que no se encuentren recargados o bien que sean de un peso tal que sea difícil utilizarlos.

Es común, en lugares donde se encuentran trabajando hombres y mujeres, que los extintores estén a tal altura o con un peso tan grande, que no puedan ser utilizados.

Otro de los problemas es el uso de extintores inadecuados, lo que puede provocar mayor perjuicio a las máquinas (extintores líquidos) o bien producir gases tóxicos.

También se debe prevenir que el personal sepa utilizar los equipos contra incendio, por lo que son importantes las prácticas en cuanto a su uso.

Se debe verificar que existan suficientes salidas de urgencia y que estén debidamente controladas, para evitar robos a través de estas salidas.

Los materiales más peligrosos son las cintas magnéticas, que al quemarse producen gases tóxicos, y el papel carbón que es altamente inflamable.

Los materiales más peligrosos son las cintas magnéticas, que al quemarse producen gases tóxicos, y el papel carbón que es altamente inflamable.

Plan de recuperación de desastres

Es importante mencionar también que un plan de seguridad funciona solo cuando funcionan todos sus componentes. Para que esto suceda es necesario

establecer procedimientos y políticas administrativas que determinen las funciones y responsabilidades de cada uno de los departamentos y áreas del centro de cómputo y de la organización misma.

Como parte de las políticas y procedimientos administrativos es de vital importancia contar con un plan de recuperación de desastres que ayude a la organización (o centro de cómputo) a recuperarse rápidamente. Las metas principales del plan son:

Como parte de las políticas y procedimientos administrativos es de vital importancia contar con un plan de recuperación de desastres.

- Proteger la vida humana.
- Minimizar el impacto en las funciones de la organización.
- Contar con un procedimiento detallado por seguir cuando se presente algún desastre.
- Considerar el medio ambiente, no con la perspectiva tecnológica, sino de seguridad y protección.
- Contar con una póliza de protección contra amenazas internas y externas.

El proceso de recuperación de desastres implica: la habilidad de una organización para continuar sus operaciones diarias, a pesar de que ocurra alguna catástrofe, por medio de una serie de actividades coordinadas y planeadas. La póliza de seguro informal da a una organización perpetuidad, desde la perspectiva que los centros de cómputo y las telecomunicaciones son un medio crítico para la supervivencia de la organización.

Los centros de cómputo y las telecomunicaciones son un medio crítico para la supervivencia de la organización.

Procedimientos de respaldo en caso de desastre

Se debe establecer en cada área de informática un plan de emergencia, el cual ha de ser aprobado por la Dirección de informática y contener tanto procedimiento como información para ayudar a la recuperación de interrupciones en la operación del sistema de cómputo.

El sistema debe ser probado y utilizado en condiciones anormales, para que en caso de usarse en situaciones de emergencia, se tenga la seguridad que funcionará.

Se deben evitar supuestos que, en un momento de emergencia, hagan inoperante el respaldo. En efecto, aunque el equipo de cómputo sea

aparentemente el mismo, puede haber diferencias en la configuración, el sistema operativo o en disco.

El plan de urgencia, una vez aprobado, se distribuye entre el personal responsable de su operación. Por precaución, es conveniente tener una copia fuera de la Dirección de informática. Debido a la información que contiene el plan de urgencia, el mismo se considerará como confidencial o de acceso restringido.

La elaboración del plan y de los componentes puede hacerse en forma independiente de acuerdo con los requerimientos de emergencia. La estructura del plan debe ser tal que facilite su actualización.

Para la preparación del plan se seleccionará el personal que realice las actividades claves del plan. El grupo de recuperación en caso de urgencia debe estar integrado por personal de administración y técnico de la Dirección de informática, debe tener tareas específicas como la operación del equipo de respaldo, la interfaz administrativa y el restablecimiento del servicio.

El grupo de recuperación en caso de urgencia debe tener tareas específicas como la operación del equipo de respaldo, la interfaz administrativa y el restablecimiento del servicio.

Los desastres se pueden clasificar de la siguiente manera:

- Destrucción completa o parcial del centro de cómputo.
- Destrucción o mal funcionamiento de los equipos auxiliares del centro de cómputo (electricidad, aire, acondicionado).
- Destrucción parcial o total de los equipos descentralizados.
- Pérdida total o parcial de información, manuales o documentación.
- Pérdida del personal clave.
- Huelga o problemas laborales.

El plan en caso de desastre debe incluir:

- La documentación de programación y de operación.

- Los equipos.
- El equipo completo.
- El ambiente de los equipos.
- Datos y archivos.
- Papelería y equipo de accesorio.
- Sistemas (sistemas operativos, bases de datos, programas)

El plan en caso de desastre debe considerar todos los puntos por separado y en forma integral como sistema. La documentación estará en todo momento tan actualizada como sea posible, ya que en muchas ocasiones no se incorporan las últimas modificaciones y eso provoca que el plan de emergencia no pueda ser utilizado.

Registros vitales

Un concepto fundamental utilizado en los programas de recuperación y de continuidad de negocios son los registros vitales. Los registros vitales son recursos, medios e insumos que ayudan a restablecer el servicio a la brevedad, entre los que se pueden mencionar:

- Archivos
- Programas
- Manuales
- Personal clave
- Instalaciones
- Dispositivos
- Equipos de cómputo
- Insumos
- Equipo de comunicaciones.

El programa de registros vitales debe incorporar a áreas clave de la organización y contar con personal responsable que lo actualice de manera periódica.

Seguridad al restaurar el equipo

En un mundo que depende cada día más de los servicios proporcionados por las computadoras, es vital definir procedimientos en caso de una posible falta o siniestro. Cuando ocurra una contingencia, es esencial que se conozca a detalle el motivo que la originó y el daño causado, lo que permitirá recuperar en el menor tiempo posible el proceso perdido. También se debe analizar el impacto futuro en el funcionamiento de la organización y prevenir cualquier implicación negativa.

En todas las actividades relacionadas con las ciencias de la computación, existe un riesgo aceptable, y es necesario analizar y entender estos factores para establecer los procedimientos que permitan analizar los riesgos al máximo y en caso que ocurran, poder reparar el daño y reanudar la operación lo más rápidamente posible.

En todas las actividades relacionadas con las ciencias de la computación, existe un riesgo aceptable.

En una situación ideal, se deberían elaborar planes para manejar cualquier contingencia que se presente.

Analizando cada aplicación se deben definir planes de recuperación y restablecimiento del servicio, para asegurarse que los usuarios se vean afectados lo menos posible en caso de falla o siniestro. Las acciones de recuperación disponibles en el ámbito operativo pueden ser algunas de las siguientes:

- Capturar nuevamente toda la información para reanudar el proceso.
- Mediante copias periódicas de los archivos se puede reanudar un proceso a partir de una fecha determinada. Este procesamiento, complementado con un registro de las transacciones que afectaron a los archivos, permitirá retroceder en los movimientos realizados a un archivo al punto de tener la seguridad del contenido del mismo a partir de la reanudación del servicio del proceso.
- Analizar el flujo de datos y procedimientos y cambiar el proceso normal por un proceso alterno de urgencia.
- Reconfigurar los recursos disponibles, tanto de equipo y sistemas como de comunicaciones.

Cualquier procedimiento que se determine que es el adecuado para un caso de emergencia deberá ser planeado y probado previamente.

El grupo de urgencia deberá tener un conocimiento de los posibles procedimientos que puede utilizar, además de un conocimiento de las características de las aplicaciones, tanto desde el punto técnico como de su prioridad, el nivel de servicio planeado y su flujo en la operación de la organización.

En este desarrollo, correspondiente a la seguridad en centros de cómputo, se consideraron puntos críticos que afectan a las operaciones del centro. Asimismo, se contempló el manejo de información, comunicación de datos, seguridad física y lógica además del plan de contingencia que es efectuado por pocos centros de cómputo.

Seguridad en el *hardware* y *software*

Es necesario proteger los equipos de cómputo instalándolos en áreas con acceso restringido y sólo de uso para personal autorizado. Además, es necesario que estas áreas cuenten con los mecanismos de ventilación y detección de incendios adecuados.

El acceso a las redes y equipo *multiusuario* debe estar restringido o asignado de acuerdo con las necesidades de acceso a la información y programas por parte de los usuarios, haciendo uso de los programas y utilerías que los sistemas operativos y el *software* en general ofrecen.

También es conveniente asignar claves de acceso (*passwords*) a cada una de las cuentas (en red o equipos *multiusuarios*) y mantener activadas las opciones de auditoría de los mismos.

Seguridad en la utilización del equipo

En la actualidad, los programas y los equipos son altamente sofisticados y solo algunas personas dentro del centro de cómputo conocen al detalle el diseño, lo que puede provocar que puedan producir algún daño a los sistemas si no se toman las siguientes medidas:

Restringir el acceso a los programas y a los archivos.

Los operadores deben trabajar con poca supervisión y sin la participación de los programadores, y no deben modificar los programas ni los archivos.

Asegurar en todo momento que los datos y archivos usados sean los adecuados, procurando no usar respaldos de manera inadecuada e indiscriminada.

Prohibir la entrada a la red a personas no autorizadas, ni usar terminales.

Revisar y *monitorear* periódicamente el uso que se les está dando a las terminales.

Hacer auditorías periódicas sobre el área de operación y la utilización de las terminales.

El usuario es el responsable de los datos, por lo que debe asegurarse que los datos recolectados sean procesados completamente. Esto solo se logrará por medio de los controles adecuados, los cuales deben ser definidos desde el momento del diseño general del sistema.

Deben existir registros que reflejen la transformación entre las diferentes funciones de un sistema.

Debe controlarse la distribución de salidas como reportes o cintas.

Se deben guardar copias de los archivos y programas en lugares ajenos al centro de cómputo y en las instalaciones de alta seguridad; por ejemplo: los bancos.

Se debe tener un estricto control sobre el acceso físico a los archivos.

En el caso de programas, se debe asignar a cada uno de ellos, una clave que identifique el sistema, subsistema, programa y versión.

También se evitará que el programador ponga nombres que no signifiquen nada y que sean difíciles de identificar, lo que impedirá que el programador utilice la computadora para trabajos personales.

Otro de los puntos en los que hay que tener seguridad es en el manejo de información. Para controlar este tipo de información se debe:

Cuidar que no se obtengan fotocopias de información confidencial sin la debida autorización.

Observar que sólo el personal autorizado tenga acceso a la información confidencial.

Controlar los listados, tanto de los procesos correctos como aquellos procesos con terminación incorrecta.

Controlar el número de copias y la destrucción de la información y del papel carbón de los reportes muy confidenciales.

El factor más importante de la eliminación de riesgos en la programación es que todos los programas y archivos estén debidamente documentados.

El siguiente factor en importancia es contar con respaldos y duplicados de sistemas, programas, archivos y documentación necesarios para que pueda funcionar el plan de urgencia.

Controlar el equipo, programas y archivos, así como controlar las aplicaciones por terminal.

Definir una estrategia de seguridad de la red y de respaldos.

Controlar los requerimientos físicos y de equipamiento.

Manejar estándares de archivos.

Incorporar controles para auditoría interna en el momento del diseño del sistema, su implantación y puntos de verificación y control.

Bibliografía

Alvarado Miguel Ángel, (1997) *Políticas de control de acceso a centros de cómputo,* (s/ed), México.

Arias Cuadros Sergio (1999) *Seguridad en centro de cómputo*, Dirección de Servicios de Cómputo, México.

Burch- Grudnitski (1998), *Diseño de Sistemas de Información,* Editorial: Megabyte, México.

Ministerio de Finanzas Públicas de Guatemala (1999), *Auditoría a Sistemas*, Guatemala.

Zella G. Ruthberg y Harold f. Tipton (1996), *Handbook of information security management,* Editors Auerbach, Nueva York.

Tema 3. Seguridad en las redes y telecomunicaciones

Por Miguel Ángel Alvarado Sandoval

Resumen

Privacidad, integridad y disponibilidad son los tres requerimientos a los que de manera fundamental se refiere la seguridad en redes. En este ámbito deben tomarse medidas para evitar los problemas más frecuentes: fallas físicas, virus, espionaje y alteración de mensajes, accesos no autorizados a la red y el mal uso de recursos.

Para ello se precisa clasificar la instalación en términos de riesgo y establecer medidas en lo tocante al control de acceso físico, el acceso lógico, la aplicación de encriptores y la protección contra virus.

Líneas similares se abordan en cuanto a la seguridad en telecomunicaciones, en la que es necesario incluir, por ejemplo, controles para la protección de dispositivos programables, limitar el uso de herramientas de control, limitar el acceso a variables de programación y el monitoreo de cableado y enlaces.

Tema 3. Seguridad en las redes y telecomunicaciones

Por Miguel Ángel Alvarado Sandoval

Seguridad en las redes

La seguridad en las redes se enfoca a tres requerimientos:

- **Privacidad**: acceso solo a las entidades o usuarios autorizados.
- **Integridad**: los activos de un sistema solo pueden ser modificados por entidades autorizadas (escritura, cambio, borrado y creación).
- **Disponibilidad**: los activos de un sistema de cómputo deben estar disponibles a las entidades autorizadas.

Los problemas más frecuentes en un ambiente de redes y contra los cuales se deben establecer medidas preventivas y correctivas son: fallas físicas, virus, espionaje y alteración de mensajes, accesos no autorizados a la red, mal uso de recursos.

Los problemas más frecuentes en un ambiente de redes son: fallas físicas, virus, espionaje y alteración de mensajes, accesos no autorizados a la red, mal uso de recursos.

Para resolver este tipo de problemas se deben realizar acciones tales como: proteger los servidores y centros de cableado de la red; emplear *UPS'* y reguladores; mantener servers en espejo o emplear servers multiprocesadores; mantener discos en espejo o RAIDS (arreglos de discos); utilizar vías alternas en las líneas de comunicación, y utilizar procedimientos de encripción y autenticación de mensajes, por ejemplo.

Seguridad lógica y confidencialidad

La computadora es un instrumento que estructura gran cantidad de información, la cual puede ser confidencial para individuos, empresas o instituciones, y puede ser divulgada a personas que hagan mal uso de ésta. También pueden ocurrir, como ya mencionábamos con anterioridad, robos, fraudes o sabotajes que provoquen la destrucción total o parcial de la información residente en el centro de cómputo.

Esta información puede ser de suma importancia, y no tenerla en el momento preciso puede provocar retrasos sumamente costosos.

En la actualidad y principalmente en las computadoras personales, se ha dado otro factor que hay que considerar: el llamado "virus" de las computadoras. Una de las formas de infección es a través de paquetes que son copiados sin autorización ("piratas"), que llegan a provocar que se borre toda la información que se tiene en discos y en el servidor.

El uso inadecuado de la computadora comienza desde el uso de la máquina para propósitos ajenos de la organización, copia de programas para fines de comercialización sin reportar los derechos de autor, hasta el acceso por vía telefónica a bases de datos para modificar la información con propósitos fraudulentos.

Un método eficaz para proteger sistemas de computación es el *software* de control de acceso. Dicho simplemente, los paquetes de control de acceso protegen contra el acceso no autorizado, pues piden del usuario una contraseña antes de permitirle el acceso a información confidencial.

Un sistema integral de seguridad, como complemento de la seguridad lógica, comprende lo siguiente:

- Elementos administrativos.
- Definición de una política de seguridad.
- Organización y división de responsabilidades.
- Seguridad física y protección civil.
- Prácticas de seguridad del personal.
- Elementos técnicos y procedimientos.
- Sistemas de seguridad (de equipos y de sistemas, incluyendo todos los elementos, tanto redes como terminales).
- Aplicación de los sistemas de seguridad, incluyendo datos y archivos.
- Participación de los auditores, tanto internos como externos.
- Planeación de programas de desastre y su prueba.

Para identificar las prioridades de seguridad es necesario medir el riesgo que tiene la información y hacer un estudio eficiente de costo/beneficio, considerando tanto el costo por pérdida de información como el costo de un sistema de seguridad. En ello se debe considerar lo siguiente:

- Clasificar la instalación en términos de riesgo (alto, mediano, pequeño).

- Identificar aquellas aplicaciones que tengan un alto riesgo.

- Cuantificar el impacto en el caso de suspensión del servicio en aquellas aplicaciones con un alto riesgo.

- Formular las medidas de seguridad necesarias dependiendo del nivel de seguridad que se requiera.

- Justificar el costo de implantar las medidas de seguridad para poder clasificar el riesgo e identificar las aplicaciones de alto riesgo.

Una vez que se ha definido, el grado de riesgo, hay que elaborar una lista de los sistemas con las medidas preventivas que se deben tomar, así como las correctivas en caso de desastre, señalando a cada uno su prioridad.

Hay que tener mucho cuidado con el uso de la información que sale del centro de cómputo, por lo que es conveniente borrarla al momento de dejar la instalación que está dando respaldo.

Para clasificar la instalación en términos de riesgo se debe:

- Clasificar datos, información y programas que contienen información confidencial con un alto valor dentro del mercado de competencia de una organización, e información que sea de difícil recuperación.

- Identificar aquella información que tenga un alto costo financiero en caso de pérdida, o bien que puede provocar un gran impacto en la toma de decisiones.

- Determinar la información vital, cuya pérdida pueda provocar la quiebra de la organización.

- Para cuantificar el riesgo es necesario que se efectúen entrevistas con los altos niveles administrativos que sean directamente afectados por la suspensión en el procesamiento y que cuantifiquen el impacto que les puede causar este tipo de situaciones.

- Al implantar sistemas de seguridad puede reducirse la flexibilidad en el trabajo, pero no debe reducir la eficiencia.

Control de acceso físico

Los dispositivos de comunicaciones deberán contar con acceso restringido para el personal técnico facultado. En las instalaciones de comunicaciones se contará con dispositivos de acceso magnéticos a través de tarjeta magnética, así como detectores infrarrojos de intrusos.

Si se solicita mantenimiento o revisión por terceras personas, los proveedores autorizados por el administrador de la red de comunicaciones podrán acceder a los dispositivos de comunicaciones para ofrecer el soporte correspondiente.

La configuración de la red deberá estar documentada y actualizada además de tener registrados los cambios y pruebas en la red. Un punto importante que se debe considerar en la red es tener un inventario de las configuraciones de equipos, puertos, enlaces y servicios de comunicaciones.

Control acceso lógico

El usuario debe estar identificado con una clave de acceso que solamente él conozca para accesar al sistema y a la información, utilizando el principio del mínimo privilegio, además de apegarse las normas básicas de claves de acceso.

Si el usuario es remoto deberá tener un mecanismo de seguridad adicional al de la clave de acceso, como por ejemplo los tokens.

Si el usuario es remoto deberá tener un mecanismo de seguridad adicional al de la clave de acceso, como por ejemplo los tokens.

Todos los eventos realizados de seguridad serán registrados para su análisis periódico y solución.

Encriptores

Para envío de datos sensitivos en la red, los mismos deben estar *encriptados* siempre con la aprobación del área de seguridad; también se deben *encriptar* aquellos que estén en medios magnéticos.

En algunas empresas la información sensitiva es protegida de ataques externos utilizando la VPN o los *firewalls*, en donde se *encripta* la información vía *software*.

La información contenida en discos duros debe estar encriptada para evitar que sea saboteada o robada.

La información contenida en discos duros debe estar encriptada para evitar que sea saboteada o robada.

Para las claves de encripción deben existir dos personas responsables de la administración de llaves de *encripción*, de esta forma la responsabilidad queda limitada a los entes facultados y autorizados.

Deben existir dos personas responsables de la administración de llaves de encripción.

Las herramientas que se utilizan para generar las llaves de *encripción* deben estar resguardadas así como las versiones documentadas ya que estas claves tienen una vida variable y deberán cambiarse periódicamente.

Una forma de proteger las llaves de *encripción* es vía controles duales para repartir el conocimiento. De manera alterna pueden ser almacenadas en módulos a prueba de violaciones; y en cualquier otro lugar diferente al *encriptor* de *hardware* o *software* deben aparecer en forma *encriptada*.

Ahora bien, como información de alta sensibilidad los documentos de generación de llaves de *encripción* deben ser protegidos de divulgación, y si ya no se van a utilizar, las llaves deben ser destruidas.

Protección contra virus

En este apartado la responsabilidad es de todos los usuarios de equipos de cómputo: desde los administradores, supervisores, programadores y usuarios finales que deben tener el compromiso formal de:

- Sujetarse a las normas y políticas establecidas para la protección de equipo de cómputo contra virus informáticos.
- Reportar con oportunidad la detección de virus informáticos encontrados en sus equipos de cómputo asignados.
- Cumplir con los procedimientos establecidos para la prevención, detección y erradicación del virus.

Se debe adquirir un *software* antivirus con las siguientes características si no iguales pero la mayor parte como son:

- Facilidad de uso.
- Resistencia a ataques virales y protección después del uso.
- Calidad del soporte técnico por parte del proveedor.
- Encuestas de servicio y desempeño del *software* con otros usuarios.
- *Software* de plataformas múltiples.
- Nivel y periodicidad de actualizaciones de sus versiones.
- *Software* antivirus diseñado especialmente para uso de internet y correo electrónico.

Lo mencionado anteriormente son puntos relevantes que no se deben escapar para estar seguros de nuestra adquisición y que la misma responderá ante cualquier contingencia de virus.

Además de contar con el *software*, hay que hacer sensible al usuario de esta herramienta y darle a conocer los riesgos si no se protege la información contenida en el equipo o estaciones de trabajo.

Hay que hacer sensible al usuario de esta herramienta y darle a conocer los riesgos si no se protege la información contenida en el equipo o estaciones de trabajo.

Para evitar contraer algún virus vía internet, correo electrónico, disquetes, *software* ilegal, o incluso legal, se deben tener presente los siguientes puntos:

- Mantenimiento preventivo y correctivo del *software* antivirus; es decir, las actualizaciones deben ser oportunas.
- Uso moderado de disquetes. Antes de introducirlos al equipo, deben ser revisados por el antivirus.
- El acceso a internet debe estar restringido para los usuarios.
- El correo electrónico debe sujetarse a las normas para utilizar el correo ya que un mensaje no identificado —por no tener remitente, llevar un título desconocido o con caracteres extraños— debe ser notificado al administrador de red antes de que éste sea abierto.

Un mensaje no identificado debe ser notificado al administrador de red antes de que éste sea abierto.

- Notificar la aparición de virus, a fin de llevar a cabo la eliminación de acuerdo con los pasos planeados para eliminar o aislarlo, ya que algunos paquetes de *software* no tienen forma de eliminarlo y se debe esperar la actualización, observando en todo momento la evolución del virus.

Seguridad en las telecomunicaciones

Proteger con controles de acceso físico. El perímetro físico donde reside el equipo de comunicaciones y se encuentra seguro debe ser claramente establecido. Todo el equipo vital y los activos deben ser identificados, e incluso en el perímetro de seguridad los controles de acceso físico y la prevención del daño inmediatamente fuera de éste deben ser cuidadosamente considerados. El equipo, tal como interruptores eléctricos, equipo de comunicación y circuitos, deben estar localizados dentro del perímetro de seguridad, el cual ha de ser simple, fácilmente identificable. Es fundamental la existencia de planos y especificaciones del perímetro para ser utilizados en cambios de instalaciones.

Controles para protección de dispositivos programables

Para prevenir la entrada a las redes y a los puertos de mantenimiento establezca controles de acceso a los dispositivos. Los puntos de entrada a la red y a los puertos de diagnóstico deben protegerse con gabinetes cerrados, pastores y procedimientos. Algunos problemas se presentan en los dispositivos conectados a la red que permiten el acceso porque los controles son insuficientes o están indebidamente implantados. Uno de estos dispositivos, como lo es el ensamblador/desensamblador de paquetes (*pad*), puede ser accesado vía la red para las configuraciones iniciales y para ajustes finos. En este caso, el *password* para el *pad* pueden estar en texto protegido. Muchos dispositivos tienen mantenimiento de puertos para una configuración y control en el *site*, por lo que el puerto y el *password* deben ser controlados adecuadamente.

Limitar el uso de herramientas de diagnóstico. Para prevenir las modificaciones y el acceso no autorizado a los sistemas de cómputo y comunicaciones, las herramientas de diagnóstico de *hardware* y *software* usadas para analizar estos sistemas deben ser cuidadosamente protegidas. Estas herramientas pueden proporcionar, con base en una configuración de red, controles de acceso a ésta y desempeño de modificaciones. Lo anterior incluye herramientas para:

1. Conocer el uso de barreras lógicas en los activos informáticos.
2. Evaluar la conveniencia del uso de estas herramientas u otras.
3. Auxiliar el análisis de violaciones de seguridad.
4. Verificar algún tipo de *password* o su configuración.
5. Proporcionar un registro para tráfico extenso y *monitoreo*.
6. Establecer alarmas en sistemas y redes, las cuales deben ser cuidadosamente controladas.

Limitar el acceso a variables de programación. Es importante proteger la configuración de red y los datos relevantes para la operación. Los datos de configuración de la red incluyen la dirección de los nodos, los accesos y facultades, por lo que su acceso solo debe permitirse a un número muy limitado de personal técnico.

Proteger el acceso a la ejecución de instrucciones con riesgos. Este tipo de instrucciones, relacionadas con la operación de la red, generalmente están disponibles en línea y frecuentemente pueden ser activadas. Deben existir

controles para proteger la acción de comandos peligrosos y solo personal autorizado debe tener acceso mantener una bitácora que registre cada intervención.

Control de copias de información. El número de copias de archivo con los datos de comunicaciones (correo electrónico, archivo, *transfer*, por ejemplo) debe ser minimizado y controlado. Para archivos de cómputo y copias impresas, deben especificarse las fechas de destrucción e instrucciones por seguir, ya que los archivos almacenados en los sistemas y medios de cómputo son generalmente más seguros que almacenarlos en papel. Los procedimientos normales de respaldo a menudo requieren que varias copias estén almacenadas en diferentes bóvedas. Sin embargo, archivos con numerosas copias en diferentes localidades contribuyen a un riesgo potencial de una divulgación de datos, por lo que la información altamente sensible debe registrarse en una bitácora para su control y clara ubicación.

Archivos con numerosas copias en diferentes localidades contribuyen a un riesgo potencial de una divulgación de datos.

***Monitoreo* periódico de cableado y enlaces.** Los cables de comunicación pueden ser fácilmente desconectados de su origen y conectarse a través de *switches* para enlazar a otros dispositivos "piratas". Otros dispositivos pueden programarse para intentar dar acceso a las bases de datos conociendo el *password*. Al realizar la inspección ocular y aleatoriamente probar los enlaces, se podrá verificar que no existen dispositivos o conexiones ilegales a la red.

Bibliografía

Alvarado Miguel Ángel, (1997) *Políticas de control de acceso a centros de cómputo*, (s/ed), México.

Arias Cuadros Sergio (1999) *Seguridad en centro de cómputo*, Dirección de Servicios de Cómputo, México.

Burch- Grudnitski (1998), *Diseño de sistemas de información*, Editorial: Megabyte, México.

Ministerio de Finanzas Públicas de Guatemala (1999), *Auditoría a sistemas*, Guatemala.

Zella G. Ruthberg y Harold f. Tipton (1996), *Handbook of information security management*, Editors Auerbach, Nueva York.

EJERCICIOS Y ACTIVIDADES DE EVALUACIÓN

SEGUNDA ACTIVIDAD
(Ejercicio individual)

Realice un ensayo sobre políticas generales de seguridad informática en el que enuncie las mismas de acuerdo con la responsabilidad que desempeñen en su institución y con la realidad concreta de ésta. Las políticas se desarrollarán tomando como base la elección de uno de los siguientes temas:

- Programa de protección de información.
- Seguridad física
- Seguridad del *hardware*
- Seguridad del *software*
- Seguridad en redes locales
- Seguridad en telecomunicaciones

Se deben desarrollar entre 15 y 20 políticas. Extensión: de dos a tres páginas.

Módulo 3. Auditoría de Informática

INTRODUCCIÓN

La auditoría de informática es una materia que ha cobrado gran relevancia en los últimos años a consecuencia de la enorme penetración de la informática en las actividades de las grandes, medianas y pequeñas empresas, así como en instituciones públicas.

En todo el mundo se están tomando decisiones estratégicas vitales apoyadas en los resultados que los sistemas de información basados en computadora y las nuevas tecnologías de la información. Por lo tanto, la puesta en marcha de medidas de control y la administración adecuada a los riesgos a los que está expuesta la información y los demás activos de la institución, también adquieren notable trascendencia.

Funciones clave de la auditoría de informática son implantar, incrementar y evaluar las medidas de control en los ámbitos trascendentes del campo informático, es decir, en el *software* (tanto en programas como en el software del sistema), en el *hardware*, en las operaciones de cómputo, en los archivos de datos y en la propia administración de la función informática (incluyendo los recursos humanos).

Al igual que el vertiginoso cambio en la tecnología, la auditoría de informática también enfrenta nuevos retos, por ejemplo, la dificultad de ejercer controles en los ambientes distribuidos, en donde miles de trabajadores pueden tener acceso desde muchos sitios remotos o la conectividad que permite integrar redes con componentes.

El módulo que ahora nos ocupa, se centra en los aspectos de la auditoría informática aplicada a los sistemas de información, que siendo uno de los campos más estudiados, también requiere de una revisión continua para estar en sintonía con la evolución de dichos sistemas.

☞ OBJETIVO

- Estudiar los fundamentos de la auditoría en informática y la evaluación de las medidas de control.

PALABRAS CLAVE

Activos
Auditoría
Control interno
Debilidad de control
Índices de auditoría
Marcas de auditoría
Objetivos de control
Papeles de trabajo de auditoría
Pistas de auditoría
Riesgo de auditoría
Riesgo de control
Riesgo de detección
Riesgo inherente
Técnicas de control

TEMAS

1. Generalidades de Auditoría
2. Auditoría a sistemas en desarrollo
3. Auditoría a sistemas en operación

Tema 1. Reingeniería en las organizaciones

Por Sara Isabel Ayala Rodiles

Resumen

Este tema inicia con las generalidades de auditoría. Aquí se estudian sus fundamentos, las normas básicas para todo tipo de auditoría, los aspectos del control interno así como los factores que determinan la conjunción de estas dos grandes áreas: la auditoría y la informática, ambas con una continua y creciente expansión en sus respectivos campos de conocimientos.

El auditor de las áreas tradicionales como las administrativas, financieras y contables, ha tenido que involucrarse poco a poco en materia de informática y adaptar la metodología clásica de la auditoría a las características del entorno tecnológico y de sistemas de información. Sin embargo, la auditoría en cualquier campo que se estudie, no tiene como fin esencial el descubrimiento de los fraudes, sino que es una función que colabora con el bienestar, progreso y competitividad de la organización.

Ante los innumerables riesgos que amenazan a las instituciones, éstas se ven obligadas a ejecutar las acciones necesarias para la salvaguarda de sus activos más importantes y en este tema, especialmente se estudian los mecanismos para la protección de la información, recurso estratégico de toda organización.

Tema 1. Generalidades de auditoría

Por Sara Isabel Ayala Rodiles

Fundamentos de auditoría

Se puede definir el riesgo como peligro o contingencia de un daño. Se dice que la única manera de no correr riesgos es morir, pues aunque los seres humanos no hagamos nada estamos expuestos a diversos riesgos. Los riesgos y problemas son inherentes a la condición humana.

Así pues, todo auditor tiene el riesgo de que ocurran errores o irregularidades importantes, de que los sistemas no prevengan y/o corrijan los errores o irregularidades y de que cualquier error o irregularidad importante no sea detectada por el auditor.

El término errores se refiere a las fallas involuntarias en la información, tales como:

- Errores aritméticos, muchas veces derivados de la deficiente comunicación o del desconocimiento claro y preciso de la reglamentación aplicable por el personal del área de informática.
- Equivocación en la aplicación de normatividad.
- Falta de criterio o mala interpretación de los hechos.

La palabra irregularidad significa distorsiones intencionales en la información provocadas por cualquier persona, miembro de la institución o terceros. Algunos ejemplos son:

- Falsificación, manipulación o alteración de los registros.
- Omisión de información significativa.
- Registro de transacciones ficticias.
- Aplicación indebida de la normatividad.
- Malversación de activos.

Algunos ejemplos que pueden implicar la existencia de actos u operaciones ilegales o irregulares son:

- Regalos a terceras personas no identificadas, normalmente por cantidades excesivas.
- Pagos importantes a instituciones afiliadas o empleados sin propósito especifico y explicable de negocios.
- Falsificación de vales, préstamos, cheques, etc.
- Inclinación a cubrir ineficiencias.
- Peticiones de la administración a auditores de iniciar tarde la auditoría y presiones para terminarla urgentemente.
- Piratería de *software*, violando la legislación en materia de derechos de autor.

Las situaciones que incrementan el riesgo o posibilidad de errores e irregularidades son:

- Dudas con respecto a la integridad o competencia de la administración; la ética y los conocimientos se deben permear de arriba hacia abajo, el respeto por las personas y por la institución se ganan todos los días.
- Situaciones extraordinarias internas y externas: nueva reglamentación, nuevos tipos de transacciones.
- Operaciones fuera del curso normal de las operaciones de la entidad.
- Dificultad para obtener evidencia suficiente y competente en la auditoría, sobre todo porque en presencia del proceso electrónico de datos generalmente no se dejan suficientes huellas en papel y, además, existe una gran incultura informática.

Con relación a los fraudes, investigaciones realizadas en EE.UU. han determinado que la mayoría de los fraudes ocurre en establecimientos foráneos (fuera del control de las oficinas centrales). Los cometen en un 50% los jefes de departamento o administradores, es decir, quienes tienen autoridad para decidir sobre las operaciones y además poseen la habilidad para eludir el control interno.

Las personas que cometen fraudes provienen de cualquier trabajo o actividad, nivel económico o clase social. Los factores que originan el que se cometan fraudes son motivos y oportunidades.

Motivos

Problemas económicos, ocasionados no solo por la necesidades básicas, sino por deudas contraídas en juegos de azar, tarjetas de crédito, ingresos percibidos inferiores a las expectativas personales o del grupo social al que pertenece.

Uso excesivo de alcohol, drogas o cualquier adicción, lo cual requiere de recursos extra y también las personas adictas casi siempre poseen serios problemas emocionales.

Injusticias sufridas en el trabajo o resentimiento con los superiores.

Oportunidades

Control interno débil: «a río revuelto, ganancia de pescadores", es decir, cuando las personas están conscientes de que los actos ilícitos no se pueden detectar por medio de los controles establecidos. Facilidad para cometer el fraude por procedimientos de control débiles.

Nivel jerárquico que ocupa la persona en la entidad, así como la antigüedad de la persona en la institución, es decir, "abuso de autoridad".

Habilidad para razonar la forma, ocultar la evidencia. Facilidad de la persona para engañar inteligentemente a terceros.

Es evidente que existen riesgos hacia la información que en algunos casos se convierten en una dolorosa realidad. A manera de ejemplo se mencionan algunos riesgos:

Riesgos externos a la entidad:

- Naturales, como temblor, incendio, inundación o tormentas eléctricas.
- Humanos, como robo, sabotaje, motines sociales y fraude o delito informático.
- Materiales, como descompostura de equipo, fallas o interrupciones de energía eléctrica.

Una institución enfrenta riesgos naturales, humanos y materiales.

Riesgos internos a la entidad:

- Robo de material (el menor), de recursos o información (grave).
- Sabotaje.
- Destrucción, voluntaria o involuntaria de datos y/o recursos.
- Contaminación voluntaria o involuntaria de datos y/o recursos con los programas destructores como es el caso de los virus, caballos de Troya, bombas de tiempo, etc.
- Huelgas.
- Fraude o delito informático.

Ante el inminente riesgo se han tomado medidas y controles como son: el desarrollo de "programas fármacos", vacunas, detectores y antídotos. Así mismo se han desarrollado programas de seguridad que permiten restringir y delimitar el acceso de acuerdo al nivel jerárquico y funciones del personal. Vigilar el uso exclusivo de programas legalmente adquiridos es otro control de gran importancia.

Normas de auditoría generalmente aceptadas

Se puede definir a la auditoría como la evaluación independiente de alguna actividad con el objeto de emitir una opinión sobre su razonabilidad, así como la revisión y supervisión sistemática de una o varias actividades.

La auditoría no debe estar orientada a descubrir fraudes, sin embargo, el auditor debe estar consciente de que al practicar su examen podría encontrar alguno y que éste afectará su opinión. El auditor actual debe luchar en contra la imagen clásica del auditor como policía en una cacería de brujas, un buen auditor es colaborador de toda la organización que irradia actitud de servicio y compresión de las labores de otros, así como del gran valor que deben tener sus comentarios para el bien común.

La auditoría no debe estar orientada a descubrir fraudes, sin embargo, el auditor debe estar consciente de que al practicar su examen podría encontrar alguno y que éste afectará su opinión.

La auditoría de informática al igual que cualquier clase de auditoría debe garantizar razonablemente los resultados finales del trabajo efectuado. Por lo anterior las normas de auditoría generalmente aceptadas representan los requisitos mínimos de calidad relativos a:

- La persona del auditor o normas personales.
- La ejecución del trabajo.
- El informe que rinde.

Las normas sobre la persona del auditor o normas personales se componen de:

Entrenamiento técnico. Se refiere fundamentalmente al desarrollo de habilidades, no solo adquisición de conocimientos, y a la capacidad profesional para aplicar correctamente los conocimientos y elegir la mejor opción disponible. Resulta de gran valor pugnar e incrementar la sensibilidad y conocimiento de que los grupos de auditoría interna y externa aborden también las funciones de auditoría de informática. Ello necesita de incrementar la preparación y crear equipos de trabajo multidisciplinarios, armónicamente integrados, promover los conocimientos tanto en auditoría, como en computación, informática y telecomunicaciones, con el fin de fortalecer la integración entre todo el personal de auditoría y responder a lo que se espera del servicio.

Cuidado y diligencia profesional. Este es un tema delicado, pues la falta de experiencia en la materia informática en ocasiones ha hecho que el auditor en informática no analice e interprete la evidencia con el cuidado apropiado, considerando los controles compensatorios o alternos y se enfrente a aspectos altamente complejos, cuyos resultados no sean lo oportuno que demandan las soluciones.

Independencia mental, es decir, que no existan lazos jerárquicos o familiares entre auditores y auditados. Cabe mencionar que el lugar que ocupa la función de auditoría de informática en la estructura organizacional no siempre es el recomendable. En la mayoría de las instituciones del sector financiero acertadamente la auditoría de informática forma parte del área de auditoría interna, quien reporta a la dirección general, pero en los demás sectores normalmente, cuando existe, es parte del área de informática.

Las normas en la ejecución del trabajo se componen de:

Planeación y supervisión. Deben ejercerse en forma inversa a la experiencia y a la preparación del auditor. Para tal fin, se han desarrollado paquetes automatizados de auditoría que son una herramienta valiosísima que brinda importante apoyo a la planeación, ejecución y control del trabajo, aunque en la mayoría de los casos no son comerciales existen por ejemplo, paquetes para evaluación de riesgos y análisis histórico de los hallazgos.

Estudio y evaluación del control interno. Se refiere al plan de organización, los métodos y procedimientos y el ambiente de control, siendo trascendente la revisión de los controles en informática y no solo los existentes alrededor de ella. Este tema se verá detalladamente en otra sección de este módulo.

Obtención de evidencia suficiente y competente. Se refiere a los papeles de trabajo que representan varias cosas: el soporte de opinión, la evidencia de supervisión y son antecedente para futuras auditorías. Las pistas de auditoría son todos aquellos elementos que permiten reconstruir los hechos, los cuales no solo son de importancia para el auditor, sino para todos los interesados en aclarar un hecho o situación. Las pistas de auditoría, en presencia del proceso electrónico de datos, no siempre se encuentran en papel y cada vez es más frecuente esta ausencia, por tanto, el auditor requiere accesar información en medios magnéticos u ópticos (discos flexibles, discos duros, cintas, etc.) para obtener evidencia suficiente y competente para rendir su opinión con elementos de juicio objetivos.

Las normas relativas al informe de auditoría (dictamen u opinión) se componen de:

El informe de auditoría externa (principalmente el de estados financieros) está ampliamente normado, sin embargo, en cuanto al informe de auditoría interna es más libre, conformado y estandarizado por cada institución. Ahora bien, es importante considerar los siguientes aspectos como parte del contenido del informe: se debe expresar claramente la responsabilidad asumida por el auditor, fundamentalmente sobre su opinión y la adherencia a la normatividad vigente; en los casos en que conviene informar con mayor detalle mayor, las declaraciones informativas deben suficientes para que el lector comprenda dichos asuntos.

Tipos de dictámenes:

Opinión limpia:	Cuando el control interno es en general bueno.
Opinión negativa:	Cuando el control interno es en general deficiente.
Opinión con salvedades:	Cuando el control interno es en general bueno, pero existen excepciones de importancia.
Abstención de opinión:	Cuando no se tienen elementos, evidencia suficiente y competente, para opinar sobre el control interno.

Continuando con el informe que rinde el auditor de informática, es común que éste no siempre se encuentre suficientemente organizado, completo y que tampoco aclare las situaciones relevantes. A veces está lleno de tecnicismos que no siempre son comprendidos por los que lo reciben y deben tomar decisiones en cuanto a las debilidades de control. Cabe recordar que una carta de observaciones o sugerencias es una comunicación formal dirigida a la alta administración con el objeto de llamar su atención sobre las debilidades de control más significativas, procurando motivarla para que se incorporen las medidas de control que procedan. La carta de observaciones o sugerencias es el producto final del trabajo de auditoría, por lo que es importante darle la calidad que requiere. Una buena carta evidencia un buen trabajo de auditoría.

Control interno

El control interno comprende el plan de organización, los métodos y procedimientos y el ambiente de control.

El control interno comprende el plan de organización, los métodos y procedimientos y el ambiente de control que en forma coordinada se adoptan en un negocio con los siguientes objetivos:

- La protección de los activos de la institución principalmente para la prevención y detección de fraudes. ¿En informática qué activos deberían protegerse?
- La obtención de información veraz y confiable que permita la localización de errores.
- La promoción de eficiencia en la operación de la institución facilitando la localización de desperdicios.
- Esta situación es preocupante porque frecuentemente, tanto el personal de informática como los usuarios, conocen la tecnología incorporada a sus

organizaciones de manera muy rápida y no siempre mediante una capacitación formal y adecuada.

- La adhesión a las políticas establecidas por la administración de la institución. La preocupación que existe a este respecto se debe a los deficientes medios de comunicación establecidos por las instituciones.

Una debilidad de control significa una situación en la que el auditor estima que los procedimientos establecidos, o el grado de cumplimiento de ellos, no suministran una razonable seguridad y pueden traer como consecuencia errores o irregularidades.

Las condiciones para el control, como su nombre lo indica, son esenciales para hacerlo posible. Algunas condiciones básicas son: la existencia de sistemas, personal competente para operarlos y documentación en que consten las operaciones y lo que se hace con ellas. A continuación se detallan cada una de estas tres condiciones básicas:

Existencia de sistemas: mientras más explícitamente se defina una operación, más fácil será llevarla a cabo en forma confiable y controlada. Idealmente, todo el personal que intervenga en una operación debería saber exactamente lo que debe hacer y lo que no debe hacer en cualquier caso, incluso ante operaciones anormales, no autorizadas, incompletas o erróneas. Sin sistema, el control es imposible, en consecuencia, el sistema mismo es probablemente el control fundamental.

El sistema mismo es probablemente el control fundamental.

Competencia e integridad: los sistemas y los otros procedimientos de control serán inútiles si el personal asignado para ejercerlos no lo hace consciente y consistentemente. En efecto, cada persona debe tener el nivel de competencia adecuado para la labor que se le asigna, y suficiente integridad para sentirse responsable de su realización. Los sistemas y la competencia de quienes los operan van de la mano. El auditor debe estar siempre alerta a los cambios de personal en la institución o a los cambios sutiles en su actitud que pudieran requerir una revalidación.

Documentación: algunos documentos o registros se requieren sólo para efectos de control, se evidencia la ejecución de una operación inicializando el documento, o por algún otro medio que identifique a quien la llevo a cabo para definir responsabilidades y permitir su supervisión. El proceso de documentar las operaciones es inherente y está también implícito en todo sistema.

El proceso de documentar las operaciones es inherente y está también implícito en todo sistema.

Para que el auditor pueda emitir su opinión en forma objetiva y profesional, tiene la obligación de reunir los elementos de juicio suficientes que permitan obtener con certeza razonable, la convicción de: la autenticidad de los hechos y

la consistencia de los criterios, sistemas y métodos usados para captar y reflejar los hechos. A los elementos de juicio antes mencionados se les denomina evidencia comprobatoria y deberá ser suficiente y competente.

Los papeles de trabajo obtenidos en cada auditoría, son propiedad exclusiva del auditor y la información contenida en ellos es de carácter confidencial, su uso está restringido por el secreto profesional. El auditor debe usar un maletín o portafolio que pueda cerrarse con llave y guardarlo en su área de trabajo en un lugar seguro. Puesto que los papeles de trabajo del auditor constituyen la evidencia comprobatoria, lo pueden favorecer o perjudicar posteriormente si surgen problemas. Es lamentable que se haya adoptado la expresión "papeles de trabajo" pues da la idea de un producto no terminado, o sea la acumulación de notas y cálculos preliminares en un block de apuntes. Si no queda evidencia del cuidado con que el auditor hizo su trabajo, parecerá que solo le prestó atención superficial. El auditor debe tener presente que no será el único que leerá los papeles de trabajo que formula y considerar la impresión que causara a otras personas. En suma, los papeles de trabajo debidamente elaborados son necesarios para que el auditor demuestre que cumplió con las normas de ejecución del mismo.

Al evaluar el control interno, el auditor deberá determinar sus deficiencias, calificarlas en cuanto a su gravedad y posibles repercusiones, y establecer el alcance de su trabajo en relación a las condiciones encontradas. Si las fallas de control interno son graves y el auditor no logra suplir esa limitación de una manera práctica, deberá abstenerse de opinar.

Al evaluar el control interno, el auditor deberá determinar sus deficiencias, calificarlas en cuanto a su gravedad y posibles repercusiones, y establecer el alcance de su trabajo en relación a las condiciones encontradas.

La auditoría debe cambiar de la simple detección de errores y/o irregularidades a la promoción de la adecuada **administración del riesgo**, un adecuado estudio y evaluación del control interno existente es la base para la determinación del alcance de las pruebas y procedimientos de auditoría.

Factores que determinan la necesidad de auditoria de informática

Todas las organizaciones, empresas e instituciones del mundo moderno tienen ante sus ojos un panorama de riesgos que tan solo hace algunos años no hubieran soñado tener, así como un amplio panorama de oportunidades y fortalezas que la tecnología genera.

Ahora se puede apreciar la enorme penetración y sofisticación de la computación, que ha invadido desde el hogar hasta las organizaciones que administran los sistemas de transferencia electrónica de fondos en el mundo o los cajeros automáticos de las instituciones bancarias de cualquier país. Desde la infancia, con juegos y programas de cómputo educativos, hasta la edad adulta,

como individuos o instituciones, vivimos cada vez más inmersos en la automatización y las telecomunicaciones. No solo vivimos una vertiginosa época de cambios sino un cambio de época, cuya velocidad de transformación de la información y cercanía de la tecnología al usuario final supera las expectativas de muchos.

Las organizaciones de hoy incrementan continuamente su dependencia operativa de las funciones de informática. Una de las razones de esta dependencia es la necesidad del procesamiento de altos y muy dinámicos volúmenes de datos. La información más relevante, financiera, fiscal y administrativa, es fruto del proceso electrónico de datos y de las comunicaciones, en ocasiones casi instantáneas. Se resume con facilidad que la informática y la computación son muy importantes para las entidades y las personas de finales del siglo xx. ¿Qué sucedería si fallara o desapareciera la informática en nuestras instituciones? ¿Qué pasaría con la información estadística de cualquier país?

Un aspecto que llama la atención es que el costo de la informática no siempre esta en proporción aceptable a los beneficios obtenidos. En muchas instituciones se ha padecido el incumplimiento de expectativas o bien fracasos. Derivado de ello aparece como motivo de preocupación de la alta gerencia el que las áreas de informática funcionen adecuadamente, con un nivel de riesgo y aprovechamiento de recursos razonable. Sin embargo, todavía no existe un autentico compromiso de la alta gerencia en asuntos de informática, aunque actualmente esto, en términos generales, guarde menores proporciones que en el pasado.

Otro fenómeno interesante es lo que se ha llamado la era de las microcomputadoras en que vivimos: ya sea para su uso independiente o en red, los enormes e impenetrables centros de cómputo tradicionales tienden cada vez más a desaparecer. Hoy día la informática se encuentra en casi todas las áreas de una entidad y los usuarios satisfacen autónomamente muchas de sus necesidades gracias al uso de los lenguajes de cuarta generación y los generadores de aplicaciones, herramientas que al ser adecuadmente utilizadas, permiten minimizar el problema de los costos de la informática.

En esto nuevo entorno informático, se hace extremadamente urgente incrementar la conciencia, la sensibilización, el compromiso y el apoyo de la alta gerencia así como la precisa determinación de su importante papel en el logro del éxito de la función de informática.

En el desarrollo de sistemas de información pueden surgir factores que determinen la necesidad de una auditoría.

Otra situación que es fundamental considerar es el proceso para el desarrollo de los sistemas de información (SI), pues en él surgen muchos puntos críticos y por ende, múltiples factores que determinan la necesidad de auditoría de informática, algunas características recurrentes son:

- **Tiempos récord o maratones para el desarrollo de SI:** a partir de un conocimiento muy vago de los requerimientos de información o necesidades de los usuarios.

- **Carencia o deficiencia en la metodología** para el desarrollo de los sistemas. En los casos en que existe una metodología correcta no es estándar o solo lo es parcialmente. Es decir, que el proceso de desarrollo depende frecuentemente del personal que participe en él, sin el establecimiento de puntos de control mínimos que permitan medir el grado de avance y calidad de los sistemas antes de ser transferidos a un ambiente de operación normal.

- **Falta de participación del auditor**, por el impreciso conocimiento de su papel en esta área. En ocasiones el auditor teme a problemas de independencia mental y/o conocimientos suficientes y competentes.

- **Sistemas aislados o islas de información**, es decir, que la información generada como salida de un sistema no se transfiere automáticamente a los otros sistemas relacionados y es necesario volver a capturar. Tal pudiera ser el caso de que la información final de nómina sea necesario introducirla a contabilidad mediante la nueva captura de un buen número de los mismos datos. Un punto a resaltar es que en sistemas las interfaces equivalen a las tuberías de una casa.

- **La integridad de los datos** es otro factor determinante, ya que no siempre los controles que se encuentran incorporados en los sistemas de información aseguran razonablemente la totalidad, la exactitud, la autorización, la permanencia, la oportunidad y la utilidad de la información resultante. Estos controles pueden ser ejercidos por los seres humanos o automáticamente por programas de cómputo, utilizando un conjunto de técnicas apropiadas a los sistemas en los que interviene el procesamiento electrónico de datos.

- **Enorme concentración de funciones** tradicionalmente segregadas para efectos de control. Muchas veces, el analista, el diseñador, el desarrollador, el operador y usuario del sistema es la misma persona, esto trae como consecuencia una alta posibilidad de manipular la información.

- **El aprendizaje por descubrimiento**, es decir, artesanal, empírico, autodidacta, muchas veces sin una clara conciencia de riesgos, responsabilidad y control, como es la documentación y respaldos, con el consecuente despilfarro de tiempo y eficiencia en el uso de los recursos tecnológicos. En este renglón es conveniente destacar que el surgimiento de las carreras universitarias en las áreas de informática, computación, cibernética, ingeniería electrónica, etc. es relativamente reciente y, por tanto, los recursos humanos altamente calificados son todavía muy escasos y la necesidad de ellos cada vez más frecuente.

- **La "Torre de Babel",** en donde trabajan equipos y paquetes de programas de cómputo de diferentes proveedores o bien versiones incompatibles y sin una adecuada evaluación de los mismos.

- **Esfuerzos aislados**, no institucionales ni articulados, para el logro armónico de objetivos de cada una de las áreas de la entidad.

Como respuesta a todas las inquietudes expresadas en los párrafos anteriores, surge la auditoría de informática como un recurso para prever, detectar y corregir las deficiencias, pero es necesario que toda la organización esté convencida de la necesidad de incorporarla. En especial la alta gerencia deberá verificar que se estén cumpliendo satisfactoriamente y de acuerdo a la normatividad los objetivos de:

- continuidad del servicio.
- integridad, coherencia, confidencialidad y seguridad de la información.

La auditoría de informática tiene como propósito evaluar la suficiencia de las medidas de control para disminuir la posibilidad de que los riesgos se materialicen, al mismo tiempo, ha ampliado los horizontes de actuación en materia de auditoría, ofreciendo la gran oportunidad de brindar una gama de servicios de alto juicio profesional y muy demandados por la sociedad. Se puede apreciar que los objetivos que siempre se han buscado en la auditoría no se han modificado, pero el entorno tecnológico ha revolucionado los medios para garantizarlos.

La auditoría de informática tiene como propósito evaluar la suficiencia de las medidas de control para disminuir la posibilidad de que los riesgos se materialicen.

El auditor de informática evalúa la suficiencia de las medidas de control adoptadas para abatir la posibilidad de que los riesgos se materialicen, al igual que cualquier auditor, debe estar familiarizado con la organización y funciones de cada una de las áreas de la institución, así como con las operaciones que se realizan ya que existen dos grandes áreas de participación de la auditoría de informática:

- **Controles específicos** también llamados controles de aplicación, que abarcan:
  - La auditoría al ciclo de vida del desarrollo de un sistema de información.
  - La auditoría de sistemas de información en operación.

- **Controles generales**, que abarcan la auditoría a todos aquellos aspectos cuyas debilidades no afectan a una información especifica, sino en general a cualquier recurso informático:
  - La administración de la función informática.
  - Revisión de controles en adquisiciones de bienes informáticos.
  - La seguridad física y lógica.
  - Sistema operativo.

Biblografía

Coopers & Lybrand (1986), *Handbook of EDP Auditing*, Nueva York.

Echenique José Antonio (1995), *Auditoria en Informática*, Editorial Mc. Graw Hill, México.

Hernández Jiménez Ricardo (1991), *Administración de Centros de Cómputo*, Editorial Trillas. México.

Vallabhaneni. S. RAO, *Information Systems Audit Process*, EDP Auditors Foundation, Inc.

Weber Ron (1986), *EDP Auditing - Conceptual Foundations and Practice*, Editorial Mc.Graw-Hill Book Company, Nueva York.

Tema 2. Auditoría a sistemas en desarrollo

Por Sara Isabel Ayala Rodiles

Resumen

Este tema se refiere a la auditoría que se aplica a los sistemas de información que están en procesos de construcción. Cabe destacar que cada una de las fases establecidas en el ciclo de vida clásico es susceptible de ser auditada y, no obstante que en el módulo anterior se estudiaron otros paradigmas de desarrollo de sistemas, el ciclo de vida clásico es una metodología que se toma como base para establecer la auditoría a sistemas de información en desarrollo.

Las etapas de planeación, análisis y diseño, constituyen momentos claves para la participación del auditor, con el fin de evaluar las medidas de control que permitan disminuir costos y riesgos en etapas posteriores como es la implantación o el mantenimiento del sistema.

Tema 2. Auditoría a sistemas en desarrollo

Por Sara Isabel Ayala Rodiles

Auditoría al ciclo de vida de desarrollo

La experiencia de la mayoría de las empresas indica que los resultados obtenidos del proceso de desarrollo de los sistemas de información son deficientes. Muchos de esos problemas se convierten en sujetos de auditoría y se pueden señalar los siguientes:

- Costos en una proporción inadecuada a los beneficios.
- Incremento en la escala inicial del proyecto.
- Sistemas no integrales o aislados.
- Deficiente comunicación entre usuarios y personal de procesamiento de datos.
- Desconocimiento del papel / responsabilidad de usuarios y dirección.
- Expectativas no cumplidas, insatisfechas, de los usuarios.
- Ausencia de pistas de auditoría.
- Falta de revisiones técnicas a detalle.
- Entrenamiento deficiente.
- Carencia o incompleta documentación de sistemas. Documentación técnica, de operación y/o de usuario.
- Carencia de metodología, o bien metodología incompleta y no estándar, para el desarrollo de los sistemas, en la que se señalen con precisión actividades, tiempo estimado y responsables. Administración insuficiente de los proyectos.
- Inoportunidad en la transferencia de sistemas en desarrollo a operación normal.
- Desaprovechamiento tecnológico.
- Pruebas del sistema incompletas, inadecuadas, desorganizadas, sin documentar y/o mal diseñadas, las cuales garanticen que los errores e irregularidades se detectan oportunamente por sistema.
- Pruebas no siempre controladas por usuario.

Es importante destacar lo vital que resulta el hecho de que el auditor esté involucrado desde el plan maestro de sistemas, pues para auditar el ciclo de vida del desarrollo de sistemas se deben tener presentes los siguientes tres puntos:

- Que exista una metodología.
- Que la metodología sea la adecuada al entorno tecnológico de la entidad, sea estándar, completa, al día, aprobada y comunicada a todo el personal.
- Que la metodología se cumpla en el caso de un sistema de información, en particular o en general.

El auditor no siempre ha participado en el ciclo de vida del desarrollo de los sistemas pues teme "ser juez y parte", pero es conveniente que el auditor esté consciente de que él no representa un factor para la toma decisiones, sino que juega un papel de control que contribuye a disminuir riesgos, no a evitarlos.

El auditor contribuye a disminuir riesgos, no a evitarlos.

La mayoría de las organizaciones destinan enormes recursos al desarrollo de nuevos sistemas o a la modificación de los mismos. A la luz del incremento en el porcentaje de fallas en las fechas de terminación, costos estimados y la satisfacción del usuario, las organizaciones pueden seguir un enfoque estructurado para el desarrollo de nuevos sistemas y el mantenimiento de los mismos. La combinación de técnicas efectivas de administración del proyecto, la participación activa del usuario y especialistas, y la utilización de una metodología estructurada para el desarrollo de sistemas pueden minimizar los riesgos en cuanto a aplicaciones inapropiadas, erróneas, con datos sin uso o bien a los cambios injustificados: el gran salto hacia adelante se logra con pequeños saltos.

Los sistemas de información se deben desarrollar para servir al usuario, proporcionándole capacidades para el proceso de datos y reportes. Cada sistema de información tiene cinco principales áreas o fases, mismas que se componen de otras actividades. Todas son sujetas a control durante el ciclo de vida del desarrollo de sistemas:

A) Planeación
Requisición de servicios.
Estudio de factibilidad.

B) Análisis y diseño
Análisis y diseño general del sistema.
Análisis y diseño detallado del sistema.

C) Desarrollo
Programación.
Prueba modular y prueba del sistema integral.
Desarrollo de manuales.
Entrenamiento.

D) Implantación
Conversión.
Revisión de la post-implantacion.

E) Mantenimiento del sistema

Reconocer que hay un ciclo de vida para el desarrollo de sistemas es el primer paso para su control. El hecho de dividir el desarrollo en fases permite predecir el proyecto íntegro, analizar y evaluar cada parte con mayor concentración y *monitorear* continuamente la calidad y avance del trabajo.

Reconocer que hay un ciclo de vida para el desarrollo de sistemas es el primer paso para su control.

La revisión del ciclo de vida del desarrollo de sistemas parte de los estándares o metodología requerida para el desarrollo de los nuevos sistemas y las modificaciones a los mismos. El propósito de la revisión efectuada por el auditor de sistemas de información es asegurar que la organización tiene y usa la metodología adecuada de desarrollo.

El objetivo de auditoría al ciclo de vida de desarrollo de sistemas es verificar que se desarrollen sistemas útiles, seguros, auditables, mantenibles y controlables y que se obtengan resultados consistentes para satisfacer los requerimientos del usuario.

Planeación

Actividad: Requisición de Servicios

Es importante que los sistemas de información se soliciten por los usuarios, que son los que deben estar conscientes de las necesidades. Asimismo, es necesario que los sistemas de información sean solicitados por escrito y de manera oficial, para precisar los compromisos en cuanto a:

Definición del proyecto:

- Justificación. ¿Por qué se requiere un nuevo sistema?
- Ambiente. ¿Quiénes y en dónde operará?
- Alcance. ¿Qué aspectos deberá cubrir a corto, mediano y largo plazo?
- Restricciones que tienen las áreas usuarias.
- Beneficios esperados: ahorro de tiempo, de papel, de personal, mejoramiento de la imagen de la institución, etc.

- Integración del equipo de trabajo asignado por el área usuaria al proyecto y sus responsabilidades.

- Definición de requisitos de información, nuevos y existentes.

Esta solicitud del desarrollo de un nuevo sistema de información debe ser presentada, de preferencia, al Comité de Planeación y Control de Recursos Informáticos, el cual deberá estar integrado por cuando menos un representante de cada una de las áreas de la institución. Este comité debiera ser quien autorice o rechace la solicitud.

Actividad: Estudio de factibilidad

Los estudios de factibilidad se deben realizar para garantizar, de manera razonable, que es posible desarrollar el sistema solicitado considerando los aspectos económicos, técnicos y operativos disponibles. Estos estudios debieran incluir:

- Estudio de los procedimientos existentes.

- Formulación de cursos alternativos de acción.

- Factibilidad tecnológica (métodos aplicables de procesamiento de datos) disponibilidad de la tecnología que satisfaga las necesidades del usuario.

- Actualización o complemento a los recursos actuales.

- Factibilidad económica:

    - Costos actuales contra costos de cada alternativa (personal de desarrollo, equipo *software,* entrenamiento, preparación de la entrada, conversión de archivos de prueba, operación, costo del *software,* etc.).
    - Identificación y cuantificación de beneficios.

- Factibilidad operativa: determinar que se operará tomando en cuenta factores como la resistencia al cambio, características del personal, ubicación de las instalaciones, etc.

- Plan maestro del proyecto (puntos de control y calendarización de actividades).

- Estado general de la función de desarrollo en la institución.

Estos estudios para el desarrollo de un nuevo sistema de información también

deben ser presentados, preferentemente, al Comité de Planeación y Control de Recursos Informáticos. Este comité debiera ser quien autorice las siguientes actividades para el desarrollo del sistema o lo detenga a tiempo.

Análisis y Diseño

Actividad: Diseño general del sistema

El diseño general de sistemas equivale a los planos para la construcción de una casa, siempre será más fácil y menos costoso corregir los planos que hacerlo ya que la casa ha sido construida. El diseño general debiera incluir:

- Estructura general del sistema.
- Definición y documentación de los requisitos de salida:
  - Contenido y formato de los informes.
  - Frecuencia de producción de reportes.
  - Lista de distribución de reportes autorizada.
  - Periodos de retención de informes.
  - Controles sobre la salida.
- Definición y documentación de los requisitos de entrada:
  - Requisitos de edición y validación (control).
  - Revisiones de seguridad para la protección de la exclusividad.
  - Controles sobre la entrada.
- Definición y documentación de los requisitos de archivos:
  - Definición de los tipos de registros o estructuración de bases de datos.
  - Métodos de organización de archivos.
  - Niveles de seguridad y controles de acceso.
  - Periodos de respaldo y retención.
- Definición y documentación de los requisitos de procesamiento (manuales y computarizados):
  - Especificación de procedimientos programados de cálculo, clasificación, etc.
  - Estimación de tiempos de respuesta.
  - Normatividad.
  - Interfaces con otros sistemas de información.
  - Niveles de seguridad.
  - Diseño de documentos fuente.

En el diseño general del sistema se deben considerar los períodos de retención de informes.

En esta parte se determinan las especificaciones de usuario, es decir, usuario es todo aquel que dentro del contexto de la organización se relaciona con el sistema. Existen usuarios primarios y usuarios secundarios.

Usuario es todo aquel que dentro del contexto de la organización se relaciona con el sistema. Existen usuarios primarios y usuarios secundarios.

> **Usuario Primario**, es aquel que usa directamente en sus tareas los resultados del sistema de información.
>
> **Usuario Secundario**, es aquel que introduce datos al sistema.

El analista de sistemas debe comprender las responsabilidades, limitaciones, necesidades del usuario, las acciones que deberá tomar el usuario, las reglas de decisión por aplicarse y los itinerarios de interacciones. Las especificaciones de usuario involucran el diagnóstico del problema y las especificaciones de solución. Estas tienen la fuerza de un contrato o compromiso entre el usuario y el personal de procesamiento de datos. Son los antecedentes para todo el equipo de desarrollo. Deben responder a las preguntas ¿cómo? ¿por qué? por tanto, se deberán quedar diagramados los procedimientos actuales y los esperados.

Como se analizó en el primer módulo del Diplomado, las decisiones que tienen que tomar los usuarios de un sistema de información se pueden darse en diferentes niveles de la organización, aquí señalaremos los tres principales:

Nivel operativo de la administración. Apoyan sus decisiones en reglas preestablecidas, operan en nivel de alta certidumbre y, fundamentalmente, consiste en la supervisión de detalles operativos.

Nivel medio de administración. Toman decisiones sobre planeación y control a corto plazo, trabajan en un ambiente de baja certidumbre y las decisiones carecen de alto grado de estructuración.

Nivel de administración estratégica.- Guían al nivel medio y operativo de administración, actúan en un clima de incertidumbre, postulan metas, estrategias y políticas.

La siguiente tabla muestra las diferentes características que asume la información dependiendo del nivel de decisiones dentro de la organización:

Nivel de dirección estratégica	Características en cuanto a:	Nivel de control operativo
Amplia	Visión de la información	Estrecha
General	Nivel de detalle	Muy detallada
Resumido	Nivel de resumen	Datos primarios
Antigua	Antigüedad de la información	Reciente
Estimaciones	Precisión de la información	Actual
Cualitativa	Fuente	Principalmente interna

Otro factor importante por considerar son las relaciones humanas, ya que los sistemas de información pueden cambiar las relaciones interpersonales y las interacciones. Se debe comprender el estilo organizacional, tomar a la organización como un todo, identificar el grado de apertura / restricción: permeabilidad. Es necesario identificar si el estilo de liderazgo es autócrata o demócrata.

La recopilación de datos involucra la investigación documental, la realización de entrevistas y la observación. ¿Qué se examinará?, ¿A quiénes se entrevistará?

El diseño de los formatos/ pantallas de captura tiene también ciertos objetivos que cumplir:

- Precisión.
- Facilidad de uso y sencillez.
- Consistencia.
- Controlables (flujo de operación).

Otros aspectos que debe observar el diseño son:

- Satisfacción del objetivo planteado.
- Adaptada al usuario.
- Adecuada cantidad de información.
- Oportunidad.
- Medio apropiado.
- Medición del grado de confidencialidad (por ejemplo, muy confidencial, confidencial y no confidencial).

Es mucho menos costoso corregir problemas cuando éstos se encuentran en sus etapas iniciales, que esperar a que se expresen mediante quejas de usuarios o aparición de crisis.

Es mucho menos costoso corregir problemas cuando éstos se encuentran en sus etapas iniciales, que esperar a que se expresen mediante quejas de usuarios o aparición de crisis.

El diseño general del sistema debe ser elaborado conjuntamente por el personal de informática y el personal usuario, pero siempre debe ser aprobado por el usuario antes de continuar con las actividades de la siguiente etapa.

Actividad: Diseño detallado del sistema

En esta etapa deben realizarse las siguientes tareas:

- Especificaciones de programas y controles programados (costo-beneficio).
- Diseño de pistas de auditoría.
- Definición de estándares de documentación de programas de cómputo:
  - Nombre de la aplicación.
  - Diagrama del sistema (menú jerárquico).
  - Aspectos generales del programa.
  - Formatos de archivos de entrada.
  - Formatos de archivos de salida.
  - Diseño y muestra de reportes.
  - Diseño y muestra de pantallas.
  - Descripción detallada de los principales.
  - Procedimientos de cálculo, clasificación etc., incorporados al programa.
  - Criterios de selección.
  - Procedimiento de conexión de cifras.
  - Instrucciones de corrida y listado de procedimientos de ejecución.
  - Medio de almacenamiento y localización del programa.
  - Requerimientos de equipo.
  - Listado del programa fuente (última compilación, con comentarios a la lógica).
- Definición de estándares para la prueba de programas y del sistema total.
- Determinación del procedimiento para establecer datos de prueba.
- Asignación de responsabilidades para la preparación de datos y evaluación de los resultados.
- Autorización y aceptación escrita del líder del proyecto en el área de informática.

En esta etapa se definen las especificaciones técnicas, que son las características y definiciones técnicas y operativas del sistema, lo cual es responsabilidad del líder de proyecto en informática. Las especificaciones técnicas incluyen:

- Instrucciones para programación.
- Itinerario para el desarrollo de programas/módulos.
- Matrices de archivos/programas, módulos/programas.
- Selección de los lenguajes de programación.
- Controles del operador.
- Instrucciones al operador en caso de interrupciones.
- Procedimientos de respaldo, reinicio y recuperación.

Esta etapa es responsabilidad del personal de informática, analistas y programadores que laboran en el desarrollo de los sistemas de información en la Institución.

Desarrollo

Actividad: Programación

Hasta esta etapa se debe efectuar el desarrollo de los programas de cómputo y la elaboración de la documentación técnica de los mismos. No debe dejarse al final el desarrollo de los manuales técnicos.

Actividad: Prueba modular y prueba del sistema integral

Se deben ejercer presiones para hacer fallar al sistema. Las pruebas deben efectuarse con volúmenes de datos y bajo condiciones reales de operación. Cualquier error detectado debe ser cuidadosamente analizado y corregido, preparándose un reporte de excepciones: problema, causa y solución, indicando la fecha de corrección. La prueba debe estar bien dirigida, organizada, ser exhaustiva y eficiente, involucrando:

- Los procedimientos manuales.
- Los programas de cómputo y procedimientos de ejecución.
- Archivos de prueba.
- Al personal.

Es importante que se documenten las pruebas y se muestre en ellas la aprobación definitiva del usuario. Los reportes aprobados deben conservarse como evidencia de la realización adecuada y completa de esta etapa.

En el caso de proyectos grandes conviene desarrollar un plan de instalación piloto o por módulos, asignando responsabilidades. Se pueden disminuir las sorpresas negativas si se planea, conjuntamente usuarios y personal de informática, los requerimientos técnicos (de equipo y personal) y la fecha más conveniente para la implantación del sistema.

Actividad: Desarrollo de manuales

La documentación de los sistemas, es decir, la elaboración de manuales, es de vital importancia para la operación y uso del sistema por los usuarios y el personal de informática involucrados, así como para efectuar con rapidez y con el menor grado de riesgo las futuras modificaciones del sistema. Debemos considerar que las personas y los sistemas no son eternos.

A continuación se indican los principales puntos que deben incluir los manuales:

Manual de operación :

- Representación gráfica de la estructura del sistema.
- Función de cada programa.
- Requerimientos de equipo.
- Tamaño estimado de archivos (normal y máximo).
- Explicación de los mensajes de la consola o pantalla, junto con la respuesta adecuada del operador.
- Instrucciones de corrida y listado de procedimientos de ejecución.
- Calendarización de procesos.
- Parámetros a alimentar.
- Creación de salida y su distribución .
- Identificación adecuada de las etiquetas de los archivos de salida.
- Puntos de reinicio y recuperación.
- Procedimientos para notificar errores o condiciones defectuosas.
- Procedimientos para casos de emergencia.

El manual de operación debe estimar el tamaño de los archivos.

Manual de usuario:

- Representación gráfica de la estructura del sistema.
- Procedimientos de preparación de datos.
- Asignación de prioridades.
- Tiempo probable de respuesta y recepción de productos finales.
- Especificaciones y diseño de entrada de datos (formatos y pantallas de captura).
- Especificaciones y diseño de salida de datos (reportes / pantallas de consulta).

- Controles de usuario.
- Procedimientos para resolver errores e incongruencias.
- Controles sobre la entrada y salida.

Manual del sistema:

- Representación gráfica de la estructura del sistema.
- Documentación de cada programa de cómputo.

La revisión de la documentación de una aplicación involucra identificar su existencia, analizar su contenido y, juzgar su oportunidad y disponibilidad (por ejemplo, en medios magnéticos u ópticos y en red, de preferencia no en papel). La calidad del mantenimiento de sistemas depende en gran medida de la calidad de la documentación. Además de la claridad y organización de la documentación, debe dedicarse especial atención al tipo de personas a quien va dirigido.

La calidad del mantenimiento de sistemas depende en gran medida de la calidad de la documentación.

Actividad: Entrenamiento

El entrenamiento del personal es un control preventivo, es decir, que ve antes de que se presenten las dudas, errores y/o irregularidades. Por tanto, es de suma importancia que se realice con alto grado de calidad. Algunos aspectos a revisar son:

- Calendarización que garantice que todo el personal que lo requiere asiste.
- Duración.
- Porcentaje de teoría y de práctica.
- Materiales de apoyo para los participantes y para el expositor.
- Métodos de la enseñanza.
- Calidad de los instructores.
- Mecanismos para evaluación del aprendizaje.

Implantación

Actividad: Conversión

La etapa de conversión significa abandonar el sistema actual, manual o computarizado, para emigrar a uno nuevo y conciliar los resultados. Los controles en la etapa de conversión persiguen asegurar que los archivos iniciales

(saldos, acumulados, catálogos, etc.) proporcionan un punto de arranque adecuado, marcando itinerarios, compromisos y condiciones de éxito.

Los controles en la etapa de conversión persiguen asegurar que los archivos iniciales (saldos, acumulados, catálogos, etc.) proporcionan un punto de arranque adecuado, marcando itinerarios, compromisos y condiciones de éxito.

Cuando se emigra a nuevo sistema se transfieren, mediante programas de cómputo para la conversión de algunos datos que se han almacenado en archivos generados por el sistema anterior. Por ejemplo, si durante el primer semestre de 1999 se procesó la información con sistema de nómina y a partir de julio se instalará un nuevo sistema de nómina, se debe aprovechar al máximo la información almacenada por el sistema anterior y garantizar que este paso se lleve a cabo satisfactoriamente.

Normalmente la conversión requiere el desarrollo de programas de conversión de archivos para pasar un formato a otro.

Las principales actividades que se realizan en la etapa de conversión de archivos o bases de datos son:

- **Identificación de fuentes de información.**
- **Recopilación de información.**
- **Revisión de la exactitud de los documentos previos a la conversión.**
- **Evaluación de los resultados de la conversión.**

Actividad: Revisión de la post-implantación

La revisión post-implantación es una etapa formalmente planeada, que debe realizarse después de transcurridos tres o seis meses de la instalación definitiva. La revisión post-implantación normalmente involucra:

- Evaluación del cumplimiento de las necesidades de usuario.
- Análisis de costo-beneficio del sistema.
- Oportunidad de la información.
- Efectividad de los controles.
- Control de modificaciones al sistema.

Mantenimiento del sistema

"El primer cambio surge el día que se instala el sistema". Debido a que lo único constante en sistemas es el cambio, en esta etapa se analiza y evalúa cómo

ha sido el mantenimiento de sistemas para proteger a la instalación de cambios incorrectos, no autorizados o decisiones equivocadas. El mantenimiento de sistemas se origina principalmente por la presencia los siguientes factores:

- Cambios en normatividad interna y externa a la entidad.
- Desarrollo tecnológico.
- Comportamiento del entorno, competencia.
- Costos actuales excesivos

Normalmente los cambios obligatorios (cambios en normatividad interna y externa a la entidad) se efectúan con menos controles, por la presión implícita, mientras que los cambios por mejoras (refinamiento, creatividad, ventajas tecnológicas) se atienden mas controladamente, pues se dispone de mayor cantidad de tiempo para realizarlos.

Al auditor le preocupa que haya un sistema para administrar los cambios a los sistemas, por ejemplo, hacer los cambios por grupos o lotes pertenecientes a un mismo modulo / programa. La documentación para el control de los cambios debiera mostrar:

- Control numérico.
- Fecha de implantación.
- Persona solicitante autorizada.
- Persona que efectúo el cambio.
- Justificación.
- Descripción narrativa.
- Documentación de las pruebas.
- Autorización formal de los resultados.

Todo cambio debiera originar la actualización de la documentación correspondiente (manuales técnicos, de usuario y de operación). Algunas instituciones incluyen la documentación técnica de los cambios dentro de los propios programas de cómputo que se modifican, como comentarios.

La conciencia de la calidad, seguridad y control debe iniciarse en las áreas de desarrollo,contemplando un balance adecuado con la productividad de los sistemas.

La detección y corrección de controles inadecuados o incompletos durante la fase de diseño ahorrará tiempo y dinero cuando el sistema esté operando cotidianamente.

La detección y corrección de controles inadecuados o incompletos durante la fase de diseño ahorrará tiempo y dinero cuando el sistema esté operando cotidianamente.

Bibliografía

Benjamin Y. Robert (1986), *Control del ciclo del desarrollo de sistemas de información,* Editorial Limusa México.

Burch John G. y Gary Grundnitski (1996), *Diseño de sistemas de información,* Editorial Megabyte, México.

Dicjmann Roberta (1986), *Selección y manejo de personal para procesamiento de datos,* Editorial Limusa, México.

Kendall Julie and Kenneth (1991), *Análisis y diseño de sistemas,* Editorial Prentice-Hall Hispanoamericana, México.

Tema 3. Auditoría a sistemas en operación

Por Sara Isabel Ayala Rodiles

Resumen

Cuando los sistemas de información están en plena operación, habrá que auditar su cumplimiento hacia los objetivos básicos de control: la totalidad, la exactitud, la autorización, el mantenimiento, la oportunidad y la utilidad. Cabe señalar que en este tema se analizan las diferentes disciplinas y técnicas que auxilian al revisor o auditor en su trabajo.

En este tipo de auditoría se verifican los diversos controles que existen a lo largo del flujo de la información: la entrada, el proceso y la salida. Dentro de este tema, se estructura un ejemplo de metodología para auditar a un sistema de información que está operando; de igual forma, se describen algunas de las muchas técnicas computarizadas que han surgido para apoyar el quehacer del auditor en el campo de la administración, en los sistemas automatizados y en la revisión de los controles.

La adquisición de bienes informáticos es una área que se torna día con día más compleja, en tanto la tecnología que hoy es vigente dejará de serlo en unos cuantos meses, por lo que la auditoría a este proceso es fundamental para las instituciones.

Tema 3. Auditoría a sistemas en operación

Por Sara Isabel Ayala Rodiles

Un sistema de información o aplicación se define como un conjunto de procedimientos manuales y computarizados, interrelacionados y que constituyen un sistema que produce información relacionada con cierto tipo de operaciones o actividades. Para que un sistema de información funcione satisfactoriamente es necesario que las partes manual y computarizada operen adecuadamente. Por tanto, el auditor debe evaluar ambos aspectos de los sistemas de información en operación.

El auditor de sistemas de información necesita conocer y evaluar el control interno de los sistemas de información computarizados para determinar: el alcance, la cobertura y profundidad, la naturaleza y tipo de pruebas y la oportunidad de sus procedimientos de auditoría.

Los objetivos de control son los aspectos que se deben controlar en el proceso de la información, son el qué del control. A continuación se presenta un cuadro que muestra los objetivos básicos de control representados con en las siglas: **TEAMOU** (**T**otalidad, **E**xactitud, **A**utorización, **M**antenimiento, **O**portunidad y **U**tilidad).

Totalidad: Este objetivo hace referencia al registro inicial, al suministro, a la alimentación, a la actualización y a los datos generados por la computadora. Persigue que, durante el flujo de información, todas las operaciones (no deben existir faltantes ni sobrantes de procesar):

- Se registren inicialmente.
- Se suministren a la persona que tiene que procesarlos.
- Alimenten al computador.
- Actualicen los diferentes archivos o bases de datos manejadas en la aplicación.
- Se consideren en los procedimientos de cálculo, totalidad, categorización, etc.

Es importante considerar también la totalidad del registro de las operaciones rechazadas inicialmente por el sistema de información, ya que esta situación puede ser frecuente y descontrolada.

Exactitud: Este objetivo hace referencia al registro inicial, a la alimentación, a la actualización y a los datos generados porla computadora. Persigue que los datos importantes de cada operación o actividad sean correctos y precisos, cuando:

- Se registren inicialmente.
- Se suministren a la persona que tiene que procesarlos.
- Alimenten al computador.
- Actualicen los diferentes archivos o bases de datos manejadas en la aplicación.
- Se consideren en los procedimientos de cálculo, totalidad, categorización, etc.

Es importante considerar también la exactitud del registro de las operaciones rechazadas inicialmente por el sistema de información, ya que esta situación puede ser frecuente y descontrolada.

Autorización: el control primario de una operación dada es el acto de su autorización, y consiste en que alguien, comparándola con los planes, condiciones, limitaciones o conocimiento general de lo que constituye una operación correcta, decide si es o no válida. El acto debe ser ejecutado por una persona reconocida en el sistema establecido como quien tiene la facultad y la competencia para hacerlo.

El control primario de una operación dada es el acto de su autorización.

Mantenimiento o continuidad: este objetivo persigue que las operaciones/ actividades permanezcan completas y exactas en el tiempo, que no se altera o modifica. Por ejemplo, que la información de junio permanece, continua, se mantiene total y exacta con posterioridad a junio, en julio, agosto, septiembre, etc.

Oportunidad: Este objetivo persigue que el registro de las operaciones/ actividades y, que la información que se genera por el sistema, sea oportuna para la toma de decisiones. El objetivo de oportunidad busca que no se retrase el proceso de la información.

Utilidad: Este objetivo persigue que la información que se produce sea útil para la toma de decisiones, que los usuarios utilicen el sistema.

La información producida debe ser útil para la toma de decisiones.

Principales técnicas de control

Las técnicas de control son los aspectos controlados en el proceso de la información, son el cómo del control.

Las técnicas de control son los aspectos controlados en el proceso de la información, son el cómo del control. Las técnicas de control pueden ejercerse manualmente o por medio de programas de cómputo. Cabe señalar que debe utilizarse la computadora no solo como una máquina que tiene la capacidad de efectuar operaciones a gran velocidad y almacenar enormes cantidades de información, sino como un aliado del control interno. La computadora puede realizar operaciones lógicas, es decir, comparaciones (mayor que, menor que, igual a, etc.) lo cual se puede aprovechar, incluyendo algunas de las técnicas de control en los programas de cómputo. Las principales técnicas de control son:

- **Verificación de secuencia numérica del registro de las operaciones**. El mejor medio para asegurarse de que al procesar las operaciones no se escape alguna de ellas, es numerarlas para después de procesadas compararlas (se numeran previamente los documentos/operaciones).

- **Verificación de uno por uno**, por ejemplo, reportes de cómputo contra documentos fuente.

- **Comparación contra datos pre-registrados**. Por ejemplo, la comparación de una orden de compra contra la factura del proveedor. El documento de una operación puede anexarse a otro originado independientemente, como evidencia de su validez. Por ejemplo, la factura del proveedor puede acompañarse con los informes de recepción y la orden de compra. Algunos datos pueden compararse con estándares predeterminados o listas de normas establecidas, por ejemplo, contra presupuestos.

- **Comparación de totales de control, cifras control**. Algunas medidas de control consisten en comparar una cifra con otra que se ha determinado independientemente, lo que con frecuencia requiere también una conciliación.

- **Conciliaciones bancarias.** La conciliación de la suma de los saldos detallados del auxiliar con el saldo global de la cuenta de control (de mayor); los recuentos físicos de caja (arqueos), de valores, de inventarios o de otros activos y, finalmente, la confirmación directa de saldos de deudores y acreedores. Algunos cifras de control pueden ser:

    - Total de documentos.
    - Total de renglones.
    - Total de importes.
    - Total de cualquier campo numérico (número de cuenta, folio, número de parte, unidades, etc.).

- **Dígito verificador.** El cálculo del dígito verificador involucra la multiplicación de cada uno de los dígitos del código original por cierto factor de ponderación, la suma de estos resultados y luego la división de esta suma por un número que representa el valor del módulo. Finalmente, se resta el valor del módulo del residuo de la división anterior. El analista de sistemas elige la ponderación y el módulo por utilizar. Los tipos de errores que puede detectar son:

    - Sustitución de dígitos
    - Transposición de dígitos

El enfoque de dígito verificador es útil cuando los códigos originales son de cinco o más cifras.

- **Verificación de razonabilidad**

    - Contra Rangos. Por ejemplo tabuladores de sueldos.
    - Contra Constantes. Por ejemplo femenino / masculino, sí/no.

- **Verificación del formato, sintaxis** (naturaleza: campos [datos] numéricos, alfabéticos, alfanuméricos y, longitud de campos)

- **Verificación de generaciones de archivos** (abuelo, padre, hijo), por medio de las etiquetas internas. Los archivos con información más antigua son los archivos abuelos, en seguidas los archivos padre y los archivos que contienen información más reciente son los archivos hijo. En los archivos de cómputo de diferencia entre abuelo, padre e hijo puede variar: un día, una semana, una semana, un mes, etc. Es importante que existan controles que garanticen que se procesan archivos de generaciones compatibles. Por ejemplo enero con enero.

- **Reproceso selectivo de partidas por los usuarios**, para garantizar que los procedimientos de cálculo efectuados porla computadora no se modifican de manera desautorizada. El mismo que ejecuta una operación puede verificarla; pero se asegurará más el control y la verificación interna si lo hace otra persona/ programa de cómputo.

- **Control de pendientes.** Otra verificación bastante común en la que todo se registra, consiste en anotar las operaciones o conservar un expediente con copia de los documentos que las originan y tachar de las listas, o retirar de los expedientes, las operaciones que se van procesando. Sin embargo, estos archivos o expedientes de asuntos no terminados o pendientes requieren, para su funcionamiento efectivo y para que constituyan una medida de control, ser revisados periódicamente para tomar las medidas procedentes y no dejar en ellos asuntos pendientes por demasiado tiempo.

- **Lista de recordatorio.** Ejemplos típicos de estas listas son los archivos de facturas o cuentas por pagar, por fecha de vencimiento o los calendarios de obligaciones fiscales.

Las disciplinas sobre los controles básicos son aquellos aspectos de un sistema que aumentan la confianza de que los controles básicos operan adecuadamente. Las disciplinas son importantes porque ofrecen una razonable seguridad de que las operaciones básicas y las técnicas de control funcionan, es decir se llevan a cabo tal como fueron diseñadas. Las disciplinas sobre los controles además incrementan la seguridad de que los errores se detectan oportunamente. A tres actividades de control se les ha dado la categoría de disciplinas:

Las disciplinas sobre los controles además incrementan la seguridad de que los errores se detectan oportunamente.

- Segregación de labores/funciones.
- Adecuada custodia de activos, es decir, acceso controlado o restringido.
- Supervisión.

Segregación de labores/funciones: En un ambiente de proceso electrónico de datos es importante considerar la segregación de funciones del personal que labora en el área de informática. La separación de una actividad de otra tiene varios propósitos: aparte de los objetivos de control, facilita la especialización de labores y del personal que las ejecuta.

En la segregación de labores, el trabajo de una persona actúa como medida disciplinaria o de verificación de otra. El acceso controlado o restringido es una disciplina necesaria para prevenir actividades no autorizadas de cualquier índole, desde la pérdida o mal uso de los activos, hasta la pérdida o mal uso del libro mayor.

No obstante, debe medirse el costo relativo en cada caso, normalmente solo se obtiene eficiencia con la segregación de labores cuando el volumen de operaciones justifica la especialización.

Normalmente solo se obtiene eficiencia con la segregación de labores cuando el volumen de operaciones justifica la especialización.

Si dos partes de una operación son ejecutadas por diferentes personas, una verificará a la otra. La segregación de labores también sirve para prevenir fraudes u ocultación de errores pues se necesitara la concurrencia de dos o más empleados en cooperación (colusión) para lograrlo.

Acceso controlado o restringido: Se refiere a la seguridad física, tanto del efectivo, inventarios, activo fijo, documentos, libros, reportes, formas, archivos del computador en medios magnéticos u ópticos, etc. Es muy común pensar en la restricción del acceso con relación a activos disponibles como dinero, valores y algunas veces inventarios y otros activos que pueden ser fácilmente vendibles o de uso personal. Sin embargo, debe aplicarse también a registros del sistema y a los medios con que pueden alterarse, como serían las formas en blanco de

pólizas, cheques, placa autográfica de cheques, archivos, sala de computación, archivos de cintas del computador y cualquier otro elemento del sistema de información. Los sistemas y las normas de disciplina deben procurar limitar el acceso a estos medios, al personal competente y responsable.

Finalmente, las medidas físicas de seguridad deben también proteger los archivos y registros contra deterioro, destrucción o perdida.

Supervisión: Probablemente es la disciplina más importante sobre los controles básicos, ya que aumenta la confianza en la información. Sin una supervisión adecuada se corre el riesgo de que aun los mejores sistemas de información y control se vuelvan erráticos y no confiables en poco tiempo, ya que las rutinas tienden a distorsionarse con la presión normal del trabajo y el personal busca formas más fáciles de hacer su tarea.

La falta de supervisión puede detectarse, aun en sistemas bien diseñados, por problemas en las cuentas, como un desusado número de errores y excepciones, retraso en el trabajo, cuellos en botellas en los registros, y el abandono de procedimientos prescritos.

Controles en el flujo de información: entrada, proceso y salida de datos

Controles en la entrada de datos. Las actividades que se realizan para la alimentación de datos, frecuentemente involucran de manera importante la intervención humana. Los controles en esta etapa buscan que la información de entrada sea validada y, cualquier error detectado sea controlado, de manera que la alimentación de datos al computador sea autentica, exacta, completa, útil y oportuna.

Las técnicas en los controles de entrada se usan para identificar errores en los datos antes de ser procesados y son ejercidos durante el flujo de la información. El ejercicio de los controles de entrada se ejecuta a nivel de:

- **Dato o campo**
  Datos requeridos
  Tipos de carácter
  Rangos
  Constantes
  Dígito verificador
  Contra archivos maestros
  Tamaño

- **Registro**
  Signo
  Secuencia numérica

- **Lote (grupo de registros o transacciones)**
  Totales de control por grupo
  Tipo de transacciones incluidas
  Número consecutivo de lote
  Secuencia numérica de partidas incluidas en el grupo
  Tamaño límite del lote
  Fecha de preparación del lote
  Información de errores detectados
  Espacio para firmas de quién preparó, verificó, procesó, etc.

- **Archivo**
  Etiqueta interna
  Número de generación
  Fecha de expiración
  Totales de control

El auditor debe estar interesado en los siguientes aspectos de las validaciones programadas: en cómo se validan los datos, cómo se manejan y reportan los errores y en cómo se emite esta documentación.

La fase de entrada, se subdivide en dos momentos: el de la captación u obtención de datos y el de la alimentación de los datos.

La captación u obtención de datos. Se refiere a la identificación y registro de los eventos que son relevantes en la organización para la adecuada operación de la misma. Los métodos de captación son:

- **Documental**. Las características de este método son su facilidad, flexibilidad, la sustencial intervención humana, su costo y su riesgo a los errores humanos. En esta etapa, el adecuado diseño de los documentos fuente, es fundamental para:
  - Aumentar la velocidad y exactitud del registro de datos.
  - Controlar el flujo del trabajo.
  - Facilitar la preparación de datos en forma legible por la máquina.
  - Facilita la verificación subsecuente.

- **Directo.** Se refiere al registro inmediato de un evento cuando ocurre, usando un dispositivo de entrada (terminales, teléfono, lápiz óptico, etc.). Este método se caracteriza por una menor intervención humana y por tanto, menos errores de captura, por la inmediata retroalimentación del sistema, sin embargo, es un método costoso tanto en *hardware* como en *software.*

- **Híbrido.** Se refiere a la combinación del método de documentos y el directo para la captura de datos. Los documentos contienen parcialmente información pre-impresa (datos constantes) acerca del evento por registrar (documentos de ida y vuelta: cheques, marbetes de inventario, etc.). Se caracteriza también por una menor intervención humana y porque sus costos pueden resultar altos tanto en *hardware* como en software.

Alimentación de los datos. Se refiere a la identificación y registro de los eventos que son relevantes en la organización para la adecuada operación de la misma. Los dispositivos de alimentación directa de datos se caracterizan por:

- Lectura rápida, por ejemplo pueden leer marcas en lugar de caracteres alfanuméricos. La posición de las marcas en el documento indica su valor.
- Almacenamiento al tiempo de lectura.
- Cierta validación.
- Fácil para el ser humano.
- Requieren impresoras de gran calidad y tinta en buen estado.
- Para altos volúmenes de entrada.
- Costosos y no muy confiables.
- Sujeta a errores de codificación.
- La preparación es fácil y sujeta a pocos errores.
- No adecuado cuando los datos a capturar varían muy frecuentemente.

Los dispositivos de alimentación directa no son adecuados cuando los datos varían frecuentemente.

Respecto a los medios utilizados en esta etapa de entrada, cabe recomendar los siguientes puntos para la definición de la estructura y estilo de los documentos fuente:

- Pre-imprimir documentos, formatos no memorandos.
- Numerar los documentos, folio.
- Proporcionar títulos, encabezados, notas e instrucciones.
- Usar técnicas de énfasis de diferencias.
- Clasificar los datos para facilitar el uso.
- Proporcionar respuestas múltiples a preguntas para evitar omisiones.
- Utilizar encuadres para identificar el tamaño del dato.
- Combinar instrucciones con preguntas.
- Proporcionar espaciado adecuado.
- Diseñar correctamente para fácil tecleo.
- Conformarlo de acuerdo con estándares de la organización.
- Proporcionar espacio para correcciones y firmas.
- Entrenamiento a los responsables en el llenado de los documentos fuente.

Un adecuado diseño de las pantallas de entrada es fundamental en esta etapa de entrada de datos. Se recomiendan los siguientes aspectos:

- Organización de la pantalla: ordenada y simétrica.
- Delimitadores e instrucciones de llenado.
- A imagen del documento fuente o conforme se obtiene los datos.
- Consistencia.
- Distinguir información ofrecida por el sistema de la solicitada al usuario.
- Evitar salto automático al siguiente dato.
- Rápido tiempo de respuesta, ayuda, uso códigos.
- Mensajes de error (cortos, significativos, corteses, neutrales) .

Pista de auditoría. Mantiene la cronología de los eventos acerca del origen de la transacción y su futuro proceso, así como la cronología de los eventos desde que los datos son validados hasta que son corregidos (cuando hay errores) y se consideran aceptables para continuar en el proceso.

Controles sobre el proceso de datos

La etapa de proceso es la responsable de calcular, clasificar, ordenar y sumar los datos. Los principales problemas en esta etapa son:

- Estilo de programación.
- Manejo del redondeo.
- Intervención del operador.
- Manejo de *overflow.*
- Manejo de cifras corrida a corrida.
- Manejo del signo.

Los principales riesgos que se encuentran en el proceso de los datos son:

- Intervención de programadores incautos o inexpertos.
- Falta de estándares.
- Utilización de la versión correcta del programa.
- Caídas del sistema.
- Desconocimiento de políticas y procedimientos (normatividad).

Para minimizar los efectos negativos, se requieren controles para:

- El adecuado manejo del redondeo.
- La impresión de totales corrida a corrida.
- Minimización de la intervención del operador.
- Establecimiento de cálculos redundantes en el caso de campos de resultados sensibles o importantes.
- Evitar el traslape de longitud de los datos (*overflow).*
- Verificación de la razonabilidad de los resultados (pago neto).

- Conciliar totales de corrida a corrida.
- Los programas de aplicación contienen las instrucciones requeridas por el usuario para el registro y control de la información cuando existan errores o irregularidades.
- Se debe impedir la entrada de datos vía consola del operador o desde el servidor en una red.
- Debe haber un control de las interrupciones.
- Se sugiere la verificación de etiquetas internas de los archivos.
- Deben existir verificaciones sobre datos numéricos para asegurar la totalidad, exactitud y autorización de los cálculos. El tipo de verificación varía debido a la diversidad del proceso.

Durante cada paso de trabajo es deseable que se generen totales de control, lo cual proporciona evidencia de la totalidad y exactitud del procesamiento de datos. Un ejemplo en la actualización de un archivo maestro: saldos anteriores, más registros adicionados, menos registros dados de baja debe ser igual a los saldos finales. Otro ejemplo es que el total de registros leídos debe ser igual al total de registros grabados.

Durante cada paso de trabajo es deseable que se generen totales de control, lo cual proporciona evidencia de la totalidad y exactitud del procesamiento de datos.

Minimizar la intervención del operador disminuye la probabilidad de errores. Se sugiere que se efectúe una validación de las acciones tomadas por el operador.

Otra sugerencia es evitar rutinas cerradas, es decir, cuando el programa asume una condición si no existe alguna de las esperadas, "valores de default". Por ejemplo cuando se busca uno de cuatro valores y en su defecto se asume un quinto valor, sin esperar algo diferente.

Pista de auditoría. Mantiene la cronología de los eventos que el dato es recibido en la entrada hasta el tiempo en que es enviado a un archivo o reporte.

Controles en la etapa de salida

En la etapa de salida se tienen funciones que determinan el contenido de los datos que deben ser proporcionados a los usuarios, el formato de los datos y la forma en que los datos serán preparados para ser enviados a los usuarios.

Los controles en esta etapa buscan que no se pierda o robe la información, de acuerdo a la sensibilidad de los datos proporcionados y el tipo de proceso: *batch* (proceso en un momento diferente a cuando ocurre el evento) o en línea (proceso en el momento que ocurre el evento).

Los medios de salida de la información son el papel o el desplegado en la pantalla. El formato es a través de tablas o gráficas.

Los controles sobre el diseño de reportes son:

- Nombre del reporte.
- Fecha y hora de producción.
- Periodo de proceso cubierto.
- Programa que lo produjo.
- Número de página.
- Encabezado de campos.
- Marca de fin de trabajo.
- Clasificación de seguridad/confidencialidad.
- Lista de distribución.
- Fecha de retención.
- Método de destrucción.

Los controles sobre papelería son:

- Inventario.
- Almacenamiento seguro.
- Control de acceso a operadores.
- Formas pre-impresas.
- Formas pre-numeradas.

Los controles sobre los programas para producir reportes aseguran:

- Uso de la versión correcta.
- Evitar alteraciones efectuadas por el operador vía consola.
- Puntos de chequeo y reinicio (console log).
- Impresión del reporte en una impresora remota.

Los controles sobre archivos para impresión (*spooling/printer files*) están diseñados para asegurar que:

- El contenido de los archivos no se altera.
- No se emitan copias no autorizadas.
- Los archivos se impriman una sola vez.
- No se utilicen respaldos de archivos para efectuar copias no autorizadas.

Los controles sobre la recolección y distribución reportes aseguran:

- Lista de reportes a producirse.
- Lista de usuarios autorizados.
- Establecimiento de periodos de recolección.
- Existencia de lugares y mobiliario seguro.
- Firma y fecha de recepción de los reportes.
- Etiqueta en el reporte para cada usuario.

Los controles sobre la destrucción de reportes aseguran el establecimiento de un procedimiento de destrucción de los reportes, el ideal es mediante trituradoras de papel (suficiencia, correcta ubicación, etc.)

La pista de auditoría. Mantiene la información acerca de los eventos que ocurren, desde el momento en que el contenido de la salida es determinado hasta que es entregado a los usuarios.

Enfoque de Auditoría

Antecedentes

- Objetivo (s) del sistema, beneficios esperados y limitaciones.
- Organigrama general de la empresa y de las áreas involucradas, señalando los puestos.
- Configuración del *hardware* en que trabajara la aplicación (medio ambiente).
- *Software* disponible para la aplicación sistema: sistema operativo, sistema de seguridad, lenguajes de programación.
- Utilerías, base de datos, *reporteadores,* etc. Se debe indicar la versión y las principales características/funciones de cada uno.
- Breve descripción de la normatividad interna y externa aplicable: políticas, leyes, disposiciones, requerimientos, etc.
- Breve descripción del entorno económico.

Conocimiento del ambiente de control en aplicaciones computarizadas. Algunas de las herramientas por utilizar para documentar el conocimiento y evaluación de los controles en los sistemas de información computarizados, tanto en lo que se refiere a los procedimientos manuales y automatizados son:

- Los flujogramas panorámicos. Se debe conocer la simbología de diagramación. (se sugiere documentar separadamente el conocimiento de los procedimientos manuales y computarizados).
- La descripción narrativa complementaria de controles de manuales y computarizados.
- El diseño de los principales archivos de datos.
- La matriz de control.

Fuentes de información. Se refiere al análisis de documentación actualizada (manuales de procedimientos y sistemas y a las entrevistas de personal que conoce las diferentes partes del sistema, usuarios, mesa de control y líder en desarrollo y mantenimiento de sistemas).

Respecto a la entrevista, es importante conocer algunos elementos que la afectan:

- Elección del personal adecuado para entrevistar.
- Familiarización con el sistema, documentos y reportes.
- Explicación de los objetivos e indicación de la duración aproximada de la sesión al entrevistado, así como la razón de haberle elegido para entrevistarlo. El uso del tiempo del auditor y del auditado es un factor muy importante por controlar.
- Conocimiento, por parte del entrevistado, del uso que el auditor da a la información, asegurándole la confidencialidad.
- Comenzar con preguntas y comentarios generales no comprometedores y después equilibrar la cantidad y el orden de preguntas abiertas, cerradas y de sondeo, evitando preguntas tendenciosas.
- Mencionar el grado de detalle que desea obtener en las respuestas y hacer énfasis en los procedimientos de control.
- Manejo adecuado del comportamiento verbal y no verbal (corporal / actitudes):
  - Contacto visual. Mirar al inicio de un tema/pregunta al interlocutor, durante el desarrollo mirar alrededor y al concluirlo mirar nuevamente al interlocutor. Una mirada persistente incomoda.
  - Movimiento de las manos. El estrechar firmemente la mano ayuda a establecer credibilidad y confianza. Las manos colocadas sobre la frente o cara son señal de que sé y intenta ocultar la verdad o revelar más de lo debido. Los dedos en contacto yema con yema denotan confianza en sí mismo.
  - Vestimenta apropiada en apego a las normas de la cultura organizacional.
  - Control de reacciones emotivas.
  - Gesticulación apropiada: entusiasmo, interés, etc.
  - Voz. No demasiado elevada ni baja de volumen.
  - Claridad al hablar, sin prisa.
- Parafrasear en aspectos complejos o dudosos, repetir en palabras propias.

En la entrevista es necesario mencionar el grado de detalle que se desea en las respuestas.

A continuación se proporciona una guía para la obtención de la información:

- Identificar al personal adecuado para la entrevista.
- Elaborar previamente un cuestionario básico.
- Estar alerta a actividades/operaciones poco frecuentes pero que pudieran ser claves.
- Analizar los efectos del exceso de actividad/detalle, ausencias o cambios de rutina.
- Considerar las consecuencias de la demasiada simplificación.
- Preguntar al personal entrevistado:
  - Los procedimientos/actividades que lleva a cabo.
  - Los registros que mantiene bajo su control.
  - Los documentos que prepara y procesa.
  - De quién recibe documentos, cuáles y de qué manera.
  - A quién envía los documentos, cuáles y de qué manera.
  - Qué métodos utiliza para detectar errores, de qué naturaleza han sido y con qué frecuencia aproximada.
  - Cuál y cuándo fue el último error detectado.
  - Qué hace para corregir errores descubiertos.

La información necesaria para la preparación/actualización de los diagramas de flujo se obtiene por medio de entrevistas al personal operativo y de niveles de mando, así como mediante el análisis de los manuales de procedimientos.

Un diagrama de flujo sirve principalmente para facilitar la comprensión, evaluación y comunicación de los procedimientos, mediante la expresión de los mismos en forma gráfica, concisa y completa.

El diagrama de flujo permite al auditor identificar aspectos de control, fortalezas y debilidades en los sistemas de información y destacarlos. Su aplicación requiere tiempo y uso frecuente como herramienta de trabajo. Sus ventajas son:

- Requieren menos tiempo que las descripciones narrativas.
- Representan más fácilmente el flujo de las operaciones.
- Reducen el riesgo de malas interpretaciones por el estilo de redacción y la capacidad de síntesis.
- Son más fáciles de actualizar, principalmente cuando se elaboran con herramientas para PC´s.

Para obtener los beneficios de la elaboración de diagramas de flujo se deberán mostrar:

- Los procedimientos/actividades en secuencia y en líneas de flujo, paso por paso desde su inicio hasta su término. Cada actividad debe ser numerada secuencialmente, sobre todo las actividades de control: los que disminuyen riesgos, cómo son las autorizaciones, la conciliación de cifras control, etc, los procedimientos manuales y los computarizados.

- Deben destacarse las diferencias en las actividades de control en operaciones del mismo tipo, cuando éstas son procesadas en diferentes localidades o por diferentes personas.

- La documentación/informes generados en las diferentes secciones, departamentos, áreas, de la empresa (obteniendo fotocopia de las hojas que sean diferentes).

- Todas las copias de los documentos y su flujo correspondiente.

N	=	foliada
O	=	original
1	=	copia numero 1
2	=	copia numero 2
3	=	copia numero 3
Azul	=	copia azul
Rosa	=	copia rosa

- Los archivos de documentos/transacciones significativas. En medios manuales:

N	=	numérico
A	=	alfabético
C	=	por fecha o cronológico

Las letras se pueden indicar en minúsculas cuando los archivos son temporales y en mayúsculas cuando son permanentes.

- El nombre del puesto y, cuando sea significativo, el nombre de las personas que ejecutan el procedimiento.

- En la preparación de los diagramas deben usarse símbolos, cuyo significado más común se muestra al final de este documento.

- Preferentemente se deben elaborar utilizando paquetes para diagramación en pc's o bien, utilizando plantillas de diagramación y a lápiz.

- Se debe considerar la claridad, buena organización y simplicidad en la presentación. Evitar gráficas excesivamente complejas. La experiencia dicta que un diagrama debe ser reorganizado a medida que se cuente con más información. Primero se puede preparar un diagrama de flujo panorámico y, adicionalmente diagramas de flujo de cada operación/procedimiento por separado. Deberá conocerse y documentarse el flujo de una operación o procedimiento a la vez, para llegar a una conclusión lógica (segregación).

Un diagrama debe ser reorganizado a medida que se cuente con más información.

- El grado el grado de subdivisión en un diagrama (s) depende de la diferenciación de las funciones que se realizan o controlan.

- La bifurcación se puede manejar por medio del uso de conectores de hoja o página, minimizando la referenciación.

- Se puede incluir una breve descripción por separado y con referencias cruzadas al diagrama de las actividades complejas y de control, mostrando aspectos como son:

    - Límites de autoridad.
    - División de labores.
    - Evidencia del ejercicio de controles.
    - Naturaleza del proceso.

- Se deben titular cada diagrama y numerar cada una de las hojas.

- Se debe explicar cada una de las abreviaturas y marcas empleadas.

- Proporciona un mejor entendimiento los diagramas de forma «horizontal», para ser leído de izquierda a derecha a lo ancho de la hoja, anotando la explicación en la última columna de la derecha.

- Se recomienda el uso de formatos estándar.

- Se debe verificar el entendimiento de los procedimientos con los responsables, obteniendo aprobación.

- Se debe mantener un ejemplar de cada versión de los procedimientos, es decir, conservar los anteriores cuando se actualicen como un registro permanente.

Elementos de los flujogramas de los procedimientos manuales:

- Departamentos o áreas involucradas.
- Documentos fuente.

- Reportes/informes elaborados manualmente.
- Procedimientos de control.

Nota: es conveniente solicitar copia de los documentos fuente (llenados) y de una hoja de los reportes preparados manualmente. También se recomienda mencionar el volumen promedio de operaciones e impacto monetario en sistemas financieros importantes.

Elementos de los flujogramas de los procedimientos computarizados:

- Archivos maestros (diseño de registros y periodicidad de respaldo y medio de almacenamiento).
- Principales archivos de transacciones (diseño de registros, periodicidad de respaldo y medio de almacenamiento) .
- Documentos fuente (nombre y procedencia).
- Reportes generados conla computadora (nombre y distribución).
- Breve descripción de los procedimientos de: validación, calculo (incluye totalización y categorización) y actualización.

Nota: obtener copia de la primera y última hoja de reportes y los diagramas de bloque de todo el sistema.

Metodología para la auditoría de sistemas de información en operación

Etapa 1. Obtención/documentación de antecedentes:

- Objetivo (s) del sistema, beneficios esperados y limitaciones.
- Organigrama general de la empresa y de las áreas involucradas, señalando los puestos.
- Configuración del *hardware* en que trabajara la aplicación (medio ambiente).
- *Software* disponible para la aplicación sistema: operativo, sistema de seguridad, lenguajes de programación, utilerías, base de datos, reporteadores, etc. Se debe indicar la versión y las principales características / funciones de cada uno.
- Breve descripción de la normatividad interna y externa aplicable: políticas, leyes, disposiciones, requerimientos, etc.
- Correspondencia de auditoría (memorandos, cartas enviadas, etc.)

Etapa 2. Obtención/documentación del conocimiento de las procedimientos manuales del sistema (fundamentalmente de las actividades de control):

- Flujogramas de los procedimientos manuales.
- Breve descripción de los principales procedimientos de control.

- Copia de los documentos fuente.
- Copia de los informes/reportes a prepararse manualmente.
- Volumen promedio de cada una de las operaciones que se registraran en el sistema.

Etapa 3. Obtención/documentación del conocimiento de los procedimientos computarizados (automatizados) del sistema (fundamentalmente de los procedimientos de control).

- Diagrama general del sistema, en el que se muestren los módulos incluidos y el número de programas por módulo.
- Diagramas de bloque de los procedimientos computarizados, por módulo y en secuencia lógica de ejecución.
- Breve descripción de los principales procedimientos de control. Fundamentalmente los procedimientos incorporados en los programas de validación, cálculo, clasificación, totalización, categorización y actualización.
- Copia de los informes/reportes a generarse con la computadora (primera y última hoja).
- Diseño de registros en archivos o base de datos
- Existencia y aprobación del manual del sistema y de operación

Etapa 4. Evaluación del ambiente de control.

- Descripción de los riesgos y controles en la etapa de frontera.
- Matriz de control de la etapa de entrada (*)
- Matriz de control de la etapa de proceso (*)
- Matriz de control de la etapa de salida (*)
- Descripción de los riesgos y controles sobre la papelería y accesorios.

(*) se debe mostrar la presencia o ausencia de procedimientos de control

- pmx = paso manual x
- pcx = procedimiento automatizado x o nombre del programa cómputo
- n/a = no aplicable
- obs = no existe control

Etapa 5. Registro de debilidades de control. Se debe mostrar por cada debilidad:

- Número consecutivo de debilidad.
- Descripción.
- Repercusión o riesgo.
- Alternativas de solución sugeridas.

El registro de debilidades de control incluye alternativas de solución.

- Resultado de la discusión con el responsable fijando compromisos (cuando sea posible).

Etapa 6. Programa de pruebas de cumplimiento (manuales y utilizadola computadora). Se debe mostrar por cada prueba:

- Número consecutivo de prueba o nombre del programa de cómputo.
- Responsables.
- Descripción.
- Alcance.
- Referencia o índice de los papeles de trabajo que soportan la prueba.
- Control de errores/debilidades (totales, corregidos y sin corregir).

Etapa 7. Pruebas de auditoría.

Etapa 8. Informe de auditoría. Se debe indicar como mínimo:

- Fecha de preparación.
- Responsabilidad asumida.
- Alcance del trabajo.
- Referencia a normatividad consultada.
- Periodo cubierto en la revisión.
- Descripción de las debilidades de control y sugerencias, repercusión y alternativas de solución.
- Nombre, puesto y firma de los auditores que participaron en la revisión.

Técnicas de auditoría asistidas por computadora

El uso de la computadora con todas sus posibilidades como una herramienta de auditoría, tanto externa como interna, es cada más frecuente y necesario, ya que incrementa sensiblemente la eficacia y eficiencia en esta disciplina, le proporciona mejores alternativas al auditor, y en muchos casos resulta la única manera de analizar y evaluar los procesos automatizados. En suma, desarrollar auditoría en informática sin usarla computadora, cada vez resulta más improcedente.

Utilizarla computadora como una herramienta para llevar a cabo el proceso de auditoría es conocido comúnmente como técnica de auditoría asistida porla computadora o CAAT (Computer Asisted Audit Tecnique).

Algunas de estas técnicas son conceptos desarrollados específicamente para apoyar objetivos de auditoría en informática; otras técnicas han sido desarrolladas

aprovechando las facilidades naturales de los computadores de sus sistemas operativos, y *software* de base.

Las áreas en que estas técnicas pueden ser aplicadas pueden variar de acuerdo al enfoque que se le dé; para efecto del presente evento se presentarán de acuerdo a las siguientes áreas funcionales:

- Técnicas tradicionales.
- Técnicas de apoyo a la administración.
- Técnicas para auditar sistemas automatizados.
- Técnicas para la revisión de controles generales.

Uso de la computadora para la aplicación de técnicas tradicionales: La utilización para la aplicación de técnicas tradicionales se refiere a la área de participación de apoyo a la auditoría tradicional, es decir, el apoyo necesario para la realización de la auditoría no informática.

Una vez que las organizaciones desarrollan e implantan sistemas automatizados, los medios en que se conserva la información cambian de documentos físicos a medios de almacenamiento magnéticos. Es entonces cuando el uso del computador es necesario para que el auditor pueda cumplir su labor por falta de pistas de auditoría en papel. De este modo, el auditor aplica de nuevas técnicas acordes con la evolución y desarrollo de las organizaciones.

Cuando el auditor utilizala computadora como herramienta de apoyo a la auditoría no informática, recupera la posibilidad de procesar la información para sus propósitos, al analizar archivos, llevar estadísticas, seleccionar registros para su revisión, etc.

Los objetivos de auditoría en informática en esta área de participación pueden resumirse como sigue:

- Servir de apoyo a la realización de auditorías no informáticas cuando las operaciones se manejan por medio de proceso electrónico de datos.

- Proporcionar la información y facilidades necesarias que permitan al auditor informático llevar sus exámenes sobre bases confiables y en forma consistente, sin faltar a las normas de esta disciplina.

Paquete de auditoría es el término empleado para un conjunto de programas que tienen la capacidad de procesar uno o varios archivos de datos en medios magnéticos, funcionando bajo el control de parámetros definidos y aplicados por el auditor. Ésta es una técnica ampliamente usada por los auditores en informática, ya que permite al auditor analizar uno o más archivos de un sistema computarizado.

Estos programas han sido desarrollados por diferentes proveedores y por firmas de contadores o consultores, y pueden ser adquiridos, con el propósito de que el auditor, después de un breve entrenamiento, pueda obtener la evidencia suficiente y competente que requiera el caso, siendo su empleo sencillo y menos costoso que programas desarrollados a la medida.

Este tipo de *software* de auditoría, normalmente es capaz de producir totales, dar sumas cruzadas, seleccionar una muestra estadística, seleccionar transacciones, comparar totales y ejecutar cálculos sobre diversos elementos contenidos en uno o varios archivos. Esta técnica de auditoría está orientada a probar datos pero ayuda poco a probar la lógica de los programas de cómputo, solamente lo que pueda deducirse de los resultados al probar archivos de datos.

El paquete de auditoría ayuda poco a probar la lógica de los programas de cómputo.

Históricamente este tipo de *software* ha operado en modo *«batch»*, pero recientemente debido a la rápida expansión de sistemas computarizados operando en línea, los paquetes de auditoría permiten la ejecución en línea.

Los archivos de datos pueden usar diferentes dispositivos magnéticos, tales como cinta o disco, y en diferente organización, por ejemplo, secuencial o de acceso directo. Los parámetros de entrada aplicados por el auditor especifican el tipo de archivo que se esté procesando, el proceso lógico a ser aplicado a los archivos y el tipo de salida requerido (por ejemplo tipo de reporte). Así, el auditor puede utilizar los paquetes de auditoría comerciales para probar un sistema computarizado en diferentes partes y de diversas formas.

Las funciones más comunes de los paquetes de auditoría son:

- *Sumarización.*
- Sumas cruzadas.
- Selección de datos y presentación detallada.
- Diversos cálculos matemáticos.
- Formato de reportes.

- Comparación de dos generaciones del mismo archivo, pero cada uno correspondiente de diferente fecha, o dos archivos diferentes a la misma fecha con datos comunes.

- Clasificación.

- Empleo de muestreo estadístico: determinación de tamaño de la muestra, selección de partidas a auditar y extrapolación de los resultados del muestreo al universo.

- Comparación de diferentes archivos.

Algunos beneficios de utilizar paquetes de auditoría comerciales son los siguientes:

- Fácil uso para el auditor.

- El paquete puede procesarse en *hardware* independiente.

- Análisis independiente de archivos, sin depender del personal de procesamiento de datos.

- Uso efectivo y eficiente del computador sin necesidad de entrenamiento intensivo y complejo.

- Modificación de los procedimientos de auditoría para adaptarlos a los cambios operativos con esfuerzos reducidos.

- Un paquete de auditoría puede utilizarse en la revisión de varios sistemas de información computarizados.

Desarrollo de programas de auditoría a la medida de las necesidades. En este concepto se encuentran todos los programas que son concebidos para realizar la revisión de una aplicación computarizada en particular utilizando normalmente archivos de producción u operación. Dicha técnica está más difundida en empresas o instituciones que no están en posibilidades de adquirir un paquete o se trata de entidades cuyas actividades son únicas en el país y, no está disponible un paquete comercial que satisfaga las necesidades de auditoría.

El empleo de esta técnica exige que se disponga de especialistas como parte del equipo de auditoría y puede resultar costoso, ya que involucra la elaboración, prueba, ejecución y documentación de los programas de auditoría, aunque son más flexibles que los paquetes de auditoría.

Estándares de documentación de programas de auditoría a la medida de las necesidades:

- Nombre de la aplicación.
- Diagrama del sistema (menú jerárquico).
- Aspectos generales del programa.
- Formatos de archivos de entrada.
- Formatos de archivos de salida.
- Diseño y muestra de reportes.
- Diseño y muestra de pantallas.
- Descripción detallada de los principales procedimientos de cálculo, clasificación etc.
- Criterios de selección.
- Procedimiento de conexión de cifras.
- Instrucciones de corrida y listado de procedimientos de ejecución.
- Medio de almacenamiento y localización del programa.
- Requerimientos de equipo.
- Lista del programa fuente (última compilación, con comentarios a la lógica).

Uso de la computadora para la aplicación de técnicas de apoyo a la administración: Existen técnicas específicas orientadas al apoyo a la administración de la función de auditoría que han sido claramente identificadas. Sin embargo, las posibilidades que se tienen en este aspecto son prácticamente ilimitadas en las diferentes etapas del proceso administrativo, como por ejemplo en la planeación, supervisión y control de los trabajos de auditoría.

Selección del área por auditar. Esta es una técnica computarizada, cuya aplicación está fundamentalmente orientada a organizaciones que operan en localidades múltiples, ayudando al auditor en la selección de cuáles de ellas auditar. El objetivo de esta técnica es el optimar el uso de los recursos limitados

de auditoría, señalando las áreas con mayores problemas potenciales y dirigiendo su atención a las de mayor relevancia. Esta técnica consiste en el desarrollo de una matriz de perfil de localidades, proporcionando información clave de cada localidad.

Los indicadores fundamentales pueden ser financieros o aspectos de control, que puedan ser usados para evaluar la situación de la localidad y su nivel de desempeño.

***Scoring*:** Esta es una técnica de planeación que ayuda al auditor en informática a seleccionar sistemáticamente el sistema de información computarizado a ser auditado y está orientada a maximizar la eficiencia de auditoría. La técnica identifica las características cuantificables en sistema automatizado en particular, que son significativas desde el punto de vista de análisis de riesgos.

Las características son ponderadas y combinadas para obtener la calificación de un sistema. Varios sistemas automatizados pueden ser calificados en esta forma y entonces, puede ser comparado el beneficio potencial al revisar un sistema u otro.

Las características son ponderadas y combinadas para obtener la calificación de un sistema. Varios sistemas automatizados pueden ser calificados en esta forma y entonces, puede ser comparado el beneficio potencial al revisar un sistema u otro.

Multisite Audit Software. Esta técnica de auditoría puede ser mejor usada por organizaciones en que la operación de sistemas automatizados se lleve a cabo en centros de proceso de datos regionales y el desarrollo de los sistemas sea centralizado.

La aplicación de esta técnica considera el desarrollo de programas de cómputo para auditoría que serán usados para probar aplicaciones automatizadas en operación en múltiples localidades. Para un efectivo empleo de esta técnica es necesario que los sistemas computarizados sean similares.

Centro de Competencia Un centro de competencia es un centro de cómputo establecido en una localidad central que es responsable de la ejecución de los programas de cómputo para pruebas de auditoría. El centro de competencia recibe archivos de datos de otras localidades, ejecuta los programas de cómputo, y distribuye los resultados a los diversos auditores.

Las responsabilidades que generalmente se reconocen en un centro de competencia son las siguientes:

- Desarrollar el *software* de auditoría para requerimientos específicos que no puedan ser satisfechos por paquetes comerciales.

- Instalar y ejecutar el *software* de auditoría y distribuir los resultados.

- Custodiar la biblioteca de respaldos de archivos de datos y *software* de auditoría.

- Mantener procedimientos de recuperación.

- Dar asistencia técnica en la ejecución del *software* de auditoría.

- Establecer y mantener actualizados procedimientos de recepción, transmisión, almacenamiento, destrucción y seguridad de archivos de datos y programas.

- Obtener *el hardware* y *software* para cumplir con las responsabilidades anteriores.

Técnicas para auditar sistemas computarizados: La auditoría de sistemas computarizados es una de las áreas de participación fundamentales de la auditoría en informática y está orientada a la verificación de los controles en la etapa de entrada, proceso y salida de datos, para promover que los resultados del sistema sean confiables y de calidad. En esta área de participación es donde se han desarrollado más técnicas de auditoría, ya que aquí se verifica el procesamiento de los sistemas en operación. El objetivo principal de estas herramientas es verificar que los procesos y los controles incorporados en los sistemas computarizados, hacerlos confiables y evitar debilidades que las expongan a riesgos significativos.

En esta área también se verifica que el sistema esté funcionando de acuerdo con los requerimientos del usuario y a la normatividad interna y externa. Algunas técnicas son:

Lote de datos de prueba. El uso de esta técnica consiste en la preparación por el auditor de juegos de datos de entrada al sistema (por ejemplo, casos base), que le presentan un repertorio de transacciones reales y ficticias, para que sean procesados por el programa (s) usado (s) en la operación normal de los procesos, con el objeto de identificar resultados predeterminados, verificación de la efectividad del rechazo de información errónea y/o no autorizada en sistemas en línea, donde los archivos se actualizan en el momento en que se realizan las transacciones. La prueba de auditoría no se realiza al mismo tiempo que la producción normal, sino posteriormente. Estas pruebas son normalmente almacenadas en archivos temporales para evitar interferencia con la operación normal y real. El auditor deberá tener cuidado en todas las ramificaciones de los sistemas para no alterar información real, así como considerar todas las condiciones variables incorporadas en los programas. Esta técnica tiene la característica de que puede ser utilizada por personal con poca experiencia en procesamiento de datos, requiriendo poca asistencia.

El auditor deberá tener cuidado en todas las ramificaciones de los sistemas para no alterar información real, así como considerar todas las condiciones variables incorporadas en los programas.

Simulación paralela: Esta técnica consiste en el desarrollo por el auditor de sus propios programas, apoyado por especialistas, para realizar el mismo proceso que efectúa el programa de producción del sistema auditado, utilizando la misma información fuente, "archivos de datos vivos», para luego comparar los resultados de ambos. Su propósito es comprobar la lógica de los programas en operación. Es conveniente la utilización en sistemas que manejan grandes volúmenes de datos.

Datos de prueba integrados (*Integrated test facility*): En este caso se establece una entidad ficticia dentro del proceso (división, subsidiaria, sucursal, etc.) en donde se almacenarán los datos del auditor, pero con la peculiaridad de que serán procesados al mismo tiempo en que las transacciones reales se registran, teniendo como referencia el marco de referencia el ciclo de operación normal de los sistemas de información. Con esta técnica se tiene la razonable certeza de que las transacciones reales y las pruebas del auditor son procesadas al mismo tiempo, con el mismo programa y sujetas ambas a los mismos controles. Esta técnica es muy útil en sistemas complejos y con un grado elevado de transformación de la información, sin dejar huella visible como en el caso de sistemas en línea. Al aplicar esta técnica deberá cuidarse la debida autorización de la gerencia y la correcta y oportuna coordinación con los diversos departamentos involucrados, pues se introducirá información falsa en el flujo normal y deberá eliminarse posteriormente y en forma total de los archivos reales.

Con esta técnica se tiene la razonable certeza de que las transacciones reales y las pruebas del auditor son procesadas al mismo tiempo, con el mismo programa y sujetas ambas a los mismos controles.

Módulos de auditoría integrados (*embedded audit modules*). Esta técnica consiste en incorporar módulos, programas o rutinas (código) en los programas de la producción normal del sistema de información computarizado auditado y ejecutarlos en el momento de operación. Estos módulos, programas o rutinas del auditor son insertados en los puntos de los programas determinados por el auditor, señalando los criterios de selección de transacciones. Funcionan permanentemente en los sistemas conforme éstos operan realmente, de manera que operaciones no usuales o fuera de ciertos limiten son detectadas y registradas inmediatamente en archivos para uso de auditoría y utilizar métodos manuales o automatizados para analizarlos. Esta técnica requiere la participación del auditor en las especificaciones para el desarrollo y mantenimiento de los sistemas de información computarizados. Se requiere de amplios conocimientos de computación e integración con los diversos departamentos de la empresa que estén involucrados.

Registros extendidos. La técnica de registros extendidos reúne los datos para propósitos de análisis y evaluación de auditoría a ser incorporados en los archivos o bases de datos de la producción normal del sistema de información a auditarse.

Análisis de la lógica de los programas: Consiste en solicitar el programa fuente correspondiente a programas de producción, estando plenamente seguro de ello, y estudiarlo para determinar su confiabilidad. Esta técnica es útil en sistemas sencillos, pero en sistemas complejos puede resultar muy arriesgado, además de la asistencia técnica que se requiere.

Imagen del contenido de memoria (*Snapshot*): Tanto los auditores como el personal de procesamiento de datos, frecuentemente encuentran difícil la reconstrucción de la toma decisiones de los programas de cómputo. La causa es una posible deficiencia en tener juntos todos los elementos involucrados en el proceso de datos, *snapshot* consiste en imprimir cierta parte de la memoria, como son los valores que tienen ciertas variables en el momento de la toma de la decisión y analizarlo. En estos casos se requiere de una lógica específica a ser programada en el sistema y hace necesarios amplios conocimientos técnicos para leer la sección extraída.

Técnicas para la revisión de controles generales. Existen algunas técnicas que se han desarrollado para el apoyo de la auditoría, aunque en este caso su orientación no es a una aplicación especial, sino están orientadas a la verificación de controles generales. Algunas de ellas pudieran ser interpretadas y utilizadas como técnicas para la revisión de sistemas de información computarizados, sin embargo, para estos efectos se les ha considerado en su posible aplicación genérica.

Seguimiento o rastreo (*Traicing*): Esta técnica consiste en enumerar los pasos de la lógica de los programas de cómputo, es decir, el flujo que sigue una transacción en el procesamiento electrónico de ella, permitiéndole al auditor verificar el cumplimiento de políticas y procedimientos establecidos por la organización. La técnica de rastreo muestra qué instrucciones han sido ejecutadas en un programa de cómputo y en qué secuencia. Generalmente el *traicing* no es una técnica desarrollada por el auditor, pero puede aplicarla en su trabajo.

Mapeo (Mapping): El mapeo es una técnica que puede utilizarse para identificar la lógica que no ha sido probada de un programa especifico. Esta técnica muestra también la cantidad de tiempo de CPU consumida por cada segmento de un programa de cómputo. El intento original del *mapping* fue ayudar a los programadores a asegurar la calidad de sus programas. Sin embargo, los auditores pueden utilizar la técnica del mapping para localizar códigos (instrucciones) no ejecutados. El análisis derivado del empleo de esta técnica puede proporcionar al auditor una imagen de la eficiencia en la operación de los programas de cómputo y puede revelar segmentos de un programa no autorizados incluidos para fines ilícitos. Este *software monitorea* la ejecución de un programa de cómputo contando el numero exacto de veces que cada instrucción del programa es ejecutada, también midiendo el tiempo de CPU consumido por cada una de ellas.

Los auditores pueden utilizar la técnica del mapping para localizar códigos (instrucciones) no ejecutados.

Bitácora (Job Accounting Data Analysis). El análisis de la información relativa al uso del computador, archivos utilizados, programas ejecutados, tiempo máquina empleado, interrupciones, registros procesados, cambios de programas, etc., podrá darle al auditor excelentes pistas de auditoría. La interpretación de la bitácora puede resultar difícil para personal con pocos conocimientos de computación.

Auditoría en la adquisición de bienes informáticos *y outsourcing*

Una de las áreas de auditoría más conflictivas y sensibles en una institución es la función de adquisiciones que tratándose de bienes informáticos se torna aun más sensible, por las dificultades materiales para el concurso y evaluación de los mismos.

Los objetivos particulares de esta revisión son los siguientes:

- Economía y factibilidad del proyecto de inversión, evaluando su efectividad de acuerdo al objetivo pretendido y como solución a la problemática planteada en la institución.

- Protección contractual adecuada, por las cláusulas del contrato que señalan las obligaciones del proveedor y su limite de responsabilidad. Este objetivo toma capital importancia por los activos involucrados en este ambiente.

- Adaptaciones y(o) modificaciones mínimas. Este objetivo aplica particularmente para la compra de software y paquetes.

- Cumplimiento de las políticas y procedimientos establecidos por la institución.

El proceso de evaluación de esta actividad abarca los conceptos de equipo (*hardware*) y programas (*software*). Actualmente, es frecuente que muchas instituciones se apoyen en la contratación de una empresa externa (proveedor/ consultor) de todo o de parte del desarrollo de sistemas de información, principalmente como consecuencia del adelgazamiento de las estructuras organizacionales. A este concepto se le conoce como *Outsourcing*. Desafortunadamente, en la mayoría de los casos los resultados obtenidos han sido muy deficientes e insatisfactorios y por tanto, se requiere fortalecer las medidas de seguridad al respecto. Es importante mencionar que la cuota por hora cobrada por la mayoría de los consultores suele ser muy elevada y requiere de una estrecha supervisión por el personal que contrata el servicio externo.

En este tipo de auditoría no solo se revisa el cumplimiento de la normatividad general existente (interna y externa) para efectuar compras, sino los requisitos

particulares e importantes de los bienes informáticos, de manera que se elija la mejor alternativa disponible.

El proceso para la adquisición principalmente deberá considerar los siguientes aspectos:

- Determinación del presupuesto. Consideraciones financieras.
- Requisitos de la aplicación/prioridades establecidas por los usuarios y el personal de informática de la institución.
- Selección de posibles proveedores, de preferencia nacionales. Estos proveedores deben demostrar no tener relación alguna con los funcionarios y empleados de la institución que adquirirá el bien o servicio.
- Petición formal de propuestas.
- A partir del análisis y definición de requerimientos, se deberán explorar las diferentes alternativas (cuando menos tres propuestas recibidas) de solución realizando un estudio de factibilidad que comprenda los siguientes elementos:
    - **Factibilidad económica,** (estudio de costo-beneficio) involucrando los costos asociados a la adquisición, considerando no solo el desembolso inicial, sino los costos por entrenamiento al personal y mantenimiento de los equipos.
    - **Factibilidad operativa,** orientado a evaluar si el equipo tendrá la capacidad de procesar los volúmenes la información requeridos, con posibilidades de crecimiento probadas.
    - **Factibilidad tecnológica,** por las restricciones que esto pudiera tener para aprovechar íntegramente la inversión que se está realizando. Existen muchos casos en que se obliga a la institución a adquirir otro tipo de dispositivos para poder hacer operativo el equipo inicialmente contratado.

Se deben abrir, de preferencia, las cotizaciones en una fecha determinada ante la presencia de todos los concursantes a fin de que no existan favoritismos en la asignación del pedido y éste se canalice hacia la mejor alternativa para la institución. Estas solicitudes de propuestas deberán incluir todas las especificaciones técnicas y operativas que deberán cumplir para estar en posibilidades de concursar.

La evaluación de cada una de las alternativas recibidas de los proveedores siempre debe efectuarse previamente a la adquisición del bien informático. Ésta debe incorporar, en forma sistemática, varios aspectos. El costo del servicio no debe ser el único elemento de juicio, ni el que tenga mayor peso. Debe efectuarse, detenidamente, la evaluación de riesgos. Los principales elementos son:

- En cuanto al proveedor:

  - Ubicación.
  - Suficiencia de líneas telefónicas.
  - Preparación y experiencia del personal de soporte técnico a usuarios y/o del de desarrollo de sistemas de información.
  - Tiempo de establecido.
  - Situación financiera.
  - Instalaciones.

- En cuanto al bien informático:

  - Calidad de las demostración de los productos: puntualidad, capacidad para responder a las dudas planteadas, materiales de apoyo utilizados, duración, etc.
  - Referencias de los principales usuarios que han recibido el producto o servicio adquirir, considerando que el tiempo que éstos tengan de trabajar con él.
  - Características de las licencias de uso del *software*.
  - Calidad de los manuales (técnico, de operación y de usuario).
  - Se debe evidenciar la facilidad que tiene el proveedor para dar mantenimiento en el propio lugar en que se encuentra instalado el equipo o los programas de cómputo, ya que esto puede entorpecer la operación normal de la función informática.

Es fundamental la capacidad del proveedor para dar mantenimiento en el lugar donde esté instalado el equipo.

Realizar las pruebas de aceptación previas. Se sugiere que los resultados de las pruebas se alimenten a un sistema que asignará calificaciones y en forma automática señalará el ganador del concurso.

Es necesario una revisión minuciosa del contrato con el proveedor. Asimismo, es recomendable solicitar la opinión del departamento legal de la institución o en su ausencia de un especialista externo, que valide la formulación del mismo. Todo contrato debe incluir sanciones por incumplimiento de lo contratado.

En el caso de adquisición de paquetes es importante definir el nivel de modificaciones *(customización)* que requiere el sistema y/o el equipo para hacerlo operativo en la institución, aceptando que los paquetes responden a necesidades generales, pero que requerirán de este proceso de adecuación razonable para hacerlos operativos. Estos trabajos deberán declararse en forma detallada dentro de los contratos respectivos.

Al término de esta actividad se autorizará la compra mediante la aprobación de la gerencia y se iniciara un sistema de seguimiento estricto del proyecto de tal manera que éste se cumpla dentro de las estimaciones de costo y tiempo definidas.

La capacitación requerida por la institución que adquirirá el bien (considerando al personal de la función de informática y usuarios) y la ofrecida por el proveedor, tanto en *hardware* como en software. Este aspecto tendrá que formar parte de la propuesta inicial de cada proveedor, para tener un panorama real de la inversión necesaria. En la mayoría de los casos la capacitación otorgada ha sido insuficiente y deficiente, además de que en algunos casos los participantes al entrenamiento pertenecen a giros diferentes a la seguridad social. Algunos aspectos por revisar son:

- Calendarización que garantice que todo el personal que lo requiere asistirá.
- Duración.
- Porcentaje de teoría y de práctica.
- Materiales de apoyo para los participantes y para el expositor.
- Métodos de la enseñanza.
- Calidad de los instructores.
- Mecanismos para evaluación del aprendizaje.

Es necesario tener claramente especificado de qué activos se trata, de qué manera y cuáles serán los requisitos de autorización necesarios, los cuales pasarán a formar parte de la evaluación del auditor.

Para finalizar, es necesario contar con:

- La planificación del local (las instalaciones). Requerimientos operativos.

- El plan de instalación.

- La planificación de la conversión del sistema anterior al nuevo.

- El plan de implantación, de acuerdo con las necesidades de la institución, por ejemplo, la disponibilidad de las áreas usuarias y de informática.

- Realización de un seguimiento de los resultados que se obtengan al utilizar las nuevas adquisiciones a fin de comparar las expectativas contra los resultados reales y estar en posibilidades de realizar los ajustes necesarios. Establecimiento de la frecuencia de los reportes de avance.

Bibliografía

Caballero Pino (1997), *Seguridad informática,* Editorial Computec Rama, Madrid.

Hérnandez Jiménez Ricardo (1998), *Administración de la función de informática*, Editorial Trillas, México.

Piattini Mario G. Emilio (1998), *Auditoría de informática*, Editorial Computec, Madrid.

Rodríguez Estrada Mauro, Raquel Treviño y Leonora M. del Campo (1991), *La entrevista productiva y creativa.* Editorial Mc Graw Hill, México.

Tanubaum Andrew S. (1992), *Sistemas operativos modernos*, Editorial Prentice-Hall, México.

EJERCICIOS Y ACTIVIDADES DE EVALUACIÓN

TERCERA ACTIVIDAD
(Ejercicio individual)

Conteste las siguientes preguntas o reflexiones en un máximo de tres páginas:

1. ¿Cuál es la actitud general o filosofía de la institución en la que usted labora en relación con la auditoría en informática?

2. En caso de que exista la función de auditoría de informática en la institución en la que labora usted, mencione el estado general de la misma: su estructura orgánica, sus funciones, experiencias, resultados, planes a futuro. En caso de que no exista, mencione brevemente cuáles serían los factores principales que impulsarían su creación y por qué.

3. ¿Cuáles cree que sean los principales riesgos de la información en su institución?

4. Indique cuál ha sido la experiencia de las áreas usuarias de la institución en la que labora usted, en cuanto a las adquisiciones de bienes informáticos.

Módulo 4. Impacto organizacional de la tecnología de la información

INTRODUCCIÓN

Los conocimientos de los módulos anteriores sobre aspectos generales de la informática, su seguridad y auditoría se ha dirigido a ofrecer elementos para que usted reflexione sobre el mejoramiento en la práctica diaria de las labores de automatización. De igual manera, es importante preguntarse ¿qué sucedería si la propia institución o área donde laboro estuviera atravesando por algún cambio estratégico mayor, que implicara nuevos planteamientos, incluyendo la actualización en la propia misión de la organización? En este caso el enfoque de la automatización dependería totalmente de las nuevas estrategias.

El contenido del módulo se pensó en un principio como la parte complementaria de los sistemas de información (recursos humanos, organización, etc.); sin embargo, en la medida en que se fue analizando y estructurando, se pudo concluir que todos los componentes de la tecnología de información (llámese sistemas de información, plataforma tecnológica o recursos humanos informáticos), deberán depender de una directriz del más alto nivel y alcance, la cual será definida por la planeación estratégica de la institución y ejecutada quizás a través de un ejercicio de reingeniería de procesos.

Por ello, es importante que usted, ya sea que se desempeñe como directivo, personal de una coordinación de informática, o de un área usuaria, conozca y aplique los conceptos contenidos en el presente módulo con el objeto de que pueda tener un panorama más amplio en el cual se ubica a la tecnología de Información, y pueda a su vez convertirse en un agente protagonista del cambio en su organización.

☞ OBJETIVO

- Analizar el impacto organizacional generado por la incorporación de las tecnologías de la información.

PALABRAS CLAVE

Alcance competitivo
Cadena de valor
Decisiones clave
Diferenciación
Factores críticos de éxito
Facultación de los empleados
Funciones de procesamiento
Medidor de desempeño
Pensamiento discontinuo
Reingeniería de procesos
Sistema de valor
Ventaja en el costo

TEMAS

1. Reingeniería en las organizaciones
2. Rediseño de los procesos para su automatización
3. El desarrollo organizacional en el cambio

Autor de todos temas: Ricardo Loranca González

Tema 1. Reingeniería en las organizaciones

Por Ricardo Loranca González

Resumen

La reingeniería de procesos en las organizaciones puede ser originada por muchas razones: cambios económicos en el ambiente externo, fusiones o absorciones entre organizaciones. Sin embargo, uno de los motivos más concretos por los que se puede iniciar un proyecto de reingeniería, es la búsqueda de la ventaja competitiva.

La ventaja competitiva puede obtenerse a través de tres estrategias básicas: liderazgo en costo, diferenciación y alcance competitivo.

La cadena de valor está constituida por todas aquellas actividades que generan valor agregado para los clientes o usuarios de los servicios o productos de una organización. El estudio sistemático de ella forma la base para poder identificar e implantar los cambios que generarán ventaja competitiva.

La tecnología de la información es un componente que influye muy especialmente en la cadena de valor; esta influencia puede ser tal, que proporcione por sí misma una ventaja competitiva para la organización en lo referente a costos, diferenciación o alcance.

Tema 1. Reingeniería en las organizaciones

Por Ricardo Loranca González

Introducción

La reingeniería de procesos comprende la identificación, el rediseño y la implantación de los procesos del negocio para obtener mejoras en su tiempo, costo y calidad.

La reingeniería tiene su fundamento en un pensamiento discontinuo, el cual permite reconocer y romper con viejos paradigmas o esquemas que pudieran no estar correspondiendo a la misión y estrategia que la organización requiere.

Para poder comprender los motivos que llevan a una organización a buscar, evaluar y planear un cambio vía la reingeniería de procesos, es conveniente que el lector se familiarice con el concepto de **cadena de valor,** término creado por el profesor Michael Porter de la Escuela de Negocios de Harvard.

El estudio de la cadena de valor se utiliza para sustentar un estudio que permita crear o mantener la ventaja competitiva de una organización. Se basa en la premisa de que la ventaja competitiva no puede ser entendida analizando a la organización como un todo. Más bien depende de cada una de las actividades que la componen en cuanto al diseño, la producción, la comercialización, la entrega y el mantenimiento de su producto. Es necesario un estudio sistemático de estas actividades y de su interacción para poder identificar las fuentes de ventaja competitiva.

El estudio de la cadena de valor se utiliza para sustentar un estudio que permita crear o mantener la ventaja competitiva de una organización.

Existe un libro previo del profesor Porter titulado *Competitive Strategy: Techniques for Analysing Industries and Competitors* en el que se describen tres estrategias genéricas para poder obtener ventaja competitiva:

- Liderazgo
- Diferenciación
- Alcance

Una organización puede poner en práctica estas estrategias mediante el análisis de la cadena de valor.

La presente lectura parte de los planteamientos del libro del profesor Porter *Competitive Advantage*, los cuales se encuentran divididos como sigue:

1. El modelo de la cadena de valor.
2. El alcance competitivo.
3. La ventaja en el costo.
4. La diferenciación.
5. La tecnología y la ventaja competitiva.

1. El modelo de la cadena de valor

Definiciones

El análisis de la cadena de valor permite disgregar a una organización en aquellas actividades que son estratégicamente relevantes para poder comprender el comportamiento de sus costos y las posibilidades de diferenciación.

> El principio consiste en separar y aislar actividades que:
>
> - Tengan estructuras de costos diferentes.
> - Posean un impacto potencial alto para diferenciar a la organización.
> - Representen una proporción del costo que sea significativa o que esté incrementándose.

La cadena de valor muestra el valor total conformado por los valores de cada una de sus actividades (actividades de valor agregado) y sus márgenes. Las actividades de valor agregado son los componentes principales mediante los cuales una organización crea un producto con valor para su cliente. El margen sería la diferencia entre el valor total de venta y el total de los costos de realizar las actividades de valor agregado.

Específicamente, la cadena de valor es el conjunto de actividades de valor agregado en los ciclos de vida de los productos y/o servicios más importantes

dentro de un segmento de la organización. El profesor Porter identifica cinco categorías genéricas de actividades primarias y cuatro categorías genéricas secundarias:

- Actividades primarias
  - Logística de entrada
  - Operaciones
  - Logística de salida
  - Mercadotecnia y venta
  - Servicio
- Actividades de soporte
  - Adquisiciones
  - Desarrollo tecnológico
  - Administración de recursos humanos
  - Infraestrucutra de la organización (administración, finanzas, contabilidad, legal).

La comparación de las cadenas de valor de los competidores exponen diferencias que determinan ventajas competitivas.

Las organizaciones dentro de una misma industria pueden tener cadenas de valor similares; sin embargo, las cadenas de los competidores frecuentemente difieren entre sí. La comparación de las cadenas de valor de los competidores exponen diferencias que determinan ventajas competitivas. A continuación se presentan ejemplos de cómo algunas organizaciones han logrando ventajas competitivas mediante cambios en algunas actividades de su cadena de valor.

Logística de entrada. Una empresa de distribución instaló terminales de un sistema computarizado en las oficinas de sus proveedores, con el objeto de poder implantar un sistema de generación de órdenes de compra en línea y en tiempo real. La empresa solicitó a sus proveedores que mantuvieran un determinado nivel de inventario y que introdujeran las cifras de existencias disponibles en el sistema, de forma que el módulo de compras pudiera determinar las existencias disponibles para generar sus órdenes de compra.

Este sistema permitió la reducción del costo tanto de mantener almacenes e inventarios como de interrupciones por falta de materiales. La necesidad de mantener niveles de inventario de seguridad y los costos de mantenimiento relativos, fueron transferidos a los proveedores.

Operaciones. Una compañía de seguros mejoró el servicio a sus asegurados permitiendo la consulta en-línea sobre el estatus de sus reclamaciones. Además, también se proporcionó el acceso en línea a los clientes para nuevos servicios y productos. En éstos se incluyeron modeladores de pólizas que permitieron a

los empleados de la compañía determinar los costos y adecuar las pólizas conforme a las necesidades de los clientes. También se cubrieron otras necesidades proporcionando sistemas a clientes corporativos que eligen auto-administrar sus pólizas de seguros.

Logística de salida. El sistema de reservaciones de American Airlines y United Airlines mediante el cual las agencias de viajes se conectan con estas empresas ha influido tan profundamente las relaciones en ese negocio, que las compañías de aerolíneas más pequeñas que no utilizan este sistema han tenido serias dificultades para relacionarse con los agentes de viajes. El acuerdo con las agencias también ha contribuido a poder cobrar a la competencia por el uso del sistema (por ejemplo: por la cantidad de reservaciones y boletos emitidos).

Mercadotecnia y ventas. Una gran compañía farmacéutica ofrece servicios para que las farmacias puedan fincar sus órdenes de compra en línea tanto para la compañía farmacéutica como para otras empresas aliadas no competidoras.

Servicio. Un fabricante de equipo industrial instaló un sistema experto de mantenimiento en sus oficinas, que permite conectarse vía telefónica con sus máquinas cuando estas sufren alguna falla. El sistema experto realiza una análisis de fallas y emite instrucciones para el operador de la máquina. Esto ha repercutido en que además de reducir las visitas por servicio en un 90 %, se ha incrementado la satisfacción de los clientes.

Adquisiciones. Una cadena de tiendas detallistas ha tenido éxito al lograr tener acceso en línea a la información sobre los inventarios y los planes de producción de sus proveedores más pequeños. Dicho acceso le ha permitido administrar sus inventarios más eficientemente y presionar a sus proveedores para obtener un mejor precio y mayor disponibilidad de producto.

Desarrollo Tecnológico. El uso de la tecnología CAD/CAM "Computer aided design and manufacturing" ha cambiado fundamentalmente la calidad y velocidad en la que la industria de la construcción y la automotriz diseñan sus productos.

Administración de recursos humanos. En una empresa petrolera se proporcionaron terminales de cómputo a los miembros del comité directivo, mediante ellas, se permite el acceso a los expedientes del personal, lo cual ha mejorado sustancialmente la toma de decisiones.

Infraestructura de la organización. Una importante agencia de viajes utiliza conexiones en línea para poder mantener pequeñas oficinas en las instalaciones de sus clientes corporativos. Estas oficinas cuentan con todas las capacidades y funcionalidad de la casa matriz. Dichas conexiones han cambiado la estructura

organizacional, de ser una gran empresa centralizada a una empresa descentralizada formada por muchas oficinas de servicio pequeñas.

El sistema de valor

La cadena de valor forma parte a su vez de una serie de actividades que el profesor Porter identifica como el *sistema de valor*. Los proveedores tienen sus propias cadenas de valor (valor de entrada), las cuales crearon y entregaron el producto que se utiliza en la cadena de valor de la organización. Muchos productos pasan a través de cadenas de valor de canales (valor de canal). Finalmente, el producto de la organización formará también parte de la cadena de valor de su cliente, la cual determina sus necesidades y el grado de diferenciación del producto.

El producto de la organización formará también parte de la cadena de valor de su cliente, la cual determina sus necesidades y el grado de diferenciación del producto.

Las ligas dentro de la cadena de valor

Las ligas dentro de las actividades de la cadena de valor presentan otra oportunidad para obtener ventajas competitivas; esto se logra mediante la optimización y/o la coordinación de las actividades.

Por ejemplo, en la compra de acero de alta calidad, obtener láminas pre-cortadas podría simplificar el proceso de manufactura y reducir el desperdicio.

Las ligas más claras son las que existen entre las actividades primarias y las actividades de soporte; otras ligas más difíciles de identificar son aquellas entre las actividades primarias.

La administración y coordinación de las ligas representa una tarea mucho más compleja que la administración de las actividades de valor. Dada la dificultad para identificarlas y manejarlas, la capacidad para administrarlas a menudo representa una fuente importante de ventaja competitiva.

La administración y coordinación de las ligas representa una tarea mucho más compleja que la administración de las actividades de valor.

Ligas verticales

Las ligas existen no solo dentro de la cadena de valor de la organización, sino también con las cadenas de valor de los proveedores y con los canales de distribución (por ejemplo las actividades de adquisiciones y de logística de entrada, interactúan con las actividades de venta y logística de salida de los proveedores).

La diferenciación, la cual representa una de las estrategias clave, se deriva

fundamentalmente de la posibilidad de crear un impacto favorable en la cadena de valor del cliente.

Las ligas entre diferentes organizaciones son también oportunidades para obtener ventajas competitivas sobre sus competidores, y frecuentemente son tan particulares que es difícil reproducirlas o imitarlas.

Las ligas entre diferentes organizaciones son también oportunidades para obtener ventajas competitivas sobre sus competidores.

2. El alcance competitivo

El alcance de las actividades de valor de una organización puede ser muy importante dentro de los esfuerzos para obtener ventaja competitiva. El alcance es la combinación de las distintas (aunque relacionadas) cadenas de valor en las que incursiona una organización. Mediante ligas entre ellas, la organización puede mejorar la economía de alguna o todas sus cadenas de valor.

El alcance es la combinación de las distintas (aunque relacionadas) cadenas de valor en las que incursiona una organización.

Un amplio alcance puede brindar beneficios en cuanto costo y control, al permitir efectuar internamente más actividades que sus competidores.

Un alcance reducido puede también brindar ventaja competitiva mediante la adecuación de la cadena de valor para poder atender en particular un segmento o región de forma única o con un costo bajo. El alcance reducido permite a la empresa concentrarse y convertirse en la mejor en una determinada especialidad.

El profesor Porter identifica cuatro dimensiones del alcance competitivo:

- Alcance de segmento: la variedad de productos y de clientes atendidos.
- Alcance vertical: el grado mediante el cual se ejecutan actividades dentro de la organización, en lugar de hacerlo a través de empresas independientes.
- Alcance geográfico: la cantidad de regiones, países o grupos de países en los que una empresa compite con una estrategia coordinada.
- Alcance de industria: la cantidad de industrias relacionadas en las que compite una empresa con una estrategia coordinada.

Alcance de Segmento. Este alcance refleja la cantidad de productos y los clientes atendidos. Por una parte, una variedad o enfoque reducidos pueden conseguir obtener ventaja competitiva.

Como un ejemplo se puede mencionar a IBM, la cual descubrió que la cadena de valor de las grandes empresas usuarias de PC's difería considerablemente de la cadena de valor de las empresas pequeñas. Estas últimas requieren mucho más soporte en términos de asistencia técnica, capacitación, *software* amigable y servicios. Ésta probablemente fue una de las razones por las que IBM vendió sus tiendas de computadoras personales.

Alcance vertical. Es la medida en el que la organización realiza actividades internamente vs. hacerlo externamente. También define el grado de integración vertical entre una empresa y sus proveedores, canales o usuarios. Un grado alto de integración vertical en comparación con la competencia, puede tener ventajas en cuanto a un costo bajo o lograr una diferenciación.

Por otra parte, una baja integración le ofrece a la empresa las ventajas de una mayor flexibilidad en poder cambiar de proveedores ó canales de distribución conforme las condiciones cambien. Tal es el caso en el que las organizaciones de países desarrollados, toman ventaja de los costos sustancialmente bajos de los países en desarrollo para fabricar en ellos sus productos; pero los cambian a otros países en cuanto las condiciones económicas cambian.

Alcance geográfico. El alcance geográfico permite a una empresa obtener ventajas competitivas al compartir o coordinar actividades de valor que son similares en lugares diferentes.

Alcance de industria. Está representada por la cantidad de industrias relacionadas en las que una organización compite con una estrategia coordinada.

Las ligas entre las cadenas de valor de unidades de negocio que compiten en industrias diferentes, presentan muchas oportunidades para obtener ventajas competitivas. Dichas ligas pueden comprender prácticamente cualquier actividad de valor, tales como: instalaciones compartidas, tecnología, personal y aun experiencia.

Alianzas y ventaja competitiva

Una organización puede considerar conveniente obtener ventaja competitiva al formar coaliciones con otras organizaciones. En lugar de tener que ampliar sus instalaciones o personal, para poder ampliar su alcance se puede apoyar con otra empresa para ligar sus actividades con las de otras empresas.

Por ejemplo, el uso de licencias permite obtener un rápido acceso a una nueva tecnología o a nuevos productos, sin necesidad de una gran inversión en investigación y desarrollo.

Las alianzas proporcionan una forma de "probar el agua" dentro de nuevos segmentos, regiones o industrias relacionadas, sin la necesidad de acudir a desarrollo interno o adquisiciones. Las alianzas también permiten que las organizaciones obtengan los beneficios de una integración vertical (costo y control), sin que las organizaciones tengan que integrarse totalmente.

Las alianzas también permiten que las organizaciones obtengan los beneficios de una integración vertical.

3. La ventaja en el costo

La ventaja en el costo representa uno de los tipos básicos de ventaja competitiva. El costo también juega un papel importante dentro de las estrategias de diferenciación, ya que cualquier diferenciador debe mantener el costo cercano al de sus competidores.

El profesor Porter identifica los siguientes pasos en el análisis estratégico de costos:

1. Identificar la cadena de valor y asignarle costos y activos.

2. Determinar cuáles son los factores que influyen en el costo para cada una de las actividades de valor y cómo interactúan.

3. Identificar las cadenas de valor de la competencia y determinar el costo relativo de los competidores y las fuentes de diferenciación en costo.

4. Desarrollar una estrategia para mantener la posición competitiva de costo, mediante el control de los factores que influyen en el costo o a través de reconfigurar la cadena de valor.

5. Asegurar que la reducción en costos no erosione la diferenciación o genere una conciencia de que se está erosionando.

6. Probar la estrategia de reducción de costos para verificar que sea sostenible.

Las categorías de factores que impactan al costo son diez:

- **Economías de escala**: impacto de la economía de escala.

- **Aprendizaje: impacto** debido al aprendizaje obtenido a través de la experiencia de otros.

- **Patrón de capacidad utilizada**: impacto del patrón de capacidad instalada que es utilizada (considerando cambios en los niveles de capacidad instalada).

- **Ligas**: impacto de otras actividades dentro de la misma cadena de valor y/o en las cadenas de valor de proveedores o de los canales de distribución (por ejemplo: ligas verticales).

- **Interrelaciones**: impacto al compartir actividades con otras unidades de negocio.

- **Integración**: impacto del nivel de integración en una actividad de valor (por ejemplo: la decisión entre "comprar o fabricar").

- **Oportunidad**: impacto del tiempo en que se realizan las actividades (por ejemplo: "pionero" vs. "seguidor").

- **Políticas**: impacto de las políticas de la organización (por ejemplo: especificación del producto, nivel del servicio proporcionado, políticas de recursos humanos y tecnología).

- **Localización**: impacto de la localización geográfica (por ejemplo: disponibilidad y costos de mano de obra y transportación.

- **Factores institucionales**: impacto de factores institucionales (por ejemplo: regulaciones del gobierno, impuestos, incentivos financieros, sindicatos y reglas locales).

El costo de una actividad de valor está determinado frecuentemente por la interacción de muchos factores, aunque alguno o unos cuantos son los que ejercen mayor influencia. La identificación de dichos factores y la cuantificación de su efecto en el costo no es una tarea fácil. Algunos de los métodos sugeridos para analizar los factores incluyen:

- Examinar la estructura de costos de cada actividad de valor.
- Analizar la propia experiencia de la organización.
- Realizar entrevistas con expertos.
- Realizar comparaciones con la competencia.

Compras

Las compras tienen un valor estratégico en casi cualquier industria, pero raramente recibe la atención requerida en las organizaciones. El costo total de las entradas por compras, incluyendo tanto compras operativas como compras de activos, como si fuera un porcentaje del valor de la organización, proporciona un indicador importante del valor estratégico de las compras.

Los pasos para analizar las compras incluyen:

- Identificar todas las compras significativas y determinar su costo anual o trimestral.
- Debido a que la atención de la dirección se enfoca frecuentemente en los productos de alto costo o que se adquieren periódicamente, aquellos artículos de costo bajo y/o que se compran irregularmente, pueden presentar mayores oportunidades para reducir costos.

Costos de la competencia

Una organización tendrá una ventaja en el costo cuando el costo acumulado al ejecutar todas sus actividades de valor es menor al costo de sus competidores.

Una organización tendrá una ventaja en el costo cuando el costo acumulado al ejecutar todas sus actividades de valor es menor al costo de sus competidores. El valor estratégico de la ventaja en el costo dependerá del tiempo en que se puede sostenerse, lo cual a su vez se mantendrá si dicha ventaja es difícil de duplicar o imitar. Así, el análisis estratégico del costo debe incluir los costos y estructuras del costo de la competencia. El punto de partida es poder determinar las cadenas de valor de los competidores y la forma en que ejecutan sus actividades.

Si las cadenas de valor de los competidores son diferentes, la eficiencia de las cadenas será la que determinará su posición competitiva en el costo. Normalmente las diferencias comprenden sólo un conjunto de actividades de valor, y así una organización puede ser capaz de aislar el efecto que tienen las cadenas de valor diferentes sobre su posición competitiva de costo, al comparar los costos de solo aquellas actividades diferentes.

Por aquellas actividades que son las mismas, la posición competitiva en el costo puede determinarse al comparar los factores que influyen en el costo de esas actividades en relación con aquellas de la competencia.

La obtención de la ventaja en el costo

Existen dos formas en que una organización puede obtener la ventaja en el costo:

- Controlar los factores que influyen en el costo (de las actividades de valor que representan una proporción significativa del total del costo).

- Reconfigurar la cadena de valor (convertirse en más eficiente en el diseño, producción, distribución y comercialización del producto).

Algunas de las formas sugeridas para poder controlar los factores que influyen en el costo podrán incluir:

- Controlar la capacitación

  - Administrar con base a la curva de aprendizaje
  - Mantener la capacitación como propietaria
  - Aprender de la competencia

- Controlar interrelaciones

  - Compartir las actividades apropiadas con clientes, proveedores o aliados
  - Transferir conocimiento al administrar actividades similares

- Controlar factores institucionales

  - No tomar los factores institucionales como un hecho.

- Controlar políticas

  - Modificar políticas costosas que no contribuyen a la diferenciación
  - Invertir en tecnología para orientar los factores que influyen en el costo en favor de la organización.

- Controlar prácticas de compras

Para reconfigurar su cadena de valor, la organización debe examinar todo lo que hace y las cadenas de valor de los competidores en busca de opciones creativas para realizar las cosas en una forma distinta. El siguiente tipo de preguntas debe realizarse para cada una de las actividades:

- ¿ Cómo podría ejecutarse esta actividad en forma diferente o aun ser eliminada?
- ¿ Cómo puede reordenarse este grupo de actividades relacionadas?
- ¿ Cómo podrán las alianzas reducir los gastos o incluso eliminar costos?

Los líderes exitosos en el costo frecuentemente obtienen su ventaja de múltiples fuentes dentro de la cadena de valor, las cuales interactúan y se refuerzan

entre sí. De hecho, esto hace difícil y costoso que los competidores puedan alcanzar su posición competitiva en el costo y por lo tanto incrementará su permanencia como líder.

4. La diferenciación

La diferenciación es el otro tipo de ventaja competitiva además de la ventaja en el costo. Muchas veces, a pesar de su importancia, las formas para diferenciarse no son bien entendidas. Las organizaciones frecuentemente se limitan a considerar la diferenciación como el producto físico o las funciones de mercadotecnia; en lugar de considerar todos los componentes de la cadena de valor como fuente de diferenciación.

Factores que determinan la diferenciación

El hecho de que una actividad de valor sea única está determinado por una serie de factores básicos, similares a los factores que influyen en el costo. El profesor Porter identifica los siguientes factores de diferenciación, en orden de importancia:

- Políticas elegidas (por ejemplo, características del producto, tecnología empleada y calidad de los elementos empleados para una actividad).
- Ligas (ligas dentro de la cadena de valor, con los proveedores o con el canal de distribución).
- Oportunidad (por ejemplo, ventajas de ser el pionero).
- Localización (en términos de conveniencia para el comprador).
- Interrelaciones (por ejemplo, mejores servicios al compartir fuerza de ventas de diferentes segmentos de negocio tales como seguros o con algunos otros servicios financieros).
- Capacitación (la capacidad para realizar mejor una actividad).
- Integración (la capacidad para controlar y coordinar mejor la ejecución de nuevas actividades de valor que se estén integrando).
- Escala (una mayor conveniencia para el comprador debido al tamaño o escala, como por ejemplo el número de sucursales bancarias).

La capacitación es un factor de diferenciación.

- Factores institucionales (buenas relaciones con los sindicatos pueden permitir que una organización establezca definiciones de puestos únicas).

El costo de la diferenciación

En ocasiones, hacer que una actividad sea única puede bajar el costo al mismo tiempo. Tal es el caso de la integración. Un ejemplo de lo anterior podrá ser una mejora en la coordinación de cotizaciones, adquisiciones y programación de la producción, lo cual permite disminuir el costo del inventario al mismo tiempo que se disminuye el tiempo de entrega.

Valor del comprador y diferenciación

Una organización puede diferenciarse de sus competidores cuando logra ser única en algo que tiene valor para sus compradores. El punto de partida para poder conocer qué tiene valor para el comprador es la cadena de valor del comprador.

Una empresa puede crear valor para su comprador mediante dos mecanismos:

- Disminuyendo el costo del comprador.
- Aumentando la ejecución del comprador.

Durante la búsqueda de la diferenciación, es importante conocer cuáles son los criterios de compra del comprador; éstos pueden dividirse en dos categorías: Criterios de uso y Criterios de señalización.

Los criterios de uso son mediciones específicas de lo que crea valor para el comprador. Los criterios de señalización son mediciones sobre cómo los compradores perciben el valor.

Los criterios de uso son mediciones específicas de lo que crea valor para el comprador. Los criterios de señalización son mediciones sobre cómo los compradores perciben el valor.

Mientras que los criterios de uso (los cuales normalmente se derivan de las ligas entre la cadena de valor de la organización y la cadena de valor de su comprador) tienden a orientarse más al producto del proveedor, a la logística de salida y a las actividades de servicio; los criterios de señalización a menudo se derivan mayormente de las actividades de mercadotecnia.

Enfoques para lograr una diferenciación exitosa

Los enfoques para poder lograr una diferenciación exitosa incluyen:

- Fortalecer las fuentes que generan la diferenciación:

  - Conseguir que el producto sea consistente con el uso que se pretende.
  - Utilizar señales de valor para reforzar la diferenciación en los criterios de uso.
  - Utilizar la información empaquetada con el producto para facilitar tanto su uso como señalización.
  - Hacer énfasis en las formas de diferenciación en las que la organización tiene alguna ventaja sostenible en el costo.
  - Reducir el costo en las actividades que no afecten al valor del comprador.

- Cambiar las reglas para crear que el producto o servicio sean únicos.

  ➢ Descubrir criterios de compra desconocidos.
  ➢ Responder a circunstancias de cambio del comprador o del canal.

- Reconfigurar la cadena de valor para lograr que sea única en formas completamente nuevas tales como:

  ➢ Un nuevo canal de distribución ó enfoque de ventas.
  ➢ Integración para controlar algunas funciones del comprador o para eliminar los canales de distribución.

El grado en que la diferenciación será sostenible dependerá de dos aspectos: el valor continuo percibido por sus compradores y la falta de imitación por parte de los competidores. La diferenciación será más sostenible bajo las siguientes circunstancias:

- Las fuentes de diferenciación involucran barreras.
- La organización posee alguna ventaja en el costo como diferenciador.
- Se cuenta con múltiples fuentes de diferenciación.

La tecnología y la ventaja competitiva

La cadena de valor es una buena herramienta para poder comprender el papel que juega la tecnología dentro de la ventaja competitiva. La tecnología de los sistemas de información influye directamente en la cadena de valor, ya que cualquier actividad de valor crea y utiliza información. Los sistemas de información se utilizan para programar, controlar, optimar, medir y de alguna u otra forma, para realizar ciertas actividades. La tecnología de los sistemas de

información también juega un importante papel en las ligas entre varios tipos de actividades, ya que para la coordinación y el aprovechamiento de las ligas se requieren flujos de información entre las actividades.

La tecnología afecta la ventaja competitiva siempre y cuando tenga un rol preponderante para determinar la posición competitiva en el costo o en la diferenciación.

La tecnología afecta la ventaja competitiva siempre y cuando tenga un rol preponderante para determinar la posición competitiva en el costo o en la diferenciación.

Los cambios tecnológicos en una organización pueden lograr una ventaja competitiva sostenible bajo las siguientes circunstancias:

- El mismo cambio tecnológico permite disminuir los costos o promueve la diferenciación; además, el liderazgo tecnológico de la organización es sostenible.
- El cambio tecnológico cambia los factores que determinan el costo o los factores que determinan la diferenciación a favor de la organización.
- Cuando se es el pionero en algún cambio tecnológico se generan ciertas ventajas, además de las ventajas del cambio tecnológico mismo.
- El cambio tecnológico mejora totalmente la estructura de una determinada industria (por ejemplo, los cajeros automáticos).

Reingeniería en las organizaciones

La razón por la que una gran cantidad de los procesos de las empresas no soportan adecuadamente la misión y estrategia de sus respectivos negocios (ni las necesidades de sus clientes por consiguiente) puede deberse a dos causas principales.

La primera es que el tiempo en el que se estructuró el negocio fue distinto a aquel en el que actualmente opera la empresa. Por lo tanto, sus descripciones de puestos, flujos de trabajo, mecanismos de control y aun su estructura de organización, podrán ya no ser los más adecuados para responder a un mercado que demanda innovación, rapidez, servicio y calidad.

La segunda es que quizás durante la creación del negocio no se realizó un proceso integrado de estructuración del mismo, sino que únicamente se respondió ante un crecimiento en las transacciones, lo cual originó el crecimiento en la estructura y el personal que maneja los procesos.

Muchos directivos de empresas han concluido que una manera práctica de responder ante estos retos es romper con viejos paradigmas y métodos de conducir el negocio, en primer lugar reconociéndolos como tales y en algunos casos eliminándolos, a la vez que se encuentran nuevas formas de responder ante nuevas demandas.

La reingeniería de procesos o el rediseño e implantación de nuevos procesos tiene su fundamento en un pensamiento discontinuo que permite reconocer y romper los viejos esquemas que dominan la operación.

Cuando se automatizan los procesos actuales o se realizan esfuerzos para disminuir la cantidad de personal, sin realizar un cuestionamiento de los esquemas o reglas actuales, es imposible lograr mejoras sustanciales; únicamente se reacomodan los mismos elementos.

Otra situación que aflora con respecto a los procesos existentes es la falta de integración necesaria para mantener una calidad y nivel de servicio adecuados. Las unidades, funciones o departamentos definen objetivos particulares en lugar de seguir un objetivo común. Cuando el trabajo está dividido entre varios departamentos, la posibilidad de errores o retrasos es en muchos casos inevitable, y más aun, ninguna persona en la organización cuenta con un panorama completo de los procesos, de tal forma que se pueda responder de manera oportuna ante nuevas situaciones.

Cuando el trabajo está dividido entre varios departamentos, la posibilidad de errores o retrasos es en muchos casos inevitable,

Una de las más importantes características de la reingeniería es que analiza los procesos con una perspectiva integral desde el punto de vista funcional, enfocándose principalmente al cliente de cada proceso y no a la separación de funciones que quizás fueron creadas para crear una división y especialización en el trabajo.

Algunos de los principios que las empresas han descubierto mientras conducen la reingeniería de sus procesos, y que pudieran guiar a otras organizaciones incluyen los siguientes:

- Eliminar actividades sin valor agregado.
- Organizarse alrededor de resultados en lugar de funciones o tareas.
- Buscar que el usuario del resultado de un proceso sea quien efectúe el proceso.
- Obtener la calidad y captar la información desde la fuente.
- Considerar los recursos geográficamente dispersos como si fueran centralizados.
- Estandarizar los procesos basándose en prácticas líder de la industria "best practices".
- Promover la creación de puestos multifuncionales.
- Localizar puntos de decisión en quien realiza el trabajo y construir el proceso con controles integrados.
- Utilizar métodos visuales para el control de los procesos.
- Reducir el tiempo de preparación.
- Utilizar procesos en paralelo.
- Establecer relaciones y acuerdos con proveedores y clientes.
- Aplicar la automatización y la tecnología aplicable.
- Construir una capacidad y mentalidad de mejora continua.

Eliminar actividades sin valor agregado. Considerando actividades de valor agregado a aquello que el cliente quiere y está dispuesto a pagar, y eliminando aquello por lo que no desea pagar, por ejemplo, actividades relacionadas con el transporte, la espera, la preparación, el almacenamiento o el reproceso.

Organizarse alrededor de resultados en lugar de funciones o tareas. El personal, los procesos y el trabajo deben organizarse para producir y facilitar lo que el cliente desea, por lo cual es posible que sea necesaria la integración de equipos de trabajo de varias funciones de la empresa en forma permanente, reduciendo así, actividades sin valor agregado entre varios departamentos, tales como transporte de información y de recursos o tiempos de espera y de consulta. El objetivo es reducir tiempos de ejecución, mejorar la comunicación y enriquecer el proceso con un grupo multifuncional.

Buscar que el usuario del resultado de un proceso sea quien efectúe el proceso. La existencia de áreas o departamentos especializados en un tipo de trabajo (por ejemplo: compras, servicio o proceso de información) ha originado que estas áreas tengan sus propios clientes dentro de la misma organización. La idea es hacer un mayor uso y aprovechamiento de las herramientas automatizadas y buscar que el personal que utiliza el resultado de un proceso, también lo efectúe; con esto se logra una disminución de las interrelaciones y esfuerzos de coordinación entre el que lo utiliza y el que lo efectúa.

Obtener calidad y capturar la información desde su origen. La identificación de las partes del proceso donde ocurren los errores y su rediseño, con el objeto de eliminar la posibilidad de que sigan ocurriendo; elimina la existencia de actividades sin valor agregado tales como revisiones, segundas opiniones, aprobaciones y auditorias de calidad.

Considerar los recursos geográficamente dispersos como si fueran centralizados. La descentralización de recursos (ya sea personal, equipo o inventario) proporciona un mejor servicio para aquellos que los utilizan, pero con un costo por redundancia, en algunas ocasiones burocracia, y en otras, la falta de aprovechamiento eficiente de los recursos centrales. Lo que se busca con este principio es el aprovechamiento de la tecnología (bases de datos, telecomunicaciones y sistemas) para lograr un equilibrio entre los beneficios derivados del servicio y la flexibilidad, con el uso eficiente de los recursos.

Estandarizar los procesos basándose en prácticas líder de la industria. Este principio involucra la investigación para identificar los procesos que utilizan las empresas del mismo ramo y asegurarse de que los procedimientos, la capacitación y el esquema de remuneración sean adecuados conforme dichas prácticas.

Promover la creación de puestos multifuncionales. La existencia de este tipo de puestos permite la sustitución en caso de ausencias o cuellos de botella, además de incidir en el nivel de motivación y satisfacción del personal.

Localizar los puntos de decisión en quien realiza el trabajo y construir el proceso con controles integrados. Se busca cambiar del concepto de dividir el trabajo entre aquellos que lo efectúan y aquellos que los supervisan y toman decisiones, por el de procurar que el personal que efectúe el trabajo tome las decisiones inherentes; siempre y cuando se cuente con controles integrados.

Utilizar métodos visuales para el control de los procesos. Dichos métodos permiten tanto a la gerencia como al personal, contar con la información que necesitan para tomar decisiones oportunas y completas. Además de ser un factor de motivación para lograr objetivos en la ejecución del trabajo.

Utilizar flujos de trabajo sobre demanda y manejo de lotes pequeños. Este principio indica que solo debe iniciarse la producción de un producto, información o servicio cuando se conozca la demanda. Este tipo de flujo de trabajo también involucra el manejo de lotes o cantidades lo suficientemente pequeños para ser manejables en una forma eficiente. Además, se incluye el manejo de medios físicos y visibles para indicar la existencia de demanda; los cuales pueden variar desde el simple uso de charolas de entrada, hasta la utilización de un menú automatizado que guíe las acciones.

Reducir el tiempo de preparación. Se considera el tiempo dedicado a la preparación de alguna actividad como sin valor agregado; aún cuando la actividad sí tenga valor agregado. Se puede hacer un uso más eficiente del tiempo si se logran eliminar actividades dedicadas a la preparación.

Utilizar procesos en paralelo. Se utiliza este tipo de procesamiento cuando el cliente requiere un producto o servicio que dependa de los resultados de dos o más procesos, y éstos pueden ejecutarse en paralelo en lugar de secuencialmente. Es importante cuidar que exista la coordinación necesaria entre las actividades que se efectúan en paralelo, a lo largo de los procesos y no sólo al final de ellos.

Establecer relaciones y acuerdos con proveedores y clientes. Este principio consiste en enfocarse a una cantidad reducida tanto de proveedores y clientes seleccionados, con los que sea posible la construcción de relaciones estratégicas que permitan ciclos de proceso reducidos, costos menores, menor consumo de recursos y mejor tiempo de respuesta hacia el mercado.

Aplicar la automatización y la tecnología aplicable. El criterio sobre el que se basa la automatización de procesos es el de actividades con valor agregado

que por sus características (de cierto volumen, repetitivas, con pocos requerimientos de creatividad y capacidad intelectual), pueden y deben automatizarse. Otra de las ventajas de la automatización son: el soporte que brinda a varias funciones o departamentos para poder efectuar un proceso integrado, el soporte para la toma de decisiones y el apoyo para el flujo de comunicaciones. Sin mencionar la reducción de costos asociados con la disminución de esfuerzos de coordinación que trae consigo la automatización.

Construir una capacidad y mentalidad de mejora continua. Este principio se basa en la convicción de que cualquier producto o proceso puede mejorarse sin importar qué tan bueno sea o por cuanto tiempo se ha estado procesando o produciendo de esa manera. El mejor recurso para lograr el cumplimiento de este principio es la involucración del personal, y esto requiere de liderazgo de la dirección en ese sentido, cooperación, motivación, respeto mutuo y capacitación.

Cualquier producto o proceso puede mejorarse sin importar qué tan bueno sea o por cuanto tiempo se ha estado procesando.

Bibliografía

Bernard C. Reimann, (1989) "Sustaining the Competitive Advantage," *Planning Review*, March/April.

Cash James I. Jr., F. Warren McFarlan y James L. McKenney, (1988) *Corporate Information Systems Management*, Dow Jones-Irwin, EE:UU.

Hammer Michael; (1990) "Reengineering Work : Don't Automate, Obliterate," *Harvard Business Review*, July/August.

Porter Michael (1985), *Competitive Advantage*, Free Press, EE.UU.

Rockart John F (1979), "Chief Executives Define Their Own Data Needs," *Harvard Business Review*, March-April.

Rusell L Ackoff (1994) "Función de los negocios en una sociedad democrática", en *El MBA portátil*, Eliza G.C. Collins, Mary Anne Devanna, Editorial Limusa, México.

Tema 2. Rediseño de los procesos para su automatización

Por Ricardo Loranca González

Resumen

La aplicación de la tecnología de información en la cadena de valor de una entidad puede ayudar al logro de ventajas competitivas, ya que cualquier actividad dentro de la cadena puede requerir información.

Un problema común en las organizaciones es la falta de información adecuada para operar exitosamente los procesos. Es por ello que es importante conocer los distintos enfoques para el desarrollo de sistemas de información automatizados: desde el enfoque en el que los directivos prefieren no hacer uso de información generada por sistemas automatizados, hasta el enfoque en el que se automatizan totalmente los requerimientos de información de los directivos.

En la continua búsqueda para hacer más eficiente el desarrollo de aplicaciones automatizadas, surge el enfoque de desarrollo a través de factores críticos de éxito. Este enfoque consiste en entrevistar a los directivos de la organización para identificar y seleccionar solo aquellos aspectos importantes que deben marchar bien para el funcionamiento de los procesos a su cargo. Estos aspectos se sustentan siempre sobre decisiones clave que el directivo debe tomar, así como de medidores de desempeño que permitirán evaluar la operación del factor crítico de éxito.

Tema 2. Rediseño de los procesos para su automatización

Por Ricardo Loranca González

Introducción

Un método tradicional para mejorar la ejecución de las operaciones en las organizaciones ha sido la automatización. Sin embargo, en algunos casos, a pesar de las grandes inversiones realizadas, los resultados son poco favorables.

Esta situación puede atribuirse a dos causas principales:

- La automatización se aplica a formas tradicionales de operar el negocio.
- Las necesidades de información se definen utilizando un enfoque inadecuado.

En el primer caso únicamente se automatizan y aceleran los procesos actuales, por lo que éstos permanecen prácticamente intactos.

Es importante reconocer que muchos de los flujos de trabajo, mecanismos de control, descripciones de puestos y aun estructuras organizacionales, probablemente fueron estructurados en un tiempo distinto al de la aparición de nuevas herramientas automatizadas, en un ambiente competitivo distinto al que prevalece actualmente, y en el que la innovación, la rapidez, el servicio y la calidad representan cualidades indispensables para el éxito.

Es importante que antes de buscar la automatización de procesos que pudieran no responder ya a las necesidades actuales, se realice un ejercicio de reingeniería de procesos.

Es importante que antes de buscar la automatización de procesos que pudieran no responder ya a las necesidades actuales, se realice un ejercicio de reingeniería de procesos. De esta forma, el desarrollo de los sistemas se efectúa sobre procesos rediseñados, lo cual asegura que los sistemas serán utilizados para mejorar la ejecución de actividades que realmente proporcionan valor agregado.

La segunda causa de que los esfuerzos de automatización no produzcan

resultados favorables, es la definición de las necesidades de información utilizando un enfoque inadecuado.

En estos casos, los síntomas son fácilmente identificables al medir el grado de satisfacción de los niveles directivos con respecto a sus necesidades de información. Es frecuente que dichos niveles requieran una gran cantidad de reportes e información para soportar sus decisiones, y que sus necesidades de información no se encuentren claramente definidas.

Ejercicio: Enfoques de desarrollo de sistemas

A continuación se presenta un ejercicio que le permitirá tener un panorama general de los distintos enfoques de desarrollo de sistemas tradicionales, y que a su vez le servirá como base para poder comprender mejor un nuevo enfoque de desarrollo titulado "factores críticos de éxito".

En los siguientes puntos se presenta la descripción de cinco enfoques de desarrollo distintos; una vez que los haya comprendido, por favor relaciónelo con la lista de enfoques que se presenta al final del ejercicio:

1. *En esta técnica se da prioridad a las necesidades operativas que representan mayor carga de trabajo manual (nóminas, cuentas por cobrar, inventarios, etc.), más que a los requerimientos de información ejecutiva.*

2. *Este enfoque se deriva de la opinión de aquellos directivos que basan sus decisiones en la comunicación oral y en opiniones de miembros de su equipo de trabajo ; los cuales en muchos casos son subjetivas.*

3. *Este enfoque se basa en dos concepto :*

    - *El primero es la selección de medidores clave sobre el estado del negocio.*

    - *El segundo es la administración por excepción; es decir, hacer llegar al directivo solo aquellos indicadores en los que su ejecución es distinta a la esperada.*

4. *Consiste en seleccionar una muestra de directivos e identificar sus requerimientos de información, dichos requerimientos son comparados con la situación actual, y las necesidades no satisfechas se conjuntan y priorizan en subsistemas por desarrollar. Este proceso es costoso y largo en términos de recursos y tiempo requeridos, y muy amplio en términos de alcance.*

[ ] ENFOQUE NULO

[ ] TÉCNICA POR PRODUCTO

[ ] ENFOQUE A TRAVÉS DE INDICADORES

[ ] PROCESO DE ESTUDIO TOTAL

Existe un nuevo enfoque para lograr la definición de necesidades de información a nivel ejecutivo de una forma más precisa y práctica.

Este enfoque lo constituye el estudio de los "Factores críticos de éxito": "Los sistemas de información deben ser selectivos, deben estar enfocados hacia factores de éxito, En la mayoría de las industrias y empresas existe un número limitado de entre tres y seis factores que determinan su éxito".

Los factores críticos de éxito son aquellas áreas en las que es indispensable una buena ejecución para asegurar el logro de los objetivos de la empresa.

Los factores críticos de éxito son aquellas áreas en las que es indispensable una buena ejecución para asegurar el logro de los objetivos de la empresa.

Algunas de las ventajas de este nuevo enfoque son:

- El tiempo y esfuerzo tanto para su definición como para su desarrollo es menor, debido a su enfoque selectivo de lo "crítico".
- Puede aplicarse a cualquiera de los niveles gerenciales sin desatender ninguno.
- Ayuda a los gerentes a determinar sobre qué factores debe concertar su atención.
- Promueve la creación de medidores de ejecución efectivos para cada uno de los factores críticos de éxito, por lo que los gerentes buscan la creación de reportes y consultas específicas sobre dichos medidores.
- Se logra una definición clara de la cantidad de información que se procesará y se limita el procesamiento de datos e información innecesaria.

Ejemplos de factores críticos de éxito

Aun cuando los factores críticos de éxito pueden aplicarse a cualquier nivel gerencial, para poder ilustrar su utilización práctica, presentamos un ejemplo de factores críticos de éxito definiéndolo a nivel de proceso del negocio.

- Organización ..... (Compañía ABC)
  - Función de negocio ..... (Finanzas)
    - Proceso de negocio ..... (Compra)
      - Función de procesamiento..... (Levantamiento de órdenes de compra)

En este caso, uno de los factores de éxito para el proceso de compras podría ser:

"Mantener un nivel de inventario consistente para poder ofrecer a las áreas usuarias un 95% de nivel de surtimiento".

En adición al factor crítico de éxito, el gerente necesitará un medidor de desempeño que le permitirá evaluar qué tan bien se está realizando la función. De esta forma, el medidor de desempeño para el ejemplo mencionado sería:

Factor crítico de éxito:

Mantener un nivel de inventario consistente para poder ofrecer a las áreas usuarias un 95% de nivel de surtimiento.

Medidor de desempeño:

El porcentaje de requisiciones de material que no fueron surtidas.

Un tercer elemento de apoyo al gerente para poder cumplir con el factor crítico de éxito son las decisiones clave. Las decisiones clave serán aquellas que deberá tomar adecuadamente para el logro del factor crítico, y se representan en forma de preguntas:

Factor crítico de éxito:

Mantener un nivel de inventario consistente para poder ofrecer a las áreas usuarias un 95% de nivel de surtimiento.

Medidor de desempeño:

El porcentaje de requisiciones de material que no fueron surtidas.

Decisiones clave:

- ¿ Cuándo reordeno?
- ¿ Cuánto reordeno?

Un último elemento complementario al factor crítico de éxito y que será utilizado por el gerente tanto para soportar sus decisiones clave como para identificar su medidor de desempeño, lo constituyen las funciones de procesamiento, y se presentan en forma de reportes (o consultas) con que deberá contar el sistema automatizado:

Factor crítico de éxito:

Mantener un nivel de inventario consistente para poder ofrecer a las áreas usuarias un 95% de nivel de surtimiento.

Medidor de desempeño:

El porcentaje de requisiciones de material que no fueron surtidas.

Decisiones clave:

- ¿ Cuándo reordeno?
- ¿ Cuánto reordeno?

Funciones de procesamiento:

- **Reporte de frecuencia de compra por producto**. Este reporte deberá mostrar con que periodicidad se emiten órdenes de compra para un determinado producto, y permitirá al gerente prevenir la frecuencia con que debe reordenar compras del producto ¿Cuándo reordeno?
- **Reporte de niveles de inventario bajos.** Este reporte permitirá que se identifiquen aquellos productos de los que se tiene muy poca existencia, para poder generar órdenes de compra, ¿cuándo reordeno? Si se toma el nivel óptimo de existencia se podrá determinar también la cantidad por comprar de cada producto ¿Cuánto reordeno?.
- **Reporte de tiempos de entrega**. En este reporte, el gerente podrá combinar la información de los reportes anteriores para considerar el tiempo que el proveedor tarda en surtir los productos y generar anticipadamente las órdenes de compra ¿Cuándo reordeno?
- **Reporte de porcentaje de requisiciones de material que no fueron surtidas**. Este reporte es básicamente el elemento base para que el gerente pueda identificar el medidor de desempeño del factor critico de éxito.

Con el objeto de que usted pueda reafirmar los conceptos de factor crítico de éxito, decisión clave y función de procesamiento; a continuación se presenta otro ejemplo:

Factor crítico de éxito:

Reducir y mantener el valor del inventario a x millones.

Medidor de desempeño:

El valor del inventario.

Decisiones clave:

- ¿Qué almaceno?
- ¿Cuánto almaceno?

Funciones de procesamiento:

- Reporte de valuación del inventario con clasificación ABC. Este reporte permitirá clasificar los productos de forma que el gerente pueda identificar cuáles son los productos más importantes para la organización, tanto en su utilización como en su costo. De esta forma podrá decidir de qué productos debe mantener una mayor o menor existencia, ¿Qué almaceno? y ¿Cuánto almaceno? Por otra parte, la valuación total de las existencias permitirá identificar el medidor de desempeño - el valor de inventario.

- Reporte de productos con lentos movimientos. Este reporte permitirá identificar aquellos productos que no son requeridos frecuentemente y que por lo tanto no requieren almacenarse en grandes cantidades, ¿Qué almaceno?, ¿Cuánto almaceno?

De todo lo anterior podemos concluir que los desarrolladores de aplicaciones pueden ser mucho más efectivos y precisos al desarrollar los componentes de sus sistemas utilizando como base el esquema de factores críticos de éxito/ medidores de desempeño/decisión clave/función de procesamiento.

Análisis de riesgo/retorno del desarrollo de aplicaciones

Planes como portafolios. Existe una razón por la que los planes estratégicos del desarrollo de aplicaciones deberían manejarse como un portafolio financiero:

El plan estratégico de sistemas debiera balancear el riesgo y el retorno de la inversión de cada proyecto.

El plan estratégico de sistemas debiera balancear el riesgo y el retorno de la inversión de cada proyecto.

Portafolios de riesgo y retorno de la inversión

Al nivel de un segmento de la organización, no todos los proyectos del plan estratégico de desarrollo de aplicaciones tienen una misma prioridad en cuanto al tiempo, o para la asignación de recursos. Como una excepción, lo anterior no aplica para aquellas aplicaciones obligatorias, ni para el mantenimiento ni la mejora de aplicaciones esenciales.

Los demás proyectos (ver la figura 1) pueden tener diferentes retornos de la inversión, riesgos y calendarios.

FIGURA. 1

Alto	Proyectos de alto rendimiento	Proyectos de esfuerzo y riesgo
RETORNO DE LA INVERSION		
Bajo	Proyectos base	Proyectos sin rendimiento
	Corto plazo	*Largo plazo*

CONSECUCION DE OBJETIVOS

Es necesario, desde un punto de vista racional y político, dar forma al plan estratégico de aplicaciones para que se convierta en un conjunto de resultados a través el tiempo, sin necesidad de incurrir en demasiados riesgos.

La función de la tecnología de información y la organización requieren tener una serie de desarrollos de aplicaciones estables que puedan ser lo suficientemente planeadas e implantadas, que puedan ser percibidos como un proceso continuo y que permitan acumular la experiencia necesaria. Al mismo tiempo, deben obtenerse algunos logros sustantivos así como innovaciones para conseguir beneficios y motivar al personal profesional.

De tal forma, el plan estratégico de desarrollo de aplicaciones debe convertirse en un portafolio que genere un flujo constante de resultados año con año, a la vez que proteja a la organización de riesgos inherentes al desarrollo.

El plan estratégico de desarrollo de aplicaciones debe convertirse en un portafolio que genere un flujo constante de resultados año con año.

El formato de la figura 1 responde a dos preguntas:

- ¿ Cuál es la ganancia de la propuesta del sistema? Esta pregunta puede responderse de forma cuantitativa o cualitativa, siempre y cuando se trate de retorno de la inversión o beneficios.

- ¿En cuánto tiempo se alcanzarán los objetivos? Esta pregunta representa una evaluación de los riesgos, calendarios y dificultades, integrándolos como una sola medida.

A continuación se explican cada uno de los casos de desarrollo representado en cada cuadrante de la figura 1:

- **Proyectos de alto rendimiento**. Estos proyectos son esenciales para la implantación de cualquier estrategia de sistemas de información. El área de tecnología de la información requiere de la obtención de logros para mantener o ganar credibilidad; de esta manera se influye de forma positiva sobre la dirección de la organización.

Cualquier plan estratégico de desarrollo de sistemas incluirá al menos un proyecto de alto rendimiento.

Cualquier plan estratégico de desarrollo de sistemas incluirá al menos un proyecto de alto rendimiento.

- **Proyectos base**. Este tipo de proyectos también es de vital importancia. El área de tecnología de información debe presentar una imagen de servicio a través de la entrega periódica de sistemas que representan un gran esfuerzo a mediano o largo plazo.

- **Proyectos de esfuerzo**. Estos proyectos no son muy comunes: si una aplicación verdaderamente va a generar ventaja competitiva, lo más probable es que se trate de mercados competitivos maduros en los que habrá dificultades o riesgos durante su implantación. Si no fuera así, los competidores ya la habrán desarrollado. Por lo tanto, muchos sistemas estratégicos pueden generar potencialmente altos rendimientos, pero involucran riesgos considerables. Una organización en busca de ventaja competitiva en el área de tecnología de información, deberá estar desarrollando al menos un proyecto de este tipo.

- **Proyectos sin rendimiento**. Estos proyectos quizás no deberían incluirse dentro de la elaboración de planes estratégicos de sistemas. Sin embargo, durante el análisis para la planeación detallada de los sistemas puede

determinarse que lo que inicialmente constituía una buena idea, resulta ser un proyecto con un retorno de inversión modesto o un proyecto muy complejo. Lo ideal será posponer la realización de estos proyectos hasta que las circunstancias cambien y la relación riesgo/retorno cambie.

Bibliografía

Bernard C. Reimann, (1989) "Sustaining the Competitive Advantage," *Planning Review*, March/April.

Cash James I. Jr., F. Warren McFarlan y James L. McKenney, (1988) *Corporate Information Systems Management*, Dow Jones-Irwin, EE:UU.

Hammer Michael; (1990) "Reengineering Work : Don´t Automate, Obliterate," *Harvard Business Review*, July/August.

Porter Michael (1985), *Competitive Advantage*, Free Press, EE.UU.

Rockart John F (1979), "Chief Executives Define Their Own Data Needs," *Harvard Business Review*, March-April.

Rusell L Ackoff (1994) "Función de los negocios en una sociedad democrática", en *El MBA portátil*, Eliza G.C. Collins, Mary Anne Devanna, Editorial Limusa, México.

Tema 3. El desarrollo organizacional en el cambio

Por Ricardo Loranca González

Resumen

La parte final de un ejercicio de reingeniería de procesos la constituyen, por una parte, el diseño de los otros componentes de la organización, (estructura, perfiles de puestos, localidades, etc.) una vez que los procesos fueron rediseñados; y por otra, las actividades que apoyarán el trabajo de implantación de los nuevos componentes (la capacitación o la conducción de actividades de transición y aceptación del cambio).

Un aspecto relevante que debe ser tomado en consideración al estar realizando el rediseño de esos componentes de la organización es que el factor humano cuenta actualmente con un mayor desarrollo y capacidades que en épocas anteriores, en las que quizás fueron concebidas muchas de las organizaciones; en ellas se requería especialización en ciertas funciones rutinarias y limitadas, y las decisiones, la supervisión y el control, siempre corrían a cargo de mandos intermedios.

La idea es buscar hacer un mayor y mejor uso de las capacidades del personal; quizás no sacrificar el control en pro de la eficiencia, sino buscar, en la medida de lo posible, que las mismas actividades del personal sean autocontroladas.

Tema 3. El desarrollo organizacional en el cambio

Por Ricardo Loranca González

Una vez que los procesos de la organización han sido rediseñados, el rediseño y la reestructuración de las otras dimensiones que la componen, tales como la estructura, el personal y la cultura, serán más eficientes, ya que estarán enfocados también a brindar soporte directo a la misión y estrategia redifinidas.

El desarrollo organizacional

El desarrollo organizacional cubre las dimensiones de: estructura de organización, personal y cultura, las cuales representan un complemento a la reingeniería de procesos. El desarrollo organizacional se logrará a través de la definición e implantación de proyectos en lo relativo a:

El desarrollo organizacional cubre las dimensiones de: estructura de organización, personal y cultura,

- Estructura de organización
- Diseño de puestos
- Políticas y procedimientos
- Actividades de transición y aceptación del cambio
- Programa de capacitación sobre nuevos procesos

Estructura de Organización

La estructura de organización incluye la organización de las unidades del negocio que soportarán la ejecución de los nuevos procesos. Esta definición se realiza mediante la asignación de la responsabilidad de cada proceso a una o varias unidades del negocio. De esta forma se obtiene una estructura en la que la evaluación de la organización estará directamente ligada a la ejecución de los procesos.

Cualquier estructura organizacional también debe ser flexible y basarse en resultados.

Es importante tomar en cuenta que cualquier estructura organizacional, (unidad, sub-unidad, o equipo) en la cual esté dividida la organización, también debe ser flexible y basarse en resultados, más que en funciones.

Además, debe poder adaptarse, reorganizarse o aun eliminarse dependiendo de los cambios del ambiente externo de la organización (cambios en el mercado ó en los usuarios de sus productos de servicios).

Diseño de puestos

El diseño de puestos se realiza mediante la agrupación de las tareas de un proceso, en descripciones y perfiles de puestos, de tal forma que al igual que la estructura de organización, los parámetros de evaluación de los procesos también son comunicados y medidos a nivel del personal.

El diseño de puestos se realiza mediante la agrupación de las tareas de un proceso.

Un concepto clave que debe tomarse en cuenta durante el rediseño de puestos para cubrir los nuevos procesos, es la facultación de los empleados.

La *facultación* de los empleados es el término que representa un cambio verdadero del poder a los empleados para poder controlar tanto sus actividades laborales, como para responsabilizarse de las mismas.

Una organización cuyo cometido es facultar a sus empleados, tendrá puestos en los cuales el personal de primera línea será mayormente tomado en cuenta y tendrá responsabilidades para un mayor número de decisiones críticas. Este tipo de empleados disfrutará de un mayor nivel de autonomía para poder administrar tanto sus tareas, como el personal de sus equipos de trabajo.

Es importante que los puestos se rediseñen de forma que resulten lo más interesante y con los mayores retos posibles. Esto requerirá no sólo especificar el puesto, sino también definir los requerimientos de la persona que cubrirá el mismo.

Es importante que los puestos se rediseñen de forma que resulten lo más interesante y con los mayores retos posibles.

Algunos de ustedes se sorprenderán al escuchar conceptos como el de *facultación* de los empleados; quizás pensarán que su organización aún no está lista para otorgar a sus empleados "tantas" capacidades. Es por ello que se consideró importante presentar el siguiente extracto de la lectura "Función de los negocios en una sociedad democrática" del autor Russell L. Ackoff; en dicho extracto, se presentan algunas ideas que pudieran sustentar la decisión de una organización para realizar un cambio de ese tipo durante el diseño de sus puestos:

> *Crecimiento y desarrollo no son lo mismo. De hecho, ninguno de ellos requiere al otro. Un montón de basura crece, pero no se desarrolla, y una persona puede desarrollarse sin hacerse de mayor tamaño. El crecimiento es un aumento en el tamaño o en el número. El desarrollo es un aumento en la habilidad y el deseo de satisfacer los deseos y las necesidades legítimas de uno mismo y de los demás. Un deseo legítimo es aquel cuya satisfacción no reduce o retarda el desarrollo de otro.*

Los objetivos y los sistemas sin un propósito pueden crecer, pero no pueden desarrollarse, solo los individuos y los sistemas que cuentan con un propósito pueden desarrollarse.

El desarrollo es un aumento en la capacidad y el potencial, no un aumento en logros. Se trata más de aprender que de ganar. Se refiere menos a lo que se tiene y más a lo que se puede hacer con lo que se tiene. Esta es la razón por la que Robinson Crusoe y la Familia Robinson son mejores modelos de desarrollo que John D. Rockefeller o J. Pierpont Morgan; y por qué el desarrollo implica más la calidad de la vida que el nivel de vida. Si se entrega riqueza a un pueblo subdesarrollado no por ello pasa a ser desarrollado. Por otra parte, si se les educa, se ayuda a su desarrollo, incluso sin aumentar su riqueza.

El desarrollo es un aumento en la capacidad y el potencial, no un aumento en logros.

El desarrollo implica más la calidad de la vida que el nivel de vida.

Debido a que el desarrollo consiste tanto en un deseo como en una habilidad, no resulta posible imponerlo o darlo a una persona u organización. Un gobierno no puede desarrollar a los gobernados; y una corporación no puede desarrollar a sus empleados, ni siquiera a sus administradores. El único tipo posible de desarrollo es el autodesarrollo. Una persona u organización puede sin embargo, animar y facilitar el desarrollo de otros.

Los niveles de vida pueden aumentar a costa de la calidad de la vida y la calidad de la vida puede aumentar sin aumento en el nivel de vida - en realidad con un descenso en éste. No quiere esto significar que la riqueza no tiene relación con el desarrollo de la calidad de la vida; la relación es grande. La forma en que muchas personas pueden aumentar realmente su calidad de vida y la de otros no depende sólo de sus capacidades, sino de los recursos de que dispone. Se puede construir una casa mejor con buenas herramientas y materiales, que con herramientas y materiales deficientes. Por otra parte, una persona bien desarrollada puede construir una casa mejor que otra persona menos desarrollada, aunque ambos dispongan de la misma calidad de herramientas y de materiales. La calidad de vida que pueden alcanzar las personas es el producto conjunto de su desarrollo y de la cantidad y calidad de los recursos de que dispongan.

Unos recursos limitados pueden limitar el crecimiento, pero no el desarrollo. Cuanto más desarrollado sea un individuo, menos será lo que lo limiten los recursos disponibles. De esta manera, la meta de las organizaciones triunfadoras es la omnicompetencia. A diferencia de la omnipotencia, que supone un poder ilimitado, la omnicompetencia significa poder para. La omnipotencia supone el control sobre otros; la omnicompetencia significa poder sobre uno mismo. Cuando examinamos

Cuanto más desarrollado sea un individuo, menos será lo que lo limiten los recursos disponibles.

la efectividad de las fuerzas de trabajo autodirigidas, nuestro objetivo es la omnicompetencia. El desarrollo es, por lo tanto, la clave de la productividad.

Políticas y procedimientos

Las políticas y los procedimientos son igualmente derivados de los nuevos procesos del negocio, tienen el objetivo de guiar y motivar, en una forma precisa, los esfuerzos para mejorar y mantener:

- La renovación de las estrategias de la organización.
- La planeación operativa y el control.
- La administración de recursos humanos y el desarrollo de la fuerza de trabajo.
- La recompensación a los empleados.

Las políticas se derivan de la misión, estrategias y factores críticos de éxito que fueron definidos como parte de la reingeniería de procesos. Éstas consisten en la formulación de sentencias que indican el curso de acción para cubrir las expectativas tanto internas como externas de la organización.

Los procedimientos señalan la secuencia de pasos necesarios para implantar las políticas.

Los procedimientos señalan la secuencia de pasos necesarios para implantar las políticas.

Es importante mencionar que dado que las políticas y procedimientos se definen y especifican después de haberse definido los nuevos procesos, ninguna nueva tarea debe surgir como resultado de la definición de las políticas y procedimientos; a menos que se requiera para satisfacer al cliente final.

Programa de capacitación sobre nuevos procesos

El programa de capacitación se desarrolla para proporcionar tanto las nuevas habilidades, como la cultura (valores, cooperación, sentido de pertenencia, etc.) que requerirá el personal para manejar los nuevos procesos. Este programa incluye el desarrollo del currículo por cubrir y los medios para proporcionar la capacitación; pueden incluir: sesiones con un instructor, procedimientos de usuario, capacitación basada en computadora, vídeo interactivo.

Actividades de transición y aceptación del cambio

Las actividades de transición se utilizan para facilitar a la organización y a todos los involucrados el manejo del proceso de cambio y están enfocadas a buscar la atención, la aceptación y el apoyo de las acciones necesarias para mejorar la ejecución del negocio.

El tipo de las actividades de transición dependerá de la estrategia de implantación que se decida; dentro de las variedades en cuanto a estrategias de implantación se pueden considerar:

- Implantación total y simultánea de las nuevas estructuras, políticas, procedimientos y procesos.
- Implantaciones piloto para probar y refinar las nuevas estructuras, políticas y procesos.
- Implantación por fases, de los componentes de la nueva estructura, políticas y procesos; de forma que cada componente ocupe el lugar del componente anterior durante cada cierto tiempo.

A continuación se presentan las ventajas y desventajas de cada una de las estrategias de implantación mencionadas:

Estrategia	Ventajas	Desventajas
• Implantación total y simultánea	Es el cambio más rápido (en las ocasiones en que resulta exitosa).	Es la estrategia más riesgosa; representa el cambio menos controlable.
• Implantaciones piloto	Es un cambio con mayor grado de control.	Es una transición más larga; existe el riesgo de que se pierda oportunidad.
• Implantación por fases	Se tiene el mayor control, sujeta a menos interrupciones.	Es una transición más larga; existe el riesgo de que se pierda oportunidad.

La futura organización, las nuevas habilidades del personal y los factores culturales se consideran implantados una vez que se encuentran operando los nuevos procesos, y la estructura y el personal los soportan adecuadamente.

Bibliografía

Bernard C. Reimann, (1989) "Sustaining the Competitive Advantage," *Planning Review*, March/April.

Cash James I. Jr., F. Warren McFarlan y James L. McKenney, (1988) *Corporate Information Systems Management*, Dow Jones-Irwin, EE:UU.

Hammer Michael; (1990) "Reengineering Work : Don't Automate, Obliterate," *Harvard Business Review*, July/August.

Porter Michael (1985), *Competitive Advantage*, Free Press, EE.UU.

Rockart John F (1979), "Chief Executives Define Their Own Data Needs," *Harvard Business Review*, March-April.

Rusell L Ackoff (1994) "Función de los negocios en una sociedad democrática", en *El MBA portátil*, Eliza G.C. Collins, Mary Anne Devanna, Editorial Limusa, México.

EJERCICIOS Y ACTIVIDADES DE EVALUACIÓN

CUARTA ACTIVIDAD
(Ejercicio individual)

A) Elija dos actividades de la lista siguiente y señale si se trata de actividades de valor primarias o secundarias. Argumente su respuesta describiendo la manera en que éstas se llevan a cabo en la institución en que labora, específicamente en su departamento o área de competencia. Extensión máxima: una página.

1. Logística de entrada
2. Adquisiciones
3. Servicio
4. Operaciones
5. Administración de recursos humanos
6. Desarrollo tecnológico
7. Infraestructura de la organización
8. Logística de salida
9. Mercadotecnia y venta

B) ¿Cuáles de las siguientes sentencias son ventajas de aplicar el enfoque de desarrollo de aplicaciones conocido como "factores críticos de éxito"? Argumente su respuesta explicando cómo las adoptaría o adopta en su área de competencia laboral. Extensión máxima: dos páginas.

1) Promueve la creación de medidores de ejecución efectivos para cada uno de los factores críticos de éxito, por lo que los gerentes buscan la creación de reportes y consultas específicas sobre dichos medidores.

2) Se logra que los directivos que basen sus decisiones en la comunicación oral y en opiniones de miembros de su equipo de trabajo; las cuales en muchos casos son subjetivas.

3) Se asigna mayor prioridad a las necesidades operativas que representan mayor carga de trabajo manual (nóminas, cuentas por cobrar, inventarios, etc.), más que a los requerimientos de información ejecutiva.

4) Se logra una definición clara de la cantidad de información que se procesará y se limita el procesamiento de datos e información innecesaria.

( ) 1, 2, 3
( ) 1, 3, 4
( ) 1, 3
( ) 1, 4

DIPLOMADO SEMIPRESENCIAL: TECNOLOGÍAS DE LA INFORMACIÓN EN LAS INSTITUCIONES DE SEGURIDAD SOCIAL

HOJA DE IDENTIFICACIÓN PARA ENVÍO

DE ACTIVIDADES DE EVALUACIÓN

DE:

NOMBRE:	FECHA:
INSTITUCIÓN:	
PAÍS:	LOCALIDAD
Fax: Correo electrónico:	

PARA: FAX: 5668 0094 / 55950644 **FAX DEL PROFESOR TUTOR:**

COORDINADORA: Lic. Fabiola Sánchez Gómez
TUTOR:

Puede fotocopiar esta forma y emplearla para enviar cada una de las actividades de evaluación.

A C T I V I D A D E S	FECHA DE ENVÍO	Número de hojas que anexa
Primera actividad.		
Segunda actividad.		
Tercera actividad.		
Cuarta actividad.		

Directorio

Mario Luis Fuentes Alcalá
Presidente de la CISS y de la Junta Directiva del CIESS

María Elvira Contreras Saucedo
Secretaria General de la CISS

Luis José Martínez Villalba
Director del CIESS

Guillermo Fajardo Ortiz
Coordinador Académico del CIESS

Fabiola Sánchez Gómez
Jefa del Area de Informática del CIESS

Martín Gómez Silva
Coordinador de la Unidad de Tecnología Educativa del CIESS

Juan José Zermeño Córdova
Jefe del Área de Comunicación del CIESS