



UNIVERSIDAD NACIONAL AUTONOMA DE MEXICO

FACULTAD DE INGENIERIA

**EL CONTROL GERENCIAL EN EL AREA DE
SISTEMAS DE INFORMACION**

TESIS

**Que para obtener el título de
INGENIERO EN COMPUTACION
presenta:**

JUAN FRANCISCO ROMAN GUZMAN

DIRECTOR DE TESIS: ING. VICTOR HUGO SALINAS H.

Ciudad de México

1997

**TESIS CON
FALLA DE ORIGEN**



Universidad Nacional
Autónoma de México



UNAM – Dirección General de Bibliotecas
Tesis Digitales
Restricciones de uso

DERECHOS RESERVADOS ©
PROHIBIDA SU REPRODUCCIÓN TOTAL O PARCIAL

Todo el material contenido en esta tesis esta protegido por la Ley Federal del Derecho de Autor (LFDA) de los Estados Unidos Mexicanos (México).

El uso de imágenes, fragmentos de videos, y demás material que sea objeto de protección de los derechos de autor, será exclusivamente para fines educativos e informativos y deberá citar la fuente donde la obtuvo mencionando el autor o autores. Cualquier uso distinto como el lucro, reproducción, edición o modificación, será perseguido y sancionado por el respectivo titular de los Derechos de Autor.

ESTE TRABAJO ESTA DEDICADO CON TODO MI AMOR A MI MADRE:

Teresa Guzmán B.

Quien me ha apoyado siempre.

Y A LA MEMORIA DE MI ABUELO:

Filiberto Guzmán P.

AGRADECIMIENTOS

Desco agradecer a mi hermano:

Víctor Alfonso Román G.

Y a mi padre:

Javier Salázar A.

Por todo el apoyo y cariño que me han brindado siempre.

Deseo agradecer a mi novia:

Patricia Iglesias M.

Por ser parte de los buenos momentos y apoyarme en los tiempos difíciles.

Desco agradecer a mi familia:

**mi abuela Rosario Guzmán, mi tía Rosa Ma. Guzmán, mi tía Concepción Guzmán,
a todos mis tíos y a todos mis primos.**

Por todo el cariño que me han demostrado.

Quiero agradecer sinceramente a mi asesor:

Ing. Víctor Hugo Salinas H.

Por su tiempo y por crecer en este proyecto.

**Y FINALMENTE QUIERO AGRADECER PROFUNDAMENTE A TODOS
MIS PROFESORES.**

Por la preparación universitaria que me otorgaron.

**EL CONTROL GERENCIAL
EN EL AREA DE
SISTEMAS DE INFORMACION**

INDICE

INTRODUCCION	I
CAPITULO I. EL CONTROL EN EL DESARROLLO DE SISTEMAS	1
1.1 Los estándares para el desarrollo de sistemas en la organización	2
1.1.1 La evolución en el desarrollo de sistemas.	3
1.1.2 La ingeniería de software.	7
1.1.3 El proceso de desarrollo de software.	9
1.1.4 El entorno de ingeniería de software.	13
1.2 Administración de proyectos	17
1.2.1 Definición del proyecto.	19
1.2.2 Planificación del proyecto.	21
1.2.3 Puesta en práctica del proyecto.	25
1.2.4 Conclusión del proyecto.	29
1.3 Normas y procedimientos para el control en el desarrollo de sistemas	32
1.4 Resumen	35
CAPITULO II. EL CONTROL EN LA UNIDAD DE COMPUTO	37
2.1 Las políticas para la administración de recursos y tecnología	38
2.1.1 La política.	38

2.2 La seguridad en el equipo de computo	41
2.2.1 Funciones y responsabilidades.	41
2.2.2 La seguridad de los datos.	43
2.2.3 La seguridad en un entorno de redes de trabajo.	47
2.2.4 Modelo para la seguridad en un entorno de redes.	53
2.2.5 El libro naranja.	57
2.3 El plan de contingencia y restablecimiento	59
2.3.1 Primer etapa: Respuesta de emergencia.	60
2.3.2 Segunda etapa: El tratamiento interno.	60
2.3.3 Tercer etapa: La restauración.	61
2.4 El inventario	63
2.4.1 Evaluación de inventarios.	64
2.4.2 El respaldo de datos.	65
2.5 Los recursos humanos	66
2.5.1 Planeación de los recursos humanos.	66
2.6 Normas y procedimientos para el control en la unidad de computo	68
2.7 Resumen	71
CAPITULO III. EL CONTROL EN LAS APLICACIONES	73
3.1 Los sistemas de información	74
3.1.1 Categorías de los sistemas de información.	77
3.1.2 Visión de los sistemas de información.	82
3.2 El control de la información	84
3.2.1 La administración de los sistemas de información.	85
3.3 Normas y procedimientos para el control en las aplicaciones	89
3.4 Resumen	91

CAPITULO IV. EL CONTROL GERENCIAL	93
4.1 La planeación en el área de sistemas de información dentro de la organización	94
4.1.1 El ciclo de planeación.	95
4.1.2 El enlace entre la empresa y la planeación.	96
4.2 Definición de políticas, estándares, normas y procedimientos	100
4.2.1 El desarrollo de políticas.	101
4.3 Definición de responsabilidades y funciones en cada área de la organización	102
4.3.1 Descripción y responsabilidades de la función del departamento de sistemas de información.	102
4.3.2 La adecuada separación de funciones.	104
4.3.3 Selección de personal.	105
4.3.4 La capacitación de personal.	106
4.4 La adquisición de equipo y servicios	107
4.4.1 La importancia del control en las adquisiciones.	108
4.4.2 La función de los comités.	108
4.5 Requerimientos externos	110
4.5.1 El derecho de autor y los sistemas de información.	110
4.5.2 El uso de software ilegal.	112
4.6 Normas y procedimientos de control gerencial en los sistemas de información	117
4.7 Resumen	120

CAPITULO V. EL VALOR AGREGADO DE LA INFORMACION	122
5.1 El valor de la información	123
5.2 La administración de las fuentes de información	126
5.2.1 Los problemas en la administración de datos.	127
5.2.2 La evolución de los sistemas administradores de bases de datos.	132
5.2.3 Los datos distribuidos.	137
5.2.4 La administración de la información.	143
5.3 Los informes	148
5.4 Resumen	149
 CONCLUSIONES	 150
 BIBLIOGRAFIA	 A

INTRODUCCION

Actualmente el área de sistemas de información es un departamento extremadamente importante dentro de una organización, el área de sistemas debe controlar las operaciones, procedimientos y los datos que se generan en el funcionamiento de la organización. Además, esta área es importante por los recursos de computo y los recursos humanos que maneja.

Los riesgos potenciales y los problemas a los que se puede enfrentar una organización por falta de procedimientos de control, puede producir serios contratiempos en los sistemas de información, en el almacenamiento de datos y en los recursos de la organización.

Dependiendo de diversos factores una empresa crecerá a corto, mediano o largo plazo en el área de sistemas. Este trabajo plantea como se puede impulsar un esquema de control dentro de la organización desde la Gerencia y como este esquema de control puede funcionar integrado al trabajo del departamento de sistemas.

Un profesional de ingeniería puede establecer la base para un esquema de control en toda una organización y mejor aún puede visualizar como integrar dichos controles al funcionamiento del departamento de sistemas. El control no sólo ayuda a reducir el riesgo de problemas relacionados con los sistemas de información, además es una herramienta de apoyo para la eficiencia de la empresa.

Con respecto al control, la función de la alta Gerencia de la organización, del gerente de auditoría y del gerente de sistemas de información es establecer en forma coordinada la estructura de control interno en toda la empresa. La función general de cada una de estas áreas es la siguiente:

- ❖ La alta gerencia debe impulsar las políticas, planes y programas para que dicho esquema pueda funcionar adecuadamente.
- ❖ El área de auditoría debe conocer detalladamente los procedimientos de control y las operaciones del área de sistemas, con el propósito de efectuar un estudio y evaluación adecuada de dichos controles periódicamente.
- ❖ El área de sistemas debe trabajar con los controles establecidos, integrados a su funcionamiento y establecer una fuente de datos corporativa.

Para el desarrollo de este trabajo se tomo como base la siguiente ¹clasificación de control en los sistemas de información:

1. El control Gerencial.
2. El control en los sistemas de información general. Controles para el diseño, desarrollo y mantenimiento de sistemas de información.
3. El control en los sistemas de información general. Tareas y operaciones del departamento de sistemas.
4. El control en las aplicaciones. Sistemas de información en operación.

¹ David H. Li. Auditoría en Centros de Computo.

El procedimiento que se desarrollará para alcanzar el objetivo de este trabajo, es el siguiente:

1. Basados en la clasificación de controles en los sistemas de información, describimos las características de estas áreas de estudio y como en teoría deben desarrollarse las tareas en cada área. El control no es un obstáculo para el desempeño del trabajo, de hecho un trabajo bien desarrollado cumple con controles inherentes.
2. Identificar los controles generales en el área de sistemas de información, considerando diversos factores que se aplican en la práctica.
3. Proponer desde el punto de la vista de la alta gerencia cuales deben ser las políticas y lineamientos en una organización que produzcan: Los programas y planes de trabajo, los estándares de calidad en las actividades de sistemas y los procedimientos de control para el funcionamiento óptimo de la organización.

El objetivo del control es disminuir los riesgos, el riesgo se puede ver como un efecto de causa, donde el control es el medio para disminuir dicha causa. Por ejemplo, mantenemos el control de inventario de la empresa mediante un sistema muy sencillo en una PC, se daña el disco duro y no contamos con ningún respaldo de la información, ni del sistema. El riesgo es la pérdida de la información, la pérdida del equipo y hasta el funcionamiento de ciertas operaciones en la empresa.

No existe una relación sencilla y directa entre controles y causas de riesgo, de esta forma se pueden tener numerosos controles para cada causa en particular, pero no podemos establecer un esquema de control de esa forma.

El objetivo de nuestra estructura de control es contar con los controles suficientes que **delimiten** el riesgo. En el caso de nuestro trabajo, intentamos establecer un **esquema de control** dentro de nuestra organización, dicho esquema de control por ser parte de la organización se denomina control interno.

Definimos control interno como la actividad que: ²“Comprende el plan de la organización y todos los métodos y procedimientos que en forma coordinada se adoptan en un negocio para salvaguardar sus activos, verificar la razonabilidad y confiabilidad de su información financiera, promover la eficiencia operacional y provocar la adherencia a las políticas prescritas por la administración”.

Por último, debemos mencionar que en los capítulos 1, 2, 3 y 4 tenemos dos tipos de resumen, excepto el capítulo 5 que sólo tiene el resumen de contenido:

- ❖ El primer resumen muestra en forma general, los controles que pueden aplicarse en esa área de sistemas de información.
- ❖ El segundo resumen se refiere al contenido y perspectiva de todo el capítulo.

² **IMCP. Normas y Procedimientos de Auditoría.**

CAPITULO 1

EL CONTROL EN EL DESARROLLO DE SISTEMAS

- 1.1 LOS ESTANDARES PARA EL DESARROLLO DE SISTEMAS EN LA ORGANIZACION.
- 1.2 LA ADMINISTRACION DE PROYECTOS.
- 1.3 NORMAS Y PROCEDIMIENTOS PARA EL CONTROL EN EL DESARROLLO DE SISTEMAS.
- 1.4 RESUMEN.

1.1 LOS ESTANDARES PARA EL DESARROLLO DE SISTEMAS EN LA ORGANIZACION

La administración es el aspecto más difícil y que más influye en el desarrollo de sistemas. La mala administración puede afectar el éxito de un proyecto más que cualquier otro aspecto. Sorprendentemente, parece ser también el punto menos entendido en el contexto de un modelo de desarrollo de sistemas. Es común ver que los modelos de desarrollo de sistemas no distinguen ningún modelo de administración, y en lugar de ver la administración como parte del modelo de proceso de desarrollo, ni siquiera se distingue del desarrollo en sí. En esta primera parte del capítulo revisaremos: Cual ha sido la evolución del desarrollo de sistemas y los estándares resultado de esta evolución, la ingeniería de software y por último el entorno de la ingeniería de software.

En la segunda parte se analizará la administración de proyectos y la estrecha relación que tiene con el desarrollo de sistemas. En la administración de proyectos no se hace mención de como el producto se realiza. Ya que el modelo de administración interviene sólo con los elementos requeridos para alcanzar y obtener un sistema de software. No que se necesita para crearlo. El punto de vista de un desarrollador es descrito en un modelo de desarrollo de software.

Como premisa en este capítulo podemos decir que "La revisión y auditoría son elementos de alto nivel que permiten al administrador verificar si una fase en particular está completa para poder entrar a otra".

¹ Marion E. Haynes. Administración de Proyectos.

1.1.1 LA EVOLUCION EN EL DESARROLLO DE SISTEMAS

La primer generación de computadoras y los programas en los años 40 fueron enfocados para resolver problemas de navegación y balística, utilizados por científicos y la milicia. En los años 50 la segunda generación de computadoras proporcionaba más facilidades y flexibilidad para su uso, así se facilitó el costo de las computadoras para ser utilizadas en el procesamiento de datos en los negocios.

Tanto en los años 40 como en los 50 se consideraba que un programa era exitoso si se podía ejecutar, se ejecutaba rápidamente y si proporcionaba una respuesta aceptable. Debido a la características de la época la habilidad de los programadores era de admirarse, utilizando los recursos de cómputo disponibles.

Así la tercera generación de computadoras permitía que se ejecutarán programas más grandes y que varios programas se ejecutarán concurrentemente. Esta capacidad hizo que la tendencia del desarrollo de software se moviera de pequeños programas o conjunto de pequeños programas, a grandes programas ensamblados o ligados a otros en un sistema mayor.

Los programas de aplicación eran demasiado grandes y complejos para ser creados por un pequeño grupo de programadores, en su lugar se requería un equipo integrado por un número mayor de programadores. El aumento de personal y la logística de soporte rápidamente sobrepasó los costos de un proyecto. Al parecer un programa más grande no funcionaba de igual forma. Entre más crecía un programa más errores se encontraban.

A finales de la década de los años 60, el término Ingeniería de Software surgió de los problemas resultado de la introducción de la 3ª generación de computadoras. Se consideraba, que el llamado problema del desarrollo de software estaba tipificado por el alto costo, la falta de confiabilidad, y la falta de mantenimiento. A continuación definiremos dos términos muy utilizados desde entonces:

- ❖ **Ingeniería de Software.** ²“La aproximación sistemática al desarrollo, operación, mantenimiento y retiro del software”.
- ❖ **Software.** ³“Programas de computadora, procedimientos, reglas y posible documentación asociada y datos pertinentes a la operación de un sistema de computo”.

En los años 70 los desarrolladores comenzaron a concentrarse en las etapas iniciales del desarrollo, ya que en la práctica se demostraba que corregir un error en las primeras etapas de desarrollo costaba mucho más que en las etapas finales.

En la primera mitad de los años 80, dos grandes sucesos cambiaron la forma en que se desarrollaba la producción de software, primero, la disponibilidad de los lenguajes de 4ª generación. Anteriormente los programas sólo se realizaban a través de lenguajes de 3ª generación. Segundo, una nueva alternativa al tradicional desarrollo de sistemas surgió, el modelo Waterfall. El modelo de desarrollo Waterfall utilizado desde los años 70 y aún en nuestros días, es un paradigma clásico del ciclo de vida en el desarrollo de sistemas. La alternativa era un desarrollo a través de prototipos de software, también conocido como desarrollo iterativo, y esto fue posible debido a la aparición de los lenguajes de 4ª generación.

² Robert Charette. *Software Engineering Environments*.

³ *ibid.*

De hecho “Los lenguajes de 4ª generación son más que lenguajes de computadora son ambientes de programación”.

El desarrollo iterativo es un modelo de desarrollo que comienza con un prototipo simple que realiza sólo unas cuantas funciones básicas. A través del uso de prototipos, los diseñadores o los usuarios finales descubren nuevos requerimientos, los cuales se incorporan a cada versión. Cada versión realiza más funciones e incrementa su eficiencia.

En la segunda mitad de los años 80, se cuestionaba acerca del efecto de los lenguajes de 4ª generación y el desarrollo de sistemas utilizando una metodología de prototipos y la interrogante era como hacer cambios realmente significativos en el desarrollo de sistemas. De esta forma surgen dos corrientes de desarrollo de software: Una corriente llamada evolutiva en donde se utilizan herramientas CASE y una corriente llamada revolucionaria en donde se utiliza la programación orientada a objetos.

CASE (Computer Aided Software Engineering)

La programación estructurada y las técnicas de análisis de los años 70 trajeron cierta disciplina a los procesos de desarrollo de aplicaciones complejas. Pero, aún así, estas metodologías requieren de un gran estudio, análisis a detalle y elaborar varios documentos de trabajo. CASE surge para ayudar al desarrollo automatizado en conjunto con estas técnicas.

⁴ Ralph H. Sprague Jr. *Information Systems Management in Practice.*

CASE es una herramienta automatizada que asiste en la creación, mantenimiento o administración de software. las características de una herramienta CASE son:

- ❖ Un repositorio de información.
- ❖ Herramientas front-end para la planeación a través del diseño.
- ❖ Herramientas back-end para la generación de código de programación.
- ❖ Estaciones de desarrollo (workstation).

Características no incluidas pero necesarias son una metodología de **desarrollo** y una metodología de **administración**.

PROGRAMACION ORIENTADA A OBJETOS

Por otra parte la revolución en el desarrollo de sistemas para negocios ocurrido a finales de los años 80, trajo consigo la programación orientada a objetos. Los lenguajes de programación orientado a objetos habían sido utilizados en los laboratorios de investigación de computo en los años 60. Estos lenguajes y herramientas se trasladaron a la PC, donde se convirtieron en un estándar especialmente en el desarrollo de interfaces gráficas para el usuario.

A finales de los años 80 la programación orientada a objetos comenzó a hacerse notar en el desarrollo de sistemas para negocios. "La participación mínima hasta entonces fue creciendo enormemente, debido al surgimiento de la arquitectura cliente/servidor a inicio de los años 90, estos lenguajes fueron utilizados ya que los desarrolladores trataron de simplificar la extrema complejidad de los sistemas cliente/servidor al reutilizar objetos".

⁵ Ralph H. Sprague Jr. *Information Systems Management in Practice*.

Las áreas más importantes en las que se desarrollan aplicaciones mediante estos lenguajes son:

- Aplicaciones gráficas.
- Aplicaciones multimedia.
- Sistemas complejos.

1.1.2 LA INGENIERIA DE SOFTWARE

La ingeniería de software tiene factores comunes, sistemas construidos por equipos de trabajo no individuos, utilizar principios de ingeniería en el desarrollo de sistemas, incluyendo aspectos técnicos y no técnicos.

El software no sólo son programas de cómputo asociados con una aplicación o producto. “El software también incluye la documentación necesaria para su instalación, uso, desarrollo y mantenimiento de esos programas”.

Los avances en la ingeniería de software han ocurrido en varias áreas: análisis de requerimientos, estrategias de implementación, modelos de costos, y la generación de código de programación, etc. Estos avances han ayudado en la reducción de los problemas planteados:

- Alto costo de software.
- La variación práctica/teoría.
- La falta de productividad.

* Ian Sommerville. Software Engineering.

Cada problema esta relacionado uno con otro y la solución en un punto ayuda en los demás. Por ejemplo, el uso de lenguajes de programación de alto nivel en el desarrollo de sistemas, en lugar de utilizar lenguajes de bajo nivel ha ayudado a la productividad del programador.

La mayor parte del dinero gastado en software está en el mantenimiento del mismo. La ingeniería de software involucra la producción, costo - efectividad. El reto es la producción de software de alta calidad con una determinada cantidad de recursos y en un periodo de tiempo fijo. Existen 4 características que un sistema de software debe tener:

1. Mantenimiento.
2. Confiabilidad.
3. Eficiencia.
4. Apropiada interfaz con el usuario.

La optimización de estos puntos puede ser difícil. La relación entre costo y mejoras en cada uno de los atributos no es lineal y tal vez las mejoras en uno de los puntos pueda exceder el presupuesto dedicado en un desarrollo de software. Los objetivos de la **Ingeniería de Software** son los siguientes:

- ❖ Seleccionar y definir la mejor metodología de desarrollo que dirija el ciclo de vida del software, su planeación, desarrollo y mantenimiento.
- ❖ Un conjunto establecido de componentes de software que documente cada paso en el ciclo de desarrollo que muestre el seguimiento de un paso a otro.
- ❖ Un conjunto predecible de fases que puedan ser revisadas en intervalos regulares a través del ciclo de vida del software.

Basados en los objetivos señalados, el proceso de Ingeniería de Software persigue algunas de las siguientes metas:

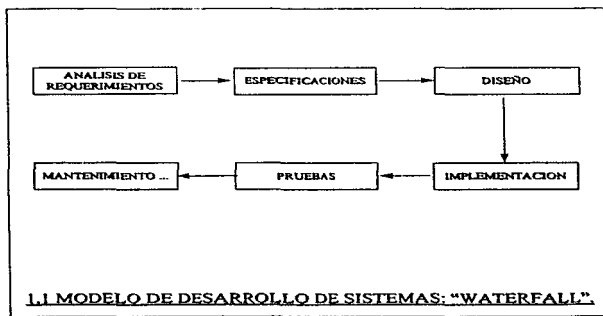
- Aplicar metodologías bien definidas para la resolución de puntos sobre sistemas y software.
- Proporcionar soluciones racionales a conflictos y la documentación de diferencias cuando una solución no es posible.
- Proporcionar cambios del producto en respuesta a nuevos requerimientos o modificación de estos.
- Proporcionar una clara comunicación entre la administración y los miembros del equipo de ingeniería/software.
- Proporcionar el entendimiento de como los sistemas actuales y la evolución de productos en un futuro será impactado por las decisiones tomadas el día de hoy.
- Anticipar las contingencias e identificar el impacto de las situaciones propuestas.
- Documentar decisiones, la racionalidad detrás de las decisiones, y las acciones tomadas; crear y mantener una memoria corporativa.

1.1.3 EL PROCESO DE DESARROLLO DE SOFTWARE

El proceso de software toma las características de cualquier otro proceso de ingeniería, así el modelo del proceso de desarrollo de software fue basado en otras actividades de ingeniería. Se mencionó el modelo de desarrollo llamado Waterfall que fue ampliamente aceptado en los años 70 por los jefes de desarrollo, ya que ofrecía los medios para hacer al proceso de desarrollo más visible.

Por ejemplo, el modelo **Waterfall** comprende las siguientes etapas de desarrollo:

- ❖ **Análisis de requerimientos:** Definición y análisis de las necesidades del usuario.
- ❖ **Especificaciones:** La traducción de los requerimientos hacia una descripción precisa de las variables del sistema.
- ❖ **Diseño:** La abstracción del software que es consistente con la especificación y proporciona una razonable descripción para la implementación.
- ❖ **Implementación:** La creación de un sistema de software el cual siga la guía del diseño.
- ❖ **Pruebas:** Determinar si las implementaciones satisfacen los requerimientos.
- ❖ **Mantenimiento:** La actualización del software necesario para arreglar problemas o realizar modificaciones. El proceso se repite durante esta fase.



De este modo, sin importar el modelo de proceso de desarrollo de software, esta actividad involucra varias etapas, como tal es un proceso variable y complejo el cual no puede ser simplemente descrito en un modelo.

En la práctica, las etapas de desarrollo se traslapan y toman información una de otra. Un modelo que esta basado en iteraciones hace difícil identificar puntos de revisión en la administración de un proyecto. La tendencia es ver en forma estática cada parte del modelo, es importante considerar la característica dinámica de cada etapa.

Un desarrollo debe ser verificado o validado, la verificación revisa si el producto, el cual esta desarrollado cumple con la definición de los requerimientos. La validación revisa si las funciones del producto son las que el usuario desea.

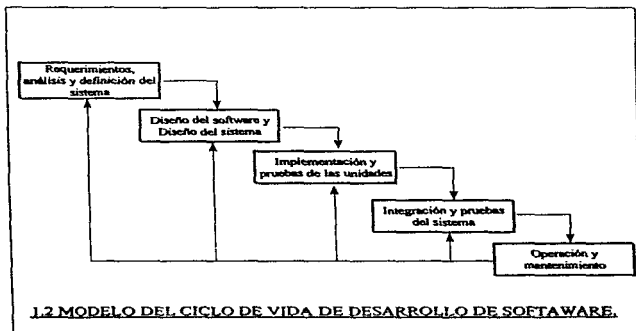
Durante la fase final del ciclo (operación y mantenimiento) la información obtenida retroalimenta a las fases previas del desarrollo. Así errores y omisiones en los requerimientos originales surgen, las modificaciones son necesarias para que el software continúe siendo útil. Estos cambios son llamados mantenimiento del software. El proceso de desarrollo se repite durante la etapa de mantenimiento debido a las modificaciones que se realizan.

Una de las finalidades de la ingeniería de software es reducir el costo total del software. Los costos varían dramáticamente dependiendo de la aplicación, de la organización y los métodos de desarrollo.

CARACTERÍSTICAS DE UN BUEN CICLO DE DESARROLLO

Lo primero, es que un buen modelo debe ser fácil de ser automatizado. Los productos de software no sólo incluyen el desarrollo del software sino también la documentación que describe al software y como fue construido. De hecho, la información contenida en cada uno de los productos debe ser reutilizable y debe poder ser analizada en cada etapa.

El ideal de un modelo de desarrollo es que éste sea general. Esto es, tener un modelo el cual sea posible cambiar y repetir. Que sea repetible es importante para entenderlo. Es decir todo este requerimiento implica separar el modelo en pequeñas partes aislando determinada información para análisis. Esto implica un proceso dinámico en lugar de un modelo de proceso estático.



Tres grandes áreas necesitan mejorar en el desarrollo de sistemas: Separar los aspectos administrativos del proceso de desarrollo en sí; separar los aspectos de ingeniería de software de los aspectos inherentes de la aplicación; y la necesidad de hacer explícita la relación entre la información requerida para desarrollar un producto y la administración del producto.

1.1.4 EL ENTORNO DE INGENIERIA DE SOFTWARE

Definimos como Entorno de Ingeniería de Software: "Los procesos, métodos y automatización requerida para producir un sistema de software".

Se ha mencionado que uno de los mayores problemas son: el alto costo del software, la variación teoría/práctica, y la falta de productividad. En general se ha acordado que la solución al problema del desarrollo de sistemas recae en la directrices del entorno de desarrollo dentro de la organización.

En una organización el objetivo es que el desarrollo de software tiene que ser de calidad y cumplir con un estándar y controles en sus fases de desarrollo, no sólo debe de funcionar, sino funcionar bien y considerar las siguientes características:

- Un diseño completo, especificaciones, y consistencia.
- Poder reutilizar diseños de software.
- Definición de objetivos y responsabilidades en cada etapa.
- Producir un software fácil de operar.
- Criterios bien definidos.
- Retroalimentación entre el equipo de desarrollo y el departamento usuario.

¹ Robert Charette. *Software Engineering Environments*.

- Coordinación de tareas, desempeño y efectividad.
- Documentación de calidad.
- Ayuda disponible para la resolución de problemas.
- Costos de desarrollo e itinerarios dentro del plan de desarrollo.
- Producir un software confiable y que pueda ser mantenido.



EL PROCESO

El modelo de proceso de desarrollo describe lo que se hará, como será alcanzado el objetivo, cuando terminará, y quien usará que para realizarlo. Un modelo pobre puede conducirnos a la confusión de nuestra metas en el proyecto, y nuestra asignación de recursos. Existen diversos modelos generales o paradigmas, algunos ya mencionados como el modelo Waterfall, el modelo de prototipos, etc.

Características de un modelo de procesos. "Un buen modelo debe cumplir con tres puntos principales: Poder descriptivo, generalidad y adaptabilidad para poder ser implementado".

- ❖ **Poder descriptivo.** Significa que posea la capacidad de describir los aspectos esenciales del problema de una forma real. Apoyo para el desarrollo así como la administración del proceso.
- ❖ **Generalidad.** Significa que debe tener la capacidad para describir una gran variedad de sistemas de software, componentes y las acciones que componen el sistema.
- ❖ **Adaptabilidad.** Significa que el sistema sea capaz de ser interpretado en una forma a través de la computadora, que permita su construcción en una estructura de datos o base de datos que contenga el modelo.

METODOS

El segundo elemento que constituye la ingeniería de software son los métodos aplicados en la creación de un producto de software.

Definimos **método** como: "La descripción explícita para realizar una actividad o conjunto de actividades requeridas por el modelo del ciclo de vida utilizado para desarrollar un producto de software".

Selección del Método. El objetivo de todo método es incrementar la confiabilidad, eficiencia, y el entendimiento del producto que se está construyendo.

▪ Robert Charette. Software Engineering Environments.

• *ibid.*

Combinando los principios con las metas y la fase del ciclo en la que se esté , un método puede ser categorizado o entendido, y lo más importante, la selección adecuada del método.

AUTOMATIZACION

El aspecto final del ambiente de ingeniería de software es la automatización de los métodos. El término automatización es referido también a las herramientas de software. Automatización por otra parte, significa ¹⁰“Apoyar un método el cual es parte integral de todo el proceso de desarrollo de software”. La automatización de un método que no puede interactuar con otros métodos utilizados, no es útil.

Hay que recordar, que la solución del problema recae en la integración de métodos dentro de una metodología comprensible, no en su automatización. La automatización es el **paso final**, **no el fin**. frecuentemente todo el enfoque se encamina a proporcionar herramientas, y más herramientas sin un propósito determinado. Por sí solas las herramientas no crean en un producto de software.

La automatización tiene un numero importante de beneficios. El más importante es que reduce las tareas al utilizar los métodos, y de alguna forma es el único camino realista para aplicar algunos métodos.

¹⁰ Robert Charette. Software Engineering Environments.

1.2 LA ADMINISTRACION DE PROYECTOS

La administración de proyectos consiste en "Una operación con un principio y un fin, llevada a cabo para obtener las metas establecidas dentro de los objetivos de costos, programa y calidad fijados. Reúne y aprovecha al máximo los recursos necesarios para completarlo con éxito". Los recursos incluyen la habilidad, talento y esfuerzo corporativo de un grupo de personas; instalaciones, herramientas y equipos; información, sistemas, técnicas y dinero.

La administración de proyectos difiere con la administración tradicional en dos puntos:

1. Se concentra sobre un proyecto que tiene un período de duración limitado, mientras que los otros departamentos o unidades pueden existir indefinidamente.
2. Los proyectos necesitan de los recursos físicos y humanos en forma parcial, mientras las organizaciones permanentes tratan de usar los recursos en todo momento.

PARAMETROS DEL PROYECTO

La duración del proyecto se concentra en tres parámetros básicos: **Calidad, Costo y Tiempo**. Un proyecto bien manejado es aquel que termina con el nivel de calidad especificado, en el plazo y dentro del presupuesto asignado.

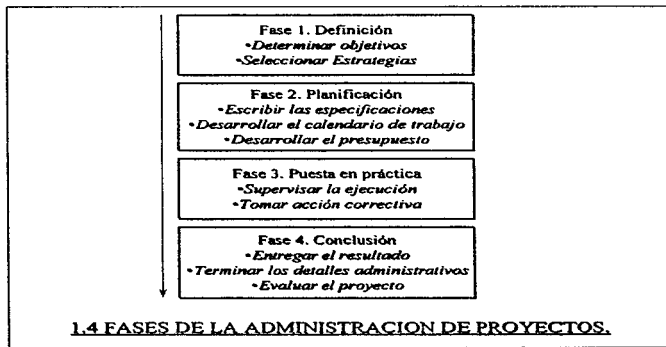
¹¹ Marion E. Haynes. Administración de Proyectos.

NEGOCIACION DE LAS ESPECIFICACIONES

Si existe algún cliente que deba aceptar el proyecto una vez terminado, se debe negociar y aceptar por este las especificaciones que definan una terminación satisfactoria.

EL CICLO DE DURACION DEL PROYECTO

Cada proyecto pasa a través de un ciclo de duración de 4 fases y cada una de ellas requiere de una habilidad diferente por parte del administrador del proyecto.



1.2.1 DEFINICION DEL PROYECTO

Los proyectos surgen de problemas u oportunidades. En el trabajo pueden iniciarse por la alta gerencia, los clientes o miembros del personal. El proyecto surge cuando alguien reacciona a un problema o cuando alguien ve la oportunidad ante una nueva empresa. El proyecto existe al tomarse la decisión de hacer algo sobre el problema y habitualmente se asigna a alguien la responsabilidad de llevarlo a cabo. El responsable es el **administrador del proyecto**.

INICIO

El iniciador del proyecto generalmente nunca tiene una idea clara sobre los aspectos importantes del mismo. Los interesados en el proyecto tienden a recalcar sus puntos de vista e interés, durante la fase de definición y estructuración. Si no se mantiene bajo control el grupo de interés se puede crear una gran confusión y pérdida de tiempo, sin embargo, se puede evitar si se inicia con una conversación clara y terminante entre el administrador del proyecto, los clientes y el personal comprendido en el mismo. Al tener una idea clara, el administrador del proyecto ya estará listo para comenzar a definir el proyecto.

LA META

El primer trabajo ante el grupo encargado de la realización del proyecto es dejar definido el proyecto y llegar a un acuerdo entre sus miembros sobre el alcance del mismo. Así como las estrategias para lograrlo.

Existe un proceso que sirve de guía para comenzar a trabajar en el proyecto:

- Estudiar, discutir y analizar.
- Escribir la definición del proyecto.
- Fijar el objetivo del resultado final.
- Enumerar lo imperativo y lo deseable.
- Crear estrategias alternas que lleven al objetivo.
- Evaluar las estrategias alternas.
- Seleccionar un curso de acción.

LA ESTRATEGIA PRELIMINAR

Antes de entrar a un proyecto a gran escala se debe efectuar un estudio de las posibilidades a fin de ensayar las estrategias preliminares. Dependiendo de la naturaleza del proyecto en una o varias alternativas. Que consisten en realizar un estudio de mercado o de factibilidad, un ensayo de ejemplo o una simulación por computadora.

¹²“Los recursos y la cantidad de dinero invertidos en los estudios de factibilidad, deben estar en proporción con la inversión que se llevará a cabo en el proyecto”.

LOS ESTUDIOS DE FACTIBILIDAD Y DE MERCADO

Si el estudio de factibilidad económico y técnico es bien concebido y ejecutado, ello nos indicará que debe seguirse adelante con el proyecto, se podrá pasar con confianza a la planificación en detalle y puesta en práctica del mismo. Si los

¹² Marion E. Haynes. Administración de Proyectos.

resultados son desalentadores entonces los datos obtenidos se usan para un nuevo diseño, un nuevo estudio de factibilidad y así sucesivamente, hasta identificar un concepto del producto que pueda tener éxito.

1.2.2 PLANIFICACION DEL PROYECTO

La planificación es de suma importancia en la administración de proyectos, ello quiere decir que se debe enumerar detalladamente todo lo necesario para terminar el proyecto con éxito siguiendo tres medidas vitales: **Calidad, tiempo y costo**. A continuación revisaremos cada una de estas medidas, junto con una variedad de herramientas y técnicas. Los pasos generales de toda planificación son:

- Establecer el objetivo del proyecto.
- Escoger una estrategia básica para lograr el objetivo.
- Dividir el proyecto.
- Determinar el estándar de ejecución, el tiempo necesario para completar cada fase y la secuencia apropiada para completar cada fase.
- Designar los costos de cada fase y la organización del personal necesario.
- Determinar el adiestramiento necesario para los miembros del grupo de trabajo.
- Desarrollar las políticas y procedimientos necesarios para llevar a cabo el proyecto.

PLANIFICACION DE LA MEDIDA DE LA CALIDAD

La meta de la planificación de la calidad es asegurar que el resultado del proyecto funcionará, es decir, que hará lo que se supone que debe hacer. El plan de la calidad

también establece los criterios de la ejecución con los cuales se comparará el resultado del proyecto una vez terminado.

Al planificar la medida de la calidad se deben incluir las especificaciones para la calidad y la clase de equipo que se utilizará, el estándar de ejecución que debe cumplirse y los medios para verificar la calidad como, por ejemplo, el ensayo y la inspección. Hay dos técnicas que facilitan la planificación de la calidad: **La estructura de la división del trabajo y las especificaciones del proyecto.**

¹³"La calidad del proyecto se define por las especificaciones detalladas del proyecto".

PLANIFICACION DE LA MEDIDA DEL TIEMPO

El objetivo al planificar la medida del tiempo es determinar el tiempo más corto necesario para completar el proyecto. Se inicia con la estructura de la división del trabajo y se determina el tiempo requerido para la terminación de cada fase o subunidad. Después, se determina en que secuencia deben finalizar las subunidades y en cuáles se puede estar trabajando al mismo tiempo. Debemos poder determinar:

- La duración de cada etapa.
- Lo más pronto que puede comenzar una etapa.
- Lo más tarde que puede comenzar una etapa.

¹³ Marion E. Haynes. Administración de Proyectos.

Existen tres métodos comúnmente usados para hacer un diagrama del proyecto:

- ❖ **Los diagramas de Gantt.** El diagrama de Gantt es una tabla horizontal que muestra gráficamente la relación del tiempo entre los pasos de un proyecto. El diagrama de Gantt muestra la secuencia del flujo de las actividades, como también las que se estén llevando a cabo al mismo tiempo.
- ❖ **Los diagramas PERT.** PERT son las siglas en inglés de Evaluación del Programa y Técnica de Revisión (Program Evaluation and Review Technique), constituyen una forma más sofisticada de la planificación que los diagramas de Gantt, y son apropiados para los proyectos que tienen muchos pasos interactivos e incertidumbre.
- ❖ **Ruta crítica.** Se describe como un proceso de administración, el cual enfoca su atención en los aspectos críticos de su trabajo, enfatiza la identificación inmediata y explícita de las desviaciones contra el plan original.

PLANIFICACION DE LA MEDIDA DEL COSTO

Un buen plan identifica las fuentes de recursos y materiales, y esta investigación cuidadosa asegura que los costos son realistas. El objetivo principal de un buen presupuesto consiste en supervisar los gastos del proyecto mientras se encuentra en progreso y quitar los gastos excesivos.

Es imposible estimar el costo de un proyecto mientras no se conozca cuanto tiempo durará, ya que el renglón más costoso será qué tiempo durarán las labores; por lo tanto, la estructura de la división del trabajo y la programación del proyecto son puntos de partida para desarrollar un presupuesto del proyecto.

Los componentes típicos de un presupuesto de proyecto son:

- **Mano de obra.** Salarios pagados a todo el personal trabajando directamente en el proyecto por el tiempo requerido.
- **Gastos globales.** Costo de los impuestos y beneficios suplementarios para todos los que trabajan directamente en el proyecto por el tiempo invertido. Calculados generalmente como un porcentaje del costo de la labor.
- **Equipo.** Costo del equipo, insumos o materiales comprados para uso en el proyecto.
- **Alquiler de equipos.** Costo del alquiler de los equipos usados en el proyecto.
- **Gastos administrativos y generales.** Costo de la administración y servicios de respaldo; por ejemplo, compras, contabilidad, etc. Por el tiempo dedicado al proyecto. Calculado generalmente como un porcentaje del costo del proyecto.
- **Ganancia.** La recompensa a la compañía por haber terminado el proyecto con éxito. Calculada generalmente como un porcentaje del costo del proyecto.

ASIGNACION DE RESPONSABILIDADES

La determinación de quién debe ser responsable de terminar cada subunidad o paso de un proyecto debe hacerse tan pronto como sea posible, de modo que todos puedan participar en la planificación, tanto de los calendarios de trabajo como de los presupuestos. Esta participación lleva a un mayor empeño por acabar el proyecto dentro de los límites de tiempo y dinero.

El número de personas comprendidas en un proyecto varía según su tamaño y alcance. No todos los proyectos tienen diferentes personas para cada una de las subunidades.

1.2.3 PUESTA EN PRACTICA DEL PROYECTO

Durante la fase de la puesta en práctica el administrador del proyecto coordina todos los elementos de un proyecto. Ello incluye el control progresivo del trabajo para ver si se está ejecutando de acuerdo con el plan; la retroalimentación a los que estén trabajando en el proyecto; contratar los materiales, suministros y servicios; y resolver las diferencias entre las personas comprendidas en el proyecto. Esta responsabilidad requiere de diversos conocimientos y experiencias. Deberes claves durante la puesta en práctica son:

- ❖ Control del desarrollo del trabajo.
- ❖ Retroalimentación.
- ❖ Contratación de los materiales, suministros y servicios.
- ❖ Solución de las diferencias.

CONTROL DEL DESARROLLO DEL TRABAJO

El control es la actividad central durante la puesta en práctica de un proyecto. La herramienta de mayor importancia en este proceso es el plan que se desarrolló para definir los tres parámetros del proyecto: las especificaciones, el calendario de trabajo y el presupuesto. Estos forman el estándar con el cual hay que medir la ejecución. El control comprende tres pasos:

1. **El establecimiento del estándar.** El estándar para el proyecto se estableció en las especificaciones creadas durante la fase de planificación. El administrador del proyecto debe consultar constantemente estas especificaciones. Si el proyecto se desvía de sus especificaciones originales, no habrá garantía del

éxito previsto en los estudios de factibilidad; el producto o resultado del proyecto no cumplirá con el estándar de ejecución.

Existen herramientas para ayudar a los administradores a controlar los proyectos y cumplir con los parámetros definidos de calidad, duración y presupuesto. Durante la etapa de planificación contamos con los diagramas de Gantt, PERT o Ruta crítica. Así, en la etapa de desarrollo podemos también utilizar las siguientes herramientas de control: Diagramas de identificación de los puntos de control, diagramas de control del proyecto, diagramas de hechos importantes y diagramas de control del presupuesto.

2. **Supervisión de la ejecución.** Las comprobaciones constituyen otra manera de verificar la calidad del proyecto. Por lo general, ciertas pruebas están escritas en las especificaciones para confirmar si se está alcanzando la calidad deseada.

Una auditoría puede hacerse durante el transcurso del proyecto, así como al concluirse, siendo las áreas más comunes sujetas a auditoría los libros de contabilidad, los procedimientos de compra y las medidas de seguridad. Los auditores deben ser expertos en el área del proyecto que se está revisando y por supuesto no ser miembros del grupo de desarrollo.

Una supervisión eficiente incluye más de una fuente de información. La combinación de las inspecciones, las revisiones del desarrollo, las comprobaciones y la auditoría proporcionan la información necesaria y sobre el estado y condiciones del proyecto. El objetivo durante la revisión periódica del desarrollo es conocer las condiciones de las operaciones e influenciar el

curso de los eventos futuros, según sea necesario. ¹⁴“Escuchando, contribuyendo, integrando y con el liderazgo para alcanzar los objetivos”.

3. **Las acciones correctivas.** A medida que el proyecto va desarrollándose y se supervisa su ejecución, habrá veces en que lo realizado no estará de acuerdo con los planes, esto significa que hay que adoptar una acción correctiva. No es realista esperar un progreso importante día tras día; a veces estará demorado y otras veces adelantado; pero en un proyecto bien planificado lo más probable es que se termine a tiempo y dentro del presupuesto.

Cuando la calidad del trabajo realizado no está de acuerdo con lo especificado, quizá la decisión final sea volver a hacer todo el trabajo, pero esta no es una solución sencilla.

Cuando el proyecto comienza a retrasarse en relación con su calendario de trabajos, existen tres alternativas que pueden corregir el problema. La primera es estudiar el trabajo que queda por hacer y decidir si en los próximos pasos a dar se puede recobrar el tiempo perdido. Si esto no es posible, se debe considerar dar algún tipo de incentivo si el proyecto se termina a tiempo, si se justifica, comparando este gasto con las posibles pérdidas por una terminación tardía. Finalmente, hay que considerar emplear más recursos; esto también será más costoso, pero puede compensar las pérdidas causadas por la demora en la terminación.

¹⁴ Marion E. Haynes. Administración de Proyectos.

RETROALIMENTACION

Los administradores de proyectos hallan muchas oportunidades de ofrecer retroalimentación a quienes toman parte en el desarrollo del proyecto. Mediante la retroalimentación los individuos conocen el efecto que su comportamiento tiene sobre los demás y cómo contribuye al éxito total del proyecto, todo esto sirve para mantener una buena ejecución y corregir el camino. Sin embargo, para que sea efectivo, hay que manejarlo en forma apropiada.

La guía más importante cuando se está dando una retroalimentación es tratar solamente con lo que se puede observar; esto limita la conversación a las acciones y resultados, ya que el administrador no tiene el tiempo para poder ver las intenciones de los miembros del equipo.

CONTRATACION DE LOS MATERIALES, SUMINISTROS Y SERVICIOS

La contratación es un proceso importante que ocupa hasta 20% del tiempo de un administrador. La negociación al contratar equipos, materiales, suministros y servicios llega a ser una manera de solucionar las diferencias, y puede contribuir significativamente al éxito del proyecto.

SOLUCION DE LAS DIFERENCIAS

La mejor solución para un departamento, o para un grupo, no siempre es también la mejor para los demás. Si esta situación se maneja apropiadamente a veces es posible obtener soluciones creativas de estas diferencias. La habilidad para

solucionar las diferencias es una cualidad importante de los administradores de proyectos. Las diferencias pueden resolverse utilizando alguna de estas estrategias.

- Demandar.
- Solucionar problemas.
- Pactar.
- Ceder.

Cada estrategia tiene su lugar; sin embargo, son pocas las personas que reconocen las condiciones que respaldan cada estrategia. Utilizar la misma estrategia para solucionar diferencias en todas las situaciones, obviamente, no será efectiva en muchos casos. Se debe distinguir entre las diferentes situaciones y adoptar un enfoque que tenga la mayor posibilidad de éxito a largo plazo. No se debe pasar por alto la importancia de mantener las relaciones de cooperación.

1.2.4. CONCLUSION DEL PROYECTO

El objetivo de la administración de proyectos es obtener la aceptación por parte del usuario del resultado obtenido. Esto quiere decir que el usuario está de acuerdo en que se cumplieron las especificaciones de calidad del proyecto. Para que todo se realice fácilmente el cliente y el administrador del proyecto deben tener **criterios bien documentados** sobre la ejecución del proyecto desde el inicio. Ello no quiere decir que no habrá algún cambio, sino que cuando estos tengan lugar, el contrato o el documento que especifica los requerimientos deben enmendarse de modo que refleje los cambios en las especificaciones y en el calendario de trabajo.

Los criterios objetivos y que pueden medirse son siempre los mejores, a diferencia de los criterios subjetivos, que pueden ser riesgosos y sujetos a interpretaciones personales. Jamás debe haber lugar para las dudas o ambigüedades.

El proyecto puede estar terminado o no al entregarse los resultados al cliente. Con frecuencia existen requisitos de documentación, por ejemplo, manuales de operaciones, manuales de usuario, especificaciones técnicas y un informe final que, por lo general, se hace después de la entrega. También puede haber algún tipo de personal adiestrado para trabajo con las nuevas instalaciones o productos y, asimismo, es habitual tener una auditoría final.

LA EVALUACION DEL PROYECTO

La evaluación de los resultados la podemos realizar a través de los siguientes parámetros:

1. Comparar la fecha de terminación con la fecha fijada en el proyecto.
2. Cuál es el aprendizaje sobre la planificación que pueda ayudarnos en el próximo proyecto.
3. Si el presupuesto estuvo dentro del costo final del proyecto.
4. Cuál fue el aprendizaje sobre el presupuesto que pueda ayudarnos en el próximo proyecto.
5. Se ajustaron los resultados a las especificaciones del usuario sin necesidad de trabajo adicional.
6. Describir el trabajo adicional, si éste fue necesario.
7. Cuál fue el aprendizaje acerca de la redacción de las especificaciones que pueda ayudarnos en el próximo proyecto.

8. El aprendizaje sobre cómo emplear el personal que pueda ayudarnos en el próximo proyecto.
9. El aprendizaje sobre la supervisión de la ejecución que pueda ayudarnos en el próximo proyecto.
10. El aprendizaje sobre como corregir actividades que pueda ayudarnos en el próximo proyecto.
11. Los adelantos técnicos que se hicieron en el proyecto.
12. Herramientas y técnicas que se desarrollaron que puedan ser útiles en el próximo proyecto.
13. Recomendaciones que se tienen para la investigación y el desarrollo en el futuro.
14. Las lecciones que se aprendieron en los tratos con las organizaciones de servicios y vendedores externos.
15. Qué se haría de diferente manera. Si tuviéramos la oportunidad de volver a desarrollar todo el proyecto.

1.3 NORMAS Y PROCEDIMIENTOS DE CONTROL EN EL DESARROLLO DE SISTEMAS

La siguiente lista es un resumen que abarca los puntos generales sobre el control en el desarrollo de sistemas:

❖ **Metodologías y Responsabilidades.**

Selección de metodologías para el desarrollo de sistemas.

Asignación de funciones y responsabilidades de cada elemento en el desarrollo.

Actualizaciones en la metodología de desarrollo de sistemas.

❖ **Inicio del Proyecto.**

El papel de la Gerencia del departamento usuario en el inicio de un proyecto.

Definición del proyecto.

Integración del equipo de trabajo y sus responsabilidades en el proyecto.

Definición de los requerimientos de la información.

Aprobación del proyecto.

❖ **Estudio de Factibilidad.**

Estudio de factibilidad tecnológica.

Estudio de factibilidad económica.

Formulación de caminos alternativos de acción.

Aprobación del proyecto.

Plan maestro del proyecto.

Control del presupuesto y de los costos.

Selección de la metodología de desarrollo de sistemas.

❖ **Fase de Diseño.**

Definición y documentación de los requerimientos de los datos de entrada.

Definición y documentación de los requerimientos de los datos de salida.

Definición y documentación de los requerimientos en los archivos y bases de datos.

Definición y documentación de los requerimientos de procesamiento

Especificaciones del sistema de información.

Diseño de documentos fuente.

Diseño de pistas de auditoría.

Diseño de controles.

Estándares en la documentación de programas.

❖ **Fase de Desarrollo e Implantación.**

Objetivos de la programación.

Descripción del programa.

Descripción de las herramientas de desarrollo.

Manual de operación.

Manual del usuario.

Estándares en la prueba de los diversos programas del sistema.

Estándares para la prueba del sistema.

Evaluación de resultados de las pruebas.

Análisis de los documentos entregados al departamento usuario.

Los planes de funcionamiento en paralelo, en el caso de algunos sistemas.

Pruebas de aceptación final.

❖ **Fase de Operación y Mantenimiento.**

Procedimientos de control de operaciones y procesos en el sistema.

Control de costos.

Modificaciones del sistema.

❖ **Fase de Post - Implantación.**

Evaluación de los resultados en la operaciones y los procesos.

Evaluación del cumplimiento de los requerimientos del usuario.

Evaluación del análisis costo/beneficio.

1.4 RESUMEN

La ingeniería de software estudia y trata sobre el desarrollo de sistemas, en este capítulo revisamos la relación entre el desarrollo de sistemas y la administración de proyectos. Sorprendente el control esta implícito en más de una etapa en la actividad de ingeniería de software y administración del proyecto, es cierto que el esquema de control puede considerarse como un trabajo adicional, pero será de gran valor para la empresa.

Existen dos materias bien definidas en el capítulo 1 para el implementar un esquema de control en el desarrollo de sistemas: La ingeniería de software y la administración de proyectos.

INGENIERIA DE SOFTWARE

En la década de los 40 y 50 se consideraba que un programa era exitoso si funcionaba simplemente, los lenguajes de programación fueron evolucionando hasta convertirse en ambientes de programación, esta evolución en la programación produjo: La programación orientada a objetos y las herramientas CASE.

En los años 60 surge el término Ingeniería de Software con el propósito de desarrollar productos de mayor calidad. Utilizando modelos para el proceso de desarrollo, como el modelo Waterfall (Análisis, especificación de requerimientos, diseño, implementación, pruebas y mantenimiento) y donde se consideran variaciones que dan como resultado nuevos paradigmas para el desarrollo de mejores productos.

La descripción del entorno de ingeniería intenta mostrar todas las características ideales para el desarrollo de sistemas dentro de la organización. Los puntos en los que se divide el entorno de ingeniería son: Los procesos, métodos y la automatización.

ADMINISTRACION DE PROYECTOS

El objetivo en este segundo tema consiste en describir la administración de un proyecto y mostrar que existe una relación muy estrecha entre el desarrollo de sistemas y la administración del proyecto. La administración del proyecto consiste en 4 etapas esenciales:

1. Definición del proyecto.
2. Planificación del proyecto.
3. Puesta en práctica.
4. Conclusión del proyecto.

La administración de un proyecto revisa dentro de una filosofía y trabajo distinto el llevar a cabo una tarea. La combinación de ambas perspectivas (ingeniería de software y administración de proyectos) nos ayuda a desempeñar un trabajo eficiente y establecer el control de la actividad. Considerando la perspectiva de la Gerencia, donde debemos considerar determinadas características en el desarrollo de un sistema de software:

- ❖ Producir un sistema de calidad.
- ❖ Dentro de un costo presupuestado.
- ❖ Y a tiempo.

CAPITULO 2
EL CONTROL EN LA UNIDAD DE COMPUTO

- 2.1 LAS POLITICAS PARA LA ADMINISTRACION DE RECURSOS Y TECNOLOGIA.**
- 2.2 LA SEGURIDAD EN EL EQUIPO DE COMPUTO.**
- 2.3 EL PLAN DE CONTINGENCIA Y RESTABLECIMIENTO.**
- 2.4 EL INVENTARIO.**
- 2.5 LOS RECURSOS HUMANOS.**
- 2.6 NORMAS Y PROCEDIMIENTOS DE CONTROL EN LA UNIDAD DE COMPUTO.**
- 2.7 RESUMEN.**

2.1 LAS POLITICAS PARA LA ADMINISTRACION DE RECURSOS Y TECNOLOGIA

Los parámetros más importantes a considerar en la unidad de computo, por la importancia que tienen en su funcionamiento y su relación directa con el control son: La seguridad, la administración de recursos y la tecnología.

La parte crítica en el desenvolvimiento de la unidad de computo es la participación de la Gerencia. Salvo que la Gerencia establezca las políticas, planes y programas a seguir sobre los aspectos de seguridad, administración de recursos y tecnología, el desarrollo de éstas tareas se quedará en sólo palabras.

En este trabajo no se intenta desarrollar una guía sobre selección de tecnología para determinada empresa. Sólo intentamos mostrar la importancia de dicha selección.

Este capítulo trata de definir en forma general la función que la Gerencia de la organización y de la unidad de computo pueden desempeñar a través de políticas, para impulsar el buen funcionamiento de la arquitectura de sistemas de información. Describiremos en que consiste la seguridad de datos, el plan de contingencia y restablecimiento, el inventario y los recursos humanos.

2.1.1 LA POLITICA

La política sobre los puntos de: Seguridad, administración de recursos y tecnología; establece las responsabilidades de cada área para la generación, explotación y utilización de los sistemas de información. Tal política debe ser

apoyada por directrices documentadas, procedimientos y normas de control interno. Estos procedimientos y normas son responsabilidad de la Gerencia plantearlas, apoyándose en el departamento de auditoría y en la unidad de computo.

El usuario, custodio y propietario de los recursos y de la información, en la mayoría de las veces no son los mismos individuos.

Si no existe algún documento acerca de la responsabilidad del uso de recursos, entonces la primera acción es colocar, describir y definir la existencia de un inventario de equipo, software, datos e instalaciones.

Por sí misma, una política en la unidad de computo o departamento de sistemas no es suficiente, sólo representa una declaración oficial de posición tomada por la dirección. La declaración política debe ser apoyada con planes y programas de trabajo para efectuar todas las acciones necesarias para la seguridad, administración de recursos y tecnología. El siguiente modelo de planes y programas de la Gerencia son generales:

Planes

- ❖ Planes sobre tecnología; tendencias y la utilización en nuestra organización.
- ❖ Plan de contingencia y restablecimiento; debemos poder continuar con procesos alternos en el funcionamiento de la organización aún en caso de contingencia.
- ❖ Plan de control de acceso a las instalaciones de la organización.
- ❖ Plan de Inventario; Es importante conocer cuál es el valor de cada elemento físico y lógico de nuestra infraestructura de sistemas.

Programas

- ❖ Programa de trabajo anual.
- ❖ Programa para la asignación de proyectos y recursos.
- ❖ Programa de clasificación de datos, instalaciones y equipo.
- ❖ Programa de cambios en los controles establecidos.

Estos planes y programas son desarrollados en distinto grado dentro de la organización, y de alguna forma deben estar establecidos en forma general. La mayoría de las organizaciones pueden identificar estos planes y programas bajo diferentes nombres. Como sea, son planes y programas básicos de la actividad de control. Actividad planeada para conducir el negocio de una forma normal y continua, bajo un estándar establecido por la Gerencia.

Se pueden considerar subdivisiones de dichos planes y programas, todo ello depende de la naturaleza de la empresa.

2.2 LA SEGURIDAD EN EL EQUIPO DE COMPUTO

Hoy en día mantenemos información en computadoras de todo tipo, un tópico de extrema importancia es la seguridad de esta información. En otros tiempos, se utilizaban barreras físicas y ello proporcionaba una adecuada seguridad. Pero el uso de computadoras y la facilidad para guardar información, ha creado el problema de seguridad. Con información basada en computadoras es hoy en día más fácil recolectar esa información sin importar si lo estoy haciendo legal o ilegalmente, o si algún proceso se realiza deliberada o accidentalmente.

La seguridad debe ser tratada como una línea y como una función de la organización. Los gerentes tienen la responsabilidad con la organización con respecto a la seguridad de equipo y datos. Ellos requieren establecer la **delegación de responsabilidades** a otros bajo su control.

La **función** básica de la administración de seguridad es **ayudar a la dirección a hacer que su propia seguridad sea fácil.**

2.2.1 FUNCIONES Y RESPONSABILIDADES

Todo departamento debe estar incluido en la **responsabilidad** del uso del equipo, software, acceso a datos e instalaciones de la **organización**, considerando el papel del propietario, el custodio y el usuario de la información. La **responsabilidad** debe ser reconocible en el uso de los sistemas de información de la organización, así como en la administración y uso del equipo de computo.

El uso de la información y equipo están basados en la política de la Gerencia. Es obligatorio que algunas políticas corporativas sean formalmente establecidas para utilizarlas como una base de control en la seguridad. La falta de políticas de control en la organización puede ser la razón principal del uso irregular de la información dentro de la compañía. Existen funciones y responsabilidades generales para la administración de la seguridad, que se detallan a continuación:

- La Gerencia debe proveer un apoyo administrativo directo para la instalación de sistemas de seguridad.
- Establecer objetivos para el desarrollo futuro de los sistemas de seguridad, considerando la evolución tecnológica.
- Determinar los requerimientos de recursos especiales, relativos a las responsabilidades de seguridad.
- Negociar el apoyo de la dirección, para la integración de los objetivos de seguridad, con la estrategia tecnológica a largo alcance.
- Analizar continuamente y evaluar las alternativas de seguridad.
- Asegurar que los proyectos en desarrollo hacen frente a los objetivos de seguridad corporativa.
- Supervisar el uso de todos las aplicaciones en operación para descubrir y actuar sobre los accesos no autorizados.
- Coordinar con el departamento jurídico y de seguridad, investigaciones internas en una base altamente confidencial.
- Dirigir auditorías de seguridad, participar en evaluaciones de seguridad y proveer guía y asistencia en los sistemas de información.
- Revisar los esfuerzos de documentación asociados con diversos sistemas de seguridad interna.

El departamento encargado de la seguridad de computo debe tener la propia confianza e iniciativa necesaria para desempeñar su función utilizando las guías abiertas de la dirección. El papel de la administración de la seguridad implica definitivamente una tarea dinámica. El trabajo se realiza en un entorno de cambio continuo.

2.2.2 LA SEGURIDAD DE LOS DATOS

La mayoría de la información sobre la toma de decisiones, competitividad de productos, procedimientos, y sobre comunicaciones privadas dentro de la empresa debe ser necesariamente clasificadas como confidenciales con el propósito de mantener el éxito de la organización.

La seguridad de datos puede ser definida como "La protección de datos ante un accidente o acceso intencional de un usuario no autorizado y de modificaciones no autorizadas". Las técnicas para seguridad incluyen características del hardware de computadora, rutinas programadas y procedimientos manuales. Así como los medios físicos de seguridad que resguardan el ambiente con seguridad personal, cerrojos o llaves.

Razones para la seguridad de datos. Primero el acceso ilegal a la información en un sistema no deja registro del robo, excepto si va acompañado del robo físico de la pieza de hardware, de hecho no se conoce si se ha perpetrado un acceso ilegal y se ha comprometido la seguridad. Segundo los recursos de computo son compartidos entre los usuarios para proporcionar un uso eficiente del equipo de esta forma es necesario proporcionar el nivel requerido de seguridad de datos. Por último, varios

¹ Harry Katzan, Jr. The Standard Data Encryption Algorithm.

sistemas incluyen comunicación de datos para transferir información y cierta exposición accidental o deliberada de información confidencial, puede ocurrir durante la transmisión de datos.

AMENAZAS A LA SEGURIDAD DE DATOS

En general, las amenazas a la seguridad de datos ha sido clasificada como accidental o deliberada.

- ❖ **Accidental.** sin importar la razón, una intromisión accidental al sistema de manejo de datos posiblemente dejará disponible información a personas no autorizadas y proporcionara la oportunidad de alterar o destruir archivos o exponer la información a personas con marcados intereses en conocerla.

- ❖ **Deliberada.** La intromisión deliberada en el sistema de manejo de datos puede tomar lugar de forma pasiva o activa. La intromisión pasiva es realizada en el uso de las facilidades de comunicación que involucran actividades como inspeccionar archivos temporales dejados por accidente o inapropiadamente. La intromisión activa involucra: Obtener acceso legítimo utilizando los derechos de otro usuario, el robo de hardware, utilizar canales de comunicación para tener acceso a la información, etc.

Resumiendo, el objetivo de la intromisión deliberada a un sistema de manejo de datos puede ser obtener información confidencial, información de interés de una persona, o tener la oportunidad de alteraciones o destrucción de un archivo.

MEDIDAS EN LA SEGURIDAD DE DATOS

Las medidas de seguridad incluyen un conjunto organizado de procedimientos, hardware y facilidades de software que colectivamente prevén que una persona no autorizada obtenga información del sistema de administración de datos.

Cada medida de seguridad es más efectiva en determinados casos, no hay una medida sencilla que elimine completamente el problema de seguridad de datos. Las medidas generales de seguridad de datos están agrupadas en 6 clases:

1. **Administración de acceso.** La administración de acceso conocida como control de acceso es un conjunto de técnicas diseñadas para evitar que personas no autorizadas utilicen servicios de computo o tengan acceso a datos. Estas técnicas contemplan los siguientes conceptos: Protección de terminales, identificación de terminales, identificación de usuarios y proporcionar varios niveles de servicio.
2. **Limitaciones de procesamiento.** Las limitaciones de procesamiento generalmente se refieren a un conjunto de características de software y hardware, que controlan la forma en que se maneja el procesamiento de datos en el sistema de computo, y restringen colectivamente el dominio del usuario a determinadas áreas asignadas o autorizadas.
3. **Auditoría y monitoreo.** La auditoría y monitoreo se refiere a la práctica de registrar los intentos de violar la seguridad en el sistema de computo o en los archivos de datos. Cuando el usuario intenta acceder recursos a los cuales no tiene derecho.

- 4. Transformaciones.** El término transformaciones se refiere al uso de técnicas criptográficas para conciliar el contenido de un mensaje o un registro de datos. El mensaje es codificado antes de una transmisión así que la información que puede ser interceptada durante este proceso no es inteligible en forma inmediata. Otro de sus usos es cuando se almacena datos en medios secundarios o externos. El uso de transformaciones proporciona relativamente un alto nivel de seguridad. El objetivo es sencillo, hacer que el costo para descifrar el código sea mucho mayor que el valor que pudiera tener la información para la persona que lo intenta descifrar.

- 5. Administración de la integridad.** La administración de la integridad se refiere a la integridad del hardware, software, del personal, de los procedimientos de operación y a la integridad en el uso de medidas físicas efectivas de seguridad.

- 6. Niveles de autorización y protección de archivos.** Los niveles de autorización se aplican cuando el usuario tiene acceso al sistema de computo. Si el usuario ejecuta su propio programa y accesa sus propios datos, entonces el problema de datos de seguridad concierne sólo a la administración de acceso. Como sea, si los programas y datos son compartidos en un sistema llámese una red de computadoras, entonces diferentes niveles de autorización son necesarios para controlar las funciones que un usuario puede desempeñar.

IMPLEMENTACION DE MEDIDAS DE SEGURIDAD

Las medidas de seguridad están disponibles principalmente a través del hardware y software que usualmente proporciona el fabricante o es desarrollada bajo bases generales de instalación, es decir, la unidad de computo debe evaluar las

características de seguridad que ofrece cada producto y determinar si cumplen con las necesidades requeridas para la organización.

De hecho, varios de los métodos menos sofisticados pueden ser programados en un período relativamente corto de tiempo y proporcionar un razonable nivel de seguridad de datos, dependiendo de las necesidades de la aplicación.

2.2.3 LA SEGURIDAD EN UN ENTORNO DE REDES DE TRABAJO

La seguridad de la información ha sufrido dos grandes cambios en las últimas décadas. El **primero** es el uso extendido de equipos de computo, y el **segundo** gran cambio que ha afectado la seguridad de datos es la introducción de sistemas distribuidos, el uso de las redes de computadoras y las facilidades de comunicación para transmitir datos. La necesidad de herramientas automatizadas para la protección de archivos almacenados en computadoras es evidente. Especialmente en los sistemas multiusuario, y la necesidad es aún mayor en los sistemas que se pueden acceder a través de una línea telefónica o una red de trabajo.

De hecho, el término de seguridad en redes de computadoras es a veces mal entendido, ya que virtualmente todos los negocios, gobierno, y las organizaciones académicas interconectan sus equipos con alguna otra red de computadoras, si esto no es cierto en todos los países, si podemos afirmar que es una tendencia a futuro en cualquier organización. Esta colección de redes se referencia con el nombre de **internetwork**.

No existen límites claros entre las diferentes formas de seguridad. Por ejemplo, uno de los tipos más publicitados de ataque a los sistemas de información son los

virus de computadora. Los virus pueden ser introducidos físicamente a través de un disco o llegar a través de la red, en cualquiera de los casos el virus está residente en el sistema de la computadora, y las herramientas de seguridad de la computadora son requeridas para detectar el virus y recuperar la información.

La **seguridad** en un entorno de redes (internetwork) consiste en medidas para determinar, prevenir, detectar, y corregir violaciones a la seguridad que involucren la transmisión de información. La seguridad en un entorno de redes es compleja e interesante, y algunas de las razones son las siguientes:

1. La seguridad que involucra las redes y comunicaciones no es tan simple como pudiera verse en primer instancia. Los requerimientos para la seguridad son complejos: confidencialidad, autenticación, no - rechazos e integridad. Pero los mecanismos utilizados para implantar estas medidas pueden ser muy complejos.
2. En el **desarrollo de un mecanismo** de seguridad, se deben considerar posibles medidas. En varios casos, las medidas se señalan visualizando el problema en una forma muy distinta a lo que ocurre en la práctica, y pueden surgir debilidades inesperadas en el mecanismo.
3. Los **procedimientos** utilizados para determinado servicio son frecuentemente intuitivos. No es obvio desde un estado o situación, que medida determinada sea necesaria.
4. Al tener el **diseño** de diversos mecanismos de seguridad, es necesario decidir donde se utilizarán. En términos del lugar físico, en que punto de la red se colocará el mecanismo. En términos lógicos, en que capa de la arquitectura.

5. Los mecanismos de seguridad usualmente involucran más que un determinado algoritmo o protocolo. Ellos generalmente requieren que el participante este en posesión de cierta **información secreta**. La cuestión recae en la creación, distribución y protección de esa información secreta. Además los protocolos de comunicación, por su funcionamiento complican el trabajo de desarrollo de los mecanismos de seguridad.

A continuación se revisarán los diferentes tipos de ataques que crean la necesidad para la seguridad en los servicios de red y los mecanismos que se desarrollan para la seguridad.

ATAQUES, SERVICIOS Y MECANISMOS

Para evaluar las necesidades de seguridad de una organización efectivamente y para seleccionar y evaluar diversos productos de seguridad y políticas, el administrador responsable de la seguridad debe buscar una forma sistemática de definir los requerimientos de seguridad y mostrar los modelos que satisfacen dichos requerimientos.

- ❖ **Ataques a la seguridad:** Cualquier acción que compromete la seguridad de la información que pertenece a la empresa.
- ❖ **Mecanismos de seguridad:** Mecanismo que es diseñado para detectar, prevenir o recuperar información de un ataque a la seguridad.
- ❖ **Servicios de seguridad.** El servicio que coloque en un entorno de seguridad a los sistemas y la transferencia de información de una organización.

ATAQUES A LA SEGURIDAD

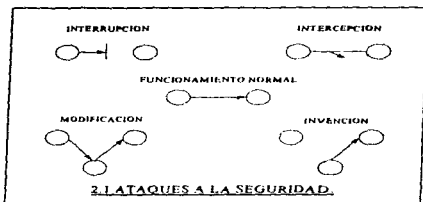
Los tipos de ataques en la seguridad de sistemas o redes son mejor caracterizados desde el punto de vista de las funciones que desempeña el sistema de computo como un proveedor de información. A continuación se muestra cuatro categorías generales de ataque:

- ❖ **Interrupción:** Una característica del sistema es destruida, no se puede disponer de ella, o es inhabilitada. Este es un ataque a la disponibilidad. Ejemplos son la destrucción de una pieza de hardware, destruir una línea de comunicación o deshabilitar el sistema operativo de la computadora.

- ❖ **Intercepción:** Un usuario no autorizado obtiene acceso a una característica del sistema. Es un ataque a la confidencialidad, el transgresor puede ser una persona, un programa o una computadora. Ejemplos, incluyen colgarse o intervenir un medio de comunicación para la captura de datos de la red, o realizar una copia ilícita de programas o archivos.

- ❖ **Modificación:** Un usuario no autorizado no sólo obtiene acceso a los archivos también puede falsificarlos a través del sistema. Este es un ataque a la integridad, ejemplos incluyen cambiar datos en un archivo, alterar un programa, o modificar el contenido de mensajes que se transmiten a través de la red.

- ❖ **Invencción:** Un usuario no autorizado inserta objetos falsificados en el sistema. Este es un ataque a la autenticidad. Ejemplos incluyen la inserción de mensajes falsos en la red o la adición de registros en archivos de datos.



MECANISMOS

No existe un mecanismo sencillo que por sí solo pueda proporcionar todos los servicios o desempeñar todas las funciones de seguridad. Como sea, no hay un elemento en particular que sobresalga en los mecanismos de seguridad más que las técnicas criptográficas. La encriptación o transformaciones de información es el medio más común para proporcionar seguridad.

SERVICIOS

Los documentos se utilizan en diversas actividades humanas, típicamente contienen firmas y fechas. Estos deben ser protegidos de falsificaciones, daño, etc. Por ello son notariados, atestiguados o sellados. Cada vez, más información electrónica toma el lugar de los documentos en papel. Diversos aspectos de los documentos electrónicos hacen de la función o servicio todo un reto.

La continua investigación y desarrollo de seguridad en las redes de computadoras se ha enfocado en tres o cuatro servicios generales, que acompañan a varias de las funciones requeridas para la seguridad de la información. La siguiente es una clasificación general de los servicios de seguridad:

- ❖ **Confidencialidad.** Requiere que la información transmitida en un sistema de computadora sea accesible sólo para su lectura a usuarios autorizados. Este tipo de accesos incluye impresión, desplegar, y otras formas de ver el documento, hasta poder revelar la existencia del objeto.
- ❖ **Autenticación.** Requiere que la identificación del origen del mensaje sea correcta, con la seguridad que la identificación no es falsa.
- ❖ **Integridad.** Requiere que las cualidades del sistema y la información transmitida sea modificada sólo por usuarios autorizados. Las modificaciones incluyen la escritura, cambios, borrar, crear, retrasar o retransmitir el mensaje.
- ❖ **No Rechazo.** Requiere que ninguno, ya sea el transmisor o el receptor puedan interrumpir la transmisión.
- ❖ **Control de acceso.** Requiere que el acceso a los recursos de información estén controlados por el sistema.
- ❖ **Disponibilidad.** Requiere que los características del sistema estén disponibles para autorizar servicios a usuarios cuando sea necesario.

2.2.4 MODELO PARA LA SEGURIDAD EN UN ENTORNO DE REDES

Si un mensaje es transferido de una computadora a otra a través de un entorno de redes, Las partes que están involucradas en la tarea deben cooperar para que se lleve a cabo exitosamente. Un canal lógico se establece al definir una ruta a través de la red o redes del origen a su destino, y por medio del uso de protocolos de comunicación por ambas partes.

Los aspectos de seguridad se toman en cuenta cuando es necesario o deseable proteger la transmisión de datos de un intruso, quien puede ser una amenaza para la confidencialidad, autenticación, etc. Todas las técnicas para proporcionar seguridad tienen dos componentes:

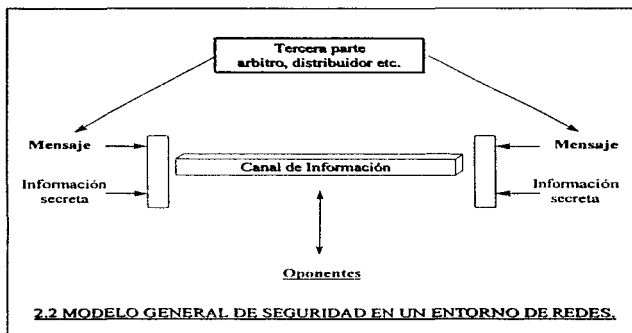
1. Una transformación de la información que se enviará. Ejemplo, la encriptación del mensaje, revolviendo la información para que ésta no pueda ser leída por el intruso, y adicionando código basado en el contenido del mensaje, el cual puede ser utilizado para verificar la identidad del transmisor.
2. Información secreta compartida por ambas partes, receptor y transmisor, y que se espera que no sea conocida por el oponente. Ejemplo, la llave de encriptación utilizada en conjunto con la transformación para revolver el mensaje antes de la transmisión y descifrarlo después en la recepción.

Una tercera parte puede necesitarse para asegurar la seguridad en la transmisión. La tercera parte puede ser el responsable de la distribución de la llave secreta a las partes involucradas y mantener esta información fuera del alcance de cualquier intruso.

El modelo general muestra que existen 4 tareas esenciales en el diseño de un servicio de seguridad:

1. **Diseñar** un algoritmo para el desarrollo de una seguridad. El algoritmo debe ser tal que un intruso no pueda transgredir el algoritmo.
2. **Generar** la información secreta que será utilizada con el algoritmo.
3. **Desarrollar** métodos o procedimientos para la distribución y poder compartir la información secreta.
4. **Especificar** un protocolo que sea utilizado por las partes que intervienen en la transmisión, que haga uso del algoritmo y de la información secreta para llevar a cabo el servicio de seguridad.

Este tipo de servicios y mecanismos encajan con el modelo de la **figura siguiente**. Como sea, existen otras situaciones acerca de la seguridad que no se consideran en este modelo. Otro modelo de seguridad es el que se refiere a la protección de los sistemas de información del acceso de un intruso. Se conoce de la existencia de piratas (hackers) que intentan acceder a un sistema a través de la red.

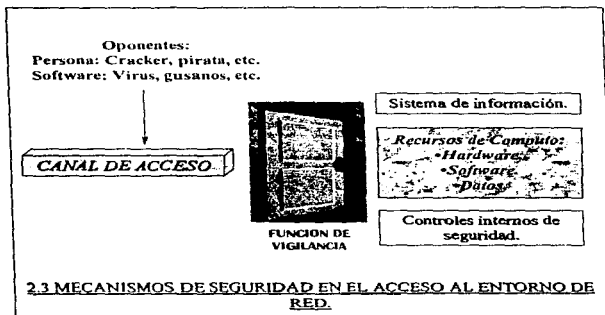


Otra clase de acceso no deseado es la posibilidad de explotar en forma lógica las vulnerabilidades del sistema y que pueden afectar aplicaciones y programas. Dos clases de amenaza pueden presentarse debido a programas de computadora:

1. Amenazas al acceso de información. Interceptar o modificar datos usurpando a usuarios que no deberían tener acceso a los datos.
2. Amenazas a los servicios. Explotar las fallas del servicio en la computadora para bloquear su uso por parte del usuario legítimo.

Los virus y gusanos son dos ejemplos de ataques por medio de programas. Dichos ataques pueden ser llevados al sistema a través de discos que contienen dicha lógica oculta, sólo mostrando el software de interés para el usuario. Pueden ser

introducidos al sistema mediante la red de trabajo, las consecuencias de este problema es una preocupación vital de la seguridad en un entorno de redes.



Los mecanismos de seguridad que se necesitan para prevenir el acceso no deseado recaen en dos grandes categorías:

1. Utilizar una función de **control de entrada** (gatekeeper) que incluye procedimientos para firmarse a la red y contraseñas diseñadas para aceptar sólo a usuarios autorizados, y software diseñado para detectar y rechazar los ataques de virus, gusanos y otros programas similares.
2. Una vez obtenido el acceso, ya sea por un intruso o software, la segunda línea de defensa consiste en una variedad de controles internos que estén **monitoreando** la actividad y analicen el almacenamiento de la información para detectar la presencia de un intruso.

2.2.5 EL LIBRO NARANJA

El centro nacional para la seguridad de computo NCSC (agencia de los E.U.) ha publicado un estándar oficial llamado "Criterios para la evaluación de sistemas de computo confiable", universalmente conocido como el Libro Naranja. El libro naranja define una serie de parámetros que un sistema de computo puede cumplir y las características para su diseño. Estos parámetros intentan dar al gobierno de E.U. y empresas un objetivo a cumplir en los sistemas de seguridad y a los fabricantes de software para colocar énfasis en la seguridad. Las categorías oficiales son:

- D** Protección mínima.
- C1** Protección de seguridad discrecional.
- C2** Protección de acceso controlado.
- B1** Protección de seguridad de etiquetas.
- B2** Protección estructurada.
- B3** Seguridad de dominios.
- A1** Diseño verificado.

Categorías que están en el rango de menos seguro a más seguro. En realidad, no existe ninguna forma para colocar las características en forma lineal. Diversas amenazas pueden ser de mayor o menor importancia dependiendo del entorno de computo. Los autores del libro naranja hicieron un esfuerzo por que estas características fueran lineales dadas sus prioridades.

³ Charlie Kaufman, et. al. Network Security. Private Communications in a Public World.

Pero el resultado puede ser confuso, por ejemplo, un sistema de clasificación A1 que no cumple con una característica sencilla puede ser clasificado como D. Los sistemas que no son diseñados bajo el esquema del libro naranja pueden obtener una clasificación muy baja y aun así, ser de hecho muy seguros.

El otro problema con la clasificación del libro naranja es que los diseñadores se enfocaron en prioridades de seguridad de la milicia (ocultar datos). En el mundo comercial la integridad de los datos es al menos igual de importante que la confidencialidad de los datos.

2.3 EL PLAN DE CONTINGENCIA Y RESTABLECIMIENTO

El objetivo del plan de contingencia y restablecimiento es asegurar la continuidad en la función de los sistemas de información del negocio, y que no se pierda la capacidad del procesamiento. Un desastre se define como ³“La pérdida de la capacidad del procesamiento de los sistemas de información en cualquier grado”.

El plan de contingencia y restablecimiento son medidas que se toman para restablecer el negocio a la normalidad lo más rápido posible después de una contingencia. El objetivo del plan debería ser reconocido como una condición de emergencia y requiere de procesos planeados para volver el negocio a un modo de operación normal tan pronto como sea posible.

En el caso de pérdida de la capacidad del procesamiento de los sistemas de información, los **usuarios son responsables** de la continuidad de su función hasta que el procesamiento pueda ser restablecido. Este es el elemento clave del plan de contingencia y restablecimiento.

Toda organización debe tener un plan de contingencia y restablecimiento ante un eventual desastre, plan probado y actualizado. El producto final, no es sólo un documento en papel, sino la capacidad probada ante una contingencia y el restablecimiento de la función de procesamiento de computo.

³ Royal P. Fischer. Seguridad en los Sistemas Informáticos.

2.3.1 PRIMER ETAPA: RESPUESTA DE EMERGENCIA

Un plan de respuesta de emergencia permite una acción inmediata a amenazas serias o catastróficas. Su objetivo es limitar el daño a recursos críticos, así como conservar la capacidad del negocio. Las amenazas de catástrofe naturales o actos humanos deben hacerse frente con acciones planeadas para preservar al personal, los recursos y a la organización. Varias estrategias pueden utilizarse para limitar inicialmente el daño de los recursos críticos y proteger la capacidad del negocio:

- ❖ Comunicar una alarma a todas las personas afectadas.
- ❖ Proteger los recursos humanos, equipo y datos de la organización.
- ❖ Evacuar y proteger a las personas.
- ❖ Proteger el equipo y datos esenciales.
- ❖ Probar el plan de respuesta de emergencia.
- ❖ Practicar ejercicios regulares aunque no programados.

2.3.2 SEGUNDO ETAPA: EL TRATAMIENTO INTERNO

Una vez que la emergencia se ha iniciado, se necesita un plan eficiente para manejar el periodo de tiempo entre la pérdida de capacidad de procesamiento de los sistemas de información y el restablecimiento. A este plan le llamaremos **plan de tratamiento interno**. Este plan proporciona la continuidad de la capacidad de procesamiento de la organización por la vía de cualquier medio hasta que tenga lugar el restablecimiento. Sus estrategias claves son:

- Definición de las responsabilidades de los usuarios.

⁴ Royal P. Fischer. Seguridad en los Sistemas Informáticos.

- Organización de planes alternativos nivel por nivel.
- Planes de acción individual.
- Identificación de configuraciones críticas.
- Identificación de las alternativas del procesamiento temporal de los sistemas de información.
- Asignación de las funciones del tratamiento interno (equipos y tareas).
- Medidas para una seguridad adecuada en una situación de procesamiento interno y temporal.
- Probar el plan de tratamiento interno.

2.3.3 TERCER ETAPA: LA RESTAURACION

El plan de restauración es el tercer mayor eslabón en la cadena que hemos denominado **plan de contingencia y restablecimiento**. Su objetivo es recuperar la capacidad de procesamiento primario una vez perdido. Las actividades integrales de este plan son:

- Determinar el estado de las instalaciones.
- Proporcionar tareas bien definidas al personal.
- Contar con el personal y reasignarlo si es necesario. Establecer comunicaciones entre la dirección y todo el personal.
- Identificar posiciones alternativas de trabajo.
- Identificar la fuente para la reposición del equipo, incluyendo facilidades en las comunicaciones.
- Identificar la fuente para la reposición de datos y software. Se debe contar con un plan de respaldo de datos y software, dicha tarea está relacionada con las funciones del inventario.

- Proporcionar disponibilidades de datos y suministros.
- Crear copias múltiples del plan de restauración.
- Distribuir copias del plan de restauración en caso de que la organización este distribuida en diverso lugares.
- Probar el plan de restauración.

EL CONTROL DE ACCESO

Por último, el control de acceso tiene el objetivo de restringir el acceso y salida a un lugar, sólo para aquellas personas que trabajan ahí. Se pueden aplicar diferentes mecanismos como: La instalación de alarmas, un distintivo codificado, claves y sistemas de tarjeta utilizadas en muchas organizaciones.

Un requisito necesario en esta fase de control que se llega a omitir generalmente, es el acceso controlado del personal **durante e inmediatamente después** de un desastre.

2.4 EL INVENTARIO

Muchas organizaciones con infraestructura de computo no tienen un registro físico actual de todos los recursos que residen en las instalaciones y almacén. Peor todavía, muchos no tienen registrados dónde están situados los recursos.

Debe considerarse por una parte los programas, aplicaciones, paquetes de software y datos para el inventario. Así como todos elementos de hardware, telecomunicaciones y demás recursos que estén relacionados con los sistemas de información.

Los elementos que componen la infraestructura de computo y sistemas de información de la organización deben estar declarados como propiedad de la compañía y controlados correctamente. Ningún grado de protección puede estar en modo alguno asegurado, si el inventario de los datos no está totalmente definido. El inventario debe ser real y debe estar actualizado.

El objetivo de un inventario es obtener información fidedigna del registro de recursos, prevenir fraudes, prevenir robos y salvaguardar información. El inventario de los recursos de computo debe cumplir con determinados **principios** generales, que a continuación mencionamos:

1. Separación de las funciones de **adquisición, custodia y registro contable**.
2. Ninguna persona que interviene en **inventarios** deberá tener acceso a los registros contables que controlen su actividad.
3. El trabajo del personal de inventarios debe ser una **función integral** y no sólo de revisión.

4. La base de la evaluación de inventarios será constante y consistente, y evidentemente bajo la guía de las políticas de la Gerencia y del departamento de sistemas.

Debemos mencionar que la **evaluación de los recursos** es la base del **análisis de riesgos**, éste análisis es un parámetro de medida para cuantificar los riesgos y luego entonces **implantar controles** eficientes y viables en todo el entorno de sistemas de información de la organización.

2.4.1 EVALUACION DE INVENTARIOS

Los inventarios de productos tangibles, como el software adquirido por la empresa y el hardware pueden ser evaluados generalmente a precio de costo o a precio de mercado. Es necesario dar un peso de responsabilidad a estas tareas, bajo la guía de la Gerencia, el departamento de sistemas y el departamento de auditoría.

La **base para el control**, inicia en la evaluación del inventario, continua con el análisis de riesgos y posteriormente la implementación e implantación del control. Los métodos generales de precios y costos para la evaluación de inventarios son:

1. Precio de mercado.
2. Costo de adquisición.
3. Costo promedio.
4. Costo PEPS (Primero en Entrar, Primero en Salir).
5. Costo UEPS (Ultimo en Entrar, Primero en Salir).
6. Costo específico.
7. Costo de producción marginal.

8. Costo Histórico.
9. Costo Estimado.
10. Costo Estándar.

2.4.2 EL RESPALDO DE DATOS

Antes de que los datos puedan ser **respaldados** y **protegidos**, éstos deben ser identificados. La siguiente clasificación muestra la importancia de los datos para la empresa:

- ❖ **Datos vitales.** La pérdida de estos datos podría acabar con la función de la organización.
- ❖ **Datos esenciales.** La pérdida de esta información rompería ciertamente la operación. Aunque la organización puede sobrevivir, el nivel de operación y productividad estaría seriamente afectado.
- ❖ **Datos importantes.** La pérdida de estos datos causa molestias, pero rara vez un bloqueo de la operación.
- ❖ **Registros útiles.** La pérdida de estos registros produce retrasos en la operación de la organización. Son frecuentemente examinados como no esenciales y llegan a ser encontrados como no muy necesarios.

El respaldo de datos debe funcionar bajo los métodos más eficientes y económicos para proteger estos registros, y para poder **disponer** de ellos de una forma rápida, y tomar en cuenta la **relación** tan estrecha con las operaciones del plan de contingencia y restablecimiento. El **objetivo** es recuperar íntegra y fácilmente los datos después de un desastre en la organización.

2.5 LOS RECURSOS HUMANOS

Para los efectos de la función de la unidad de computo consideramos que los recursos humanos son los elementos con que cuenta la organización, para promover el logro de las metas y objetivos. La contratación de recursos humanos está a cargo de otro departamento, pero la decisión final de contratación y la administración del personal del área de sistemas debe ser una facultad total del departamento de sistemas.

LOS RECURSOS HUMANOS COMO UN SISTEMA

Los elementos humanos se encuentran interrelacionados con otros elementos, recursos materiales y técnicos, que coordinados mediante un proceso lógico permiten el logro de metas y objetivos. Por lo anterior, conviene notar la importancia de los recursos humanos considerando que estos pueden modificar y perfeccionar el desempeño de la función del departamento de sistemas.

2.5.1 PLANEACION DE LOS RECURSOS HUMANOS

Se considera a la planeación como el proceso organizado mediante el cual se establecen directrices, se definen estrategias, se seleccionan alternativas y cursos de acción por parte de la dirección y de la unidad de computo, de acuerdo con la disponibilidad de recursos.

Por ello, es conveniente que en esta etapa se relacionen las metas y objetivos de la organización con el presupuesto y recursos ya existentes, a fin de determinar el

estado actual de la organización con respecto a los recursos. El personal disponible y las necesidades reales reflejadas en los programas y presupuestos aprobados.

RECLUTAMIENTO

“El reclutamiento es el proceso de promoción que tiene como finalidad localizar y atraer candidatos idóneos que estén interesados en ocupar puestos vacantes. Constituye el nexo entre la planeación y la selección de personal. Consiste en crear una cartera de candidatos, los cuales serán seleccionados posteriormente con base en sus habilidades, capacidades y experiencias”.

SELECCION DE PERSONAL

Se puede definir a la selección de personal como la elección de la persona adecuada para el puesto adecuado con el costo adecuado para la organización, de tal manera que permita la realización del trabajo a su cargo, con el medio ambiente idóneo, para que de esta manera contribuya al logro de los objetivos de la empresa.

CONTRATACION DE PERSONAL

Una vez aceptado el candidato, se lleva a cabo el acto de contratación, mediante el cual se establece una relación de trabajo entre el que presta un servicio y el que lo recibe, quien se compromete al pago de un sueldo o salario. Finalmente, conviene precisar que la organización deberá entregar el pago directamente al beneficiario o apoderado, y cubrir al pie de la letra todos los aspectos legales de la relación laboral.

⁵ **IMCP. Normas y Procedimientos de Auditoría.**

**2.6 NORMAS Y PROCEDIMIENTOS PARA EL CONTROL EN LA UNIDAD DE
COMPUTO**

El siguiente resumen es una lista general de los elementos de control que se tienen en las actividades de la unidad de cómputo o departamento de sistemas de la organización:

❖ **Planeación y administración de recursos.**

- Presupuesto anual de las operaciones del departamento de sistemas.
- Plan anual de adquisición de equipo.
- Evaluación de rendimiento del equipo.

❖ **Operación.**

- Programa de cargas de trabajo.
- Distribución de personal.
- Calendario de mantenimiento: Hardware y software.
- Evaluación de la efectividad de los itinerarios y calendarios.
- Proyectos con cambio de recursos.
- Contabilidad de los trabajos.
- Procedimientos de facturación a usuario, si es que existen.
- Asignación de responsabilidades en el respaldo y almacenamiento de datos.
- Identificación de archivos.
- Revisión de operaciones.

❖ **Software no desarrollado dentro de la empresa.**

Selección de software.

Análisis costo/beneficio del software.

Instalación del software.

Mantenimiento del software.

Procedimientos para el cambio o actualización del software.

Implementación de cambios en el ambiente de uso del software.

Registro de los cambios hechos en el ambiente de uso del software.

Análisis de la seguridad que ofrece el software.

❖ **Control de acceso y seguridad.**

Responsabilidad para el control de acceso y seguridad física.

Acceso al departamento de sistemas de información (instalaciones).

Escolta de visitantes.

Acceso físico al equipo: nodos de red, minicomputadoras, mainframes, etc.

Bitácora o reporte de actividades del uso del equipo.

Acceso a la Biblioteca, si cuenta con una la empresa.

Acceso en línea a programas y datos.

Prácticas de seguridad.

Protección contra desastres.

Protección física de archivos.

Medidas de seguridad para documentos finales y formatos.

Capacitación en conocimientos y procedimientos de seguridad.

Pruebas de los planes de seguridad.

❖ **Contingencia, Restablecimiento y Respaldo.**

Plan de contingencia y restablecimiento en caso de siniestro.

Procedimientos de emergencia y capacitación para seguridad del personal.

Identificación de las aplicaciones críticas.

Identificación de recursos críticos.

Servicios de comunicación.

Equipo de respaldo.

Programación de las operaciones de respaldo de equipo y datos.

Procedimiento para respaldo de equipo y datos.

Pruebas del plan de respaldo.

Reconstrucción del departamento de sistemas de información.

Procedimientos manuales de respaldo.

❖ **Recursos humanos.**

Procedimientos de reclutamiento.

Selección de personal.

Contratación del personal.

2.7 RESUMEN

La unidad de computo o departamento de sistemas es el responsable y el que toma las decisiones dentro de la empresa en cuanto a los aspectos de sistemas de información. Su funcionamiento requiere de un esquema de control, es importante que una organización visualice el trabajo de su unidad de computo y se comprometa a trabajar con esta unidad. Un problema muy grave es que la Gerencia de la empresa no realice éste trabajo, estaría en desventaja ante sus competidores y ante sí misma.

- ❖ El departamento de sistemas debe tener políticas o líneas de acción bien definidas. Las políticas para las funciones y responsabilidades de la unidad de computo deben estar apoyadas en planes y programas para poder surtir efecto.
- ❖ La seguridad es el segundo punto en este marco, la seguridad física y lógica es una tarea vital en el funcionamiento de la unidad de computo, donde partimos de la siguiente base:
 - Funciones y responsabilidades de cada departamento en el uso de instalaciones, equipo y de la información.
 - La seguridad de datos en general y los elementos de control.
 - La seguridad en un entorno de redes (internetwork), que consiste en medidas para determinar, prevenir, detectar y corregir violaciones a la seguridad que involucra la transmisión de información. También, para evaluar las necesidades de seguridad de información dentro de una organización.

- ❖ La unidad de computo debe contar con un plan de contingencia y restablecimiento, ya que la organización debe poder hacer frente a cualquier problema que pudiese presentarse y que afecta el funcionamiento de la unidad de computo y a los sistemas de información, se debe poder continuar operando bajo circunstancias anormales. Se presenta la siguiente propuesta dividida en 4 etapas: La respuesta de emergencia, el tratamiento interno (tiempo entre la emergencia y el restablecimiento), la restauración y el control de acceso a las instalaciones.

- ❖ El control del inventario de equipo debe ser una función de la unidad de computo, y lo más importante este inventario debe ser fidedigno, real. Esta función es la base del análisis de riesgos y de la siguiente etapa que es la implantación de controles.

- ❖ La actividad de reclutamiento es de gran importancia para la unidad de computo, la unidad de computo debe estar ligada desde un inicio al reclutamiento de su personal y estar trabajando conjuntamente con las áreas que lleven a cabo dicho proceso dentro de la empresa.

CAPITULO 3
EL CONTROL EN LAS APLICACIONES
(SISTEMAS DE INFORMACION EN OPERACION)

3.1 LOS SISTEMAS DE INFORMACION.

3.2 EL CONTROL DE LA INFORMACION.

3.3 NORMAS Y PROCEDIMIENTOS PARA EL CONTROL EN LAS APLICACIONES.

3.4 RESUMEN.

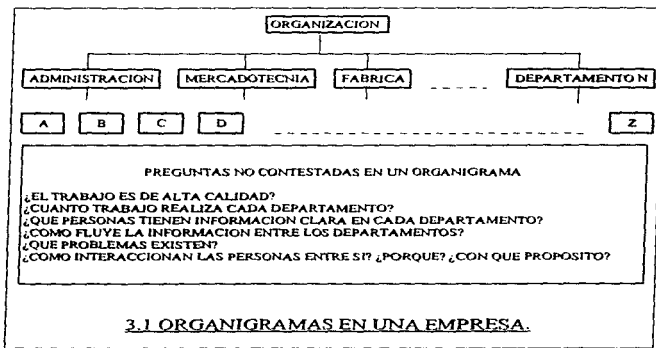
3.1 LOS SISTEMAS DE INFORMACION

Dado que los sistemas de información en una empresa son el soporte para el funcionamiento de la organización, los analistas tienen primero que estudiar el sistema organizacional como un todo, para entonces detallar los sistemas de información.

Los organigramas se emplean con frecuencia, para describir la forma en que están relacionados los diferentes componentes de la organización, tales como divisiones, departamentos, oficinas y empleados. Aunque los organigramas indican con precisión las relaciones formales entre los diferentes componentes no dicen nada con respecto a la forma en que opera el sistema organizacional; ya que en este tipo de diagramas no es posible plasmar todos los detalles importantes. A continuación se mencionarán los aspectos más importantes para el desarrollador de sistemas:

- ❖ **Canales informales.** Que interacciones existen entre las personas y los departamentos que no aparecen en el organigrama o no están descritos en los procedimientos de operación.
- ❖ **Interdependencias.** De que otros departamentos y componentes de la organización depende un elemento en particular.
- ❖ **Personas y funciones clave.** Cuales son las personas y elementos más importantes en el sistema para que este tenga éxito.
- ❖ **Enlaces críticos de comunicación.** Como es el flujo de información e instrucciones entre los distintos componentes de la organización y como se comunican las áreas entre sí.

La lista anterior no es exhaustiva, pero engloba la importancia de investigar y analizar la manera en que operan las organizaciones, esto con el propósito de establecer los controles y validar la confiabilidad de los sistemas de información que están operando en la compañía.



En contraste, durante el diseño los desarrolladores tienen la responsabilidad de identificar las características importantes y necesarias que deben tener los nuevos sistemas. El desarrollador especifica la forma en que va a operar el sistema y sus módulos, las entradas requeridas, las salidas que se deben producir y los trabajos que se efectúan tanto por las computadoras como en forma manual.

Por otro lado, los desarrolladores también participan en el control de los sistemas básicamente en dos formas: La **primera** cuando describen los elementos de control, tales como estándares y métodos para evaluar el desempeño del sistema en relación con los demás estándares desarrollados hasta ese momento. La **segunda**, al concluirse estos sistemas, la información proporcionada a los directivos y usuarios permite que estos determinen si los sistemas que administran operan correctamente.

Incorporar mecanismos de retroalimentación es un paso esencial en el diseño ya que su inclusión permite sostener las actividades de proceso y control. Ninguno de los sistemas perdurará si falta un control adecuado.



3.1.1 CATEGORIAS DE LOS SISTEMAS DE INFORMACION

El analista de sistemas desarrolla diferentes tipos de sistemas de información para satisfacer las diversas necesidades de una empresa. Bajo la teoría de sistemas de información, tenemos la siguiente clasificación:

- ❖ **Sistemas para el procesamiento de transacciones.** Sustituye los procedimientos manuales por otros basados en computadora. Trata con procesos de rutina bien estructurados. Incluye aplicaciones para el mantenimiento de registros.
- ❖ **Sistemas de información administrativa.** Proporciona la información que será empleada en los procesos de decisión administrativos. Trata con el soporte de situaciones de decisión bien estructuradas. Es posible anticipar los requerimientos de información más comunes.
- ❖ **Sistemas para el soporte de decisiones.** Proporciona información a los directivos que deben tomar decisiones sobre situaciones particulares. Apoyan la toma de decisiones en circunstancias que no están bien estructuradas.

SISTEMAS PARA EL PROCESAMIENTO DE TRANSACCIONES

Los sistemas de información más importantes dentro de una organización son los que están relacionados con el procesamiento de las transacciones. Los sistemas de procesamiento de transacciones tienen como finalidad mejorar las actividades rutinarias de una empresa y de las que depende toda la organización.

¹ James A. Senn. Análisis y Diseño de Sistemas de Información.

Una transacción es cualquier suceso o actividad que afecta a toda la organización. Las transacciones más comunes incluyen: facturación, entrega de mercancía, pago a empleados y depósito de cheques. Los tipos de transacciones cambian en cada una de las diferentes organizaciones. Sin embargo, la mayor parte de las compañías procesan dichas transacciones como una mayor parte de sus actividades cotidianas. ²“Las empresas con mayor éxito llevan a cabo este trabajo en una forma ordenada y eficiente”.

Todas las actividades que forman parte del nivel operacional de cualquier organización muestran la existencia de características similares entre ellas:

1. Gran volumen de transacciones.
2. Gran similitud entre las transacciones.
3. Los procedimientos para el procesamiento de transacciones están bien comprendidos y se pueden describir con detalle.
4. Existen muy pocas excepciones a los procedimientos normales.

Estas características permiten establecer rutinas para el manejo de transacciones. Las rutinas describen que buscar en cada transacción, los pasos y procedimientos a seguir, y lo que debe hacerse en caso que se presente una excepción. Los **procedimientos para el proceso** de transacciones se denominan procedimientos de operación estándar, y son los **puntos claves en el control** de un sistema de información en operación.

² James A. Senn. Análisis y Diseño de Sistemas de Información.

Capítulo 3. El control en las aplicaciones.

Un gran volumen de transacciones exactas, asociado con el nivel operativo de una organización, conduce a la necesidad del implantar sistemas de información. Muchas empresas comienzan a buscar este tipo de ayuda porque necesitan desarrollar formas más eficientes y eficaces para procesar los datos de una transacción. Lo anterior es cierto tanto para empresas grandes como pequeñas. Los procedimientos forman parte de los programas de computadora que controlan la entrada de datos, el procesamiento de los detalles y la presentación de los datos y la información en sí.

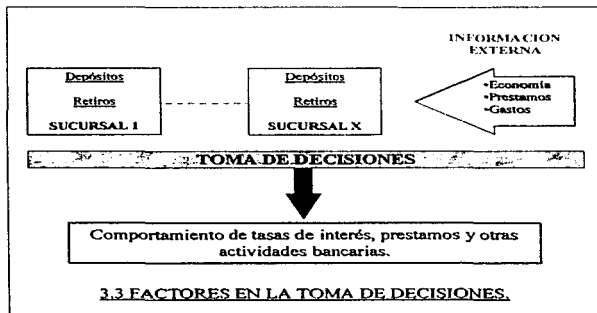
SISTEMAS DE INFORMACION ADMINISTRATIVA

Los sistemas de transacciones están orientados hacia operaciones. En contraste, los sistemas de información administrativa ayudan a los directivos a tomar decisiones y resolver problemas. Los directivos recurren a los datos almacenados como consecuencia del procesamiento de las transacciones, pero también emplean otra información.

En cualquier organización se deben tomar decisiones sobre muchos asuntos que se presentan con regularidad (diario, semanalmente, mensual, anual, etc.) y para hacerlo se requiere de cierta información. Dado que los procesos de decisión están claramente definidos, entonces se puede identificar la información necesaria para formular la mejor presentación. Se pueden desarrollar sistemas de información para que, en forma periódica se preparen reportes para el soporte de decisiones. Cada vez que se necesita la información, esta se prepara y presenta en un formato diseñado con anterioridad.

Con frecuencia, los especialistas en sistemas de información describen las decisiones apoyadas por estos sistemas como decisiones estructuradas. El aspecto estructurado se refiere al hecho de que los administradores conozcan de antemano los factores que deben tenerse en cuenta para la toma de decisiones así como las variables con influencia más significativa sobre el resultado de una decisión (buena o mala). A su vez, los analistas de sistemas desarrollan reportes bien estructurados que contienen la información necesaria para las decisiones o que indican el estado de las variables importantes.

Con frecuencia la información proporcionada se combina con otra de naturaleza externa. Con esta información los funcionarios de la organización pueden tomar decisiones con respecto a los rubros de la empresa. La necesidad de tomar una decisión se presenta con cierta frecuencia, como ya se mencionó y por lo tanto, la información necesaria para ello debe prepararse con regularidad.



SISTEMA PARA EL SOPORTE DE DECISIONES

No todas las decisiones son de naturaleza recurrente. Algunas se presentan sólo una vez o escasamente. Los sistemas para el soporte de decisiones ayudan a los directivos que deben tomar decisiones no muy estructuradas. Una decisión se considera no estructurada si no existen procedimientos claros para tomarla y si tampoco es posible identificar con anticipación, todos los factores que deben considerarse en la decisión.

Un factor clave en el uso de estos sistemas es determinar la información necesaria. En situaciones bien estructuradas es posible identificar esta información con anticipación, pero en un ambiente no estructurado resulta difícil hacerlo. Conforme se adquiere la información, puede ocurrir que el gerente se de cuenta que se necesita más información; es decir, tener información puede conducir a otros requerimientos.

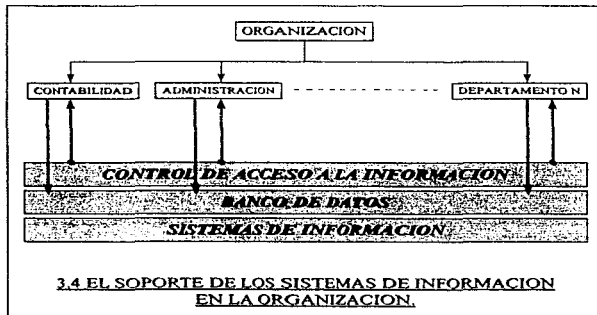
En estos casos es imposible diseñar de antemano tanto el formato como el contenido de los reportes del sistema. En consecuencia, los sistemas para el soporte de decisiones deben tener una flexibilidad mayor que la de los demás sistemas de información.

El usuario debe ser capaz de solicitar informes definiendo su contenido y especificando la forma para producir la información. De manera similar, los datos necesarios para generar la información pueden encontrarse en diferentes archivos o base de dato más que en un solo archivo maestro, que es el caso más frecuente en los sistemas de transacciones y en muchos otros sistemas que generan reportes.

El criterio de los gerentes tiene un papel importante en la toma de decisiones donde el problema no es estructurado. Los sistemas para el soporte de decisiones ayudan pero no reemplazan el criterio del directivo.

3.1.2 VISION DE LOS SISTEMA DE INFORMACION

Como se mencionó en el punto anterior, en cualquier organización existen varios tipos de sistemas de información. Desde el punto de vista de la estructura de la organización, los sistemas de información se forman a partir de las tareas de la empresa como mercadotecnia, manufactura, compras y otras funciones de la empresa. Cada una de estas funciones comprende actividades a nivel de transacciones, toma de decisiones, junto con la ocurrencia de requerimientos únicos y aplicaciones para el soporte de decisiones en oficinas y departamentos.



Lo anterior permite comprender por que las diferentes funciones comerciales de una organización necesitan el soporte de los sistemas de información, es decir cada función de la empresa tiene diferentes tareas que realizar. Y esta es la forma en que evolucionan los sistemas de información dentro la organización.

“Hace algún tiempo se especulo en torno a los sistemas de información totales; sistemas de información administrativa únicos que permitieran satisfacer las necesidades de una organización en todos sus niveles y funciones comerciales. Sin embargo, en la actualidad no prevalece este punto de vista. Los administradores se han dado cuenta que es imposible y peligroso intentar construir un sistema de información monolítico”.

³ James A. Senn. Análisis y Diseño de Sistemas de Información.

3.2 EL CONTROL DE LA INFORMACION

La función de la alta gerencia es establecer políticas claras y precisas sobre el control de la información. Otra vez, necesitamos planes y programas para **producir una normatividad** sobre el control y flujo de la información. Debe existir una norma que defina que información es realmente confidencial o restringida dentro de la empresa.

La información proporciona mando en el sentido de poder. Es decir, el administrador o empleado que guarda información para sí mismo, es un problema para toda la organización. El empleado que realiza esta táctica en su desempeño rechazará cualquier sugerencia o idea de sus subordinados, su objetivo es personal y no en beneficio de la organización. Como consecuencia se presentará un alto grado de ineficiencia en el trabajo.

Tres aspectos que se deben eliminar y tomar en cuenta para generar una normatividad y los procedimientos de control de la información son:

1. **Distorsión de la información.** Barreras al proporcionar la información o en el flujo de la información.
2. **Reglas y regulaciones.** Un grupo puede establecer procedimientos escritos con el sólo propósito de **darse a notar**.
3. **Canales de información informales.** El grupo afectado por las regulaciones utilizará canales informales **no apropiados de comunicación** para obtener la información.

3.2.1 LA ADMINISTRACION DE LOS SISTEMAS DE INFORMACION

El gran alcance de los sistemas en la teoría de organizaciones, es que estos abarcan en su concepto contribuciones de un gran número de disciplinas, desde la ingeniería hasta las ciencias sociales. Los sistemas dentro de una organización traslapan e interrelacionan las partes, las estructuras y a los miembros. Por ello es muy importante el control del flujo de la información, determinada información sólo puede ser accesada por algunos miembros de la organización dependiendo del puesto y de las funciones del departamento.

En la teoría de organizaciones los sistemas son de diversos tipos lógicos, ya sea todo un proceso de la organización o componentes mayores de otros sistemas. Los sistemas son definidos por su propósito e involucran procesos a través de la estructura de la organización. Un sistema dentro de la organización se puede ver desde diferentes enfoques y debe existir un control para hacer válido dicho enfoque.

Los sistemas de información, así como todo en el diseño organizacional, necesita ser apropiadamente diferenciado. Se puede analizar esta diferencia visualizando el propósito para el cual fue desarrollado el sistema.

EL PROPOSITO DE UN SISTEMA

Existen diferentes maneras de clasificar los sistemas dentro de una organización, por ejemplo, podemos hacer una clasificación por funciones: el control del inventario, afiliaciones a un departamento, etc. Sin embargo, bajo la teoría de organizaciones, podemos definir 4 posibles propósitos para los cuales puede funcionar un sistema.

1. **Planeación.** Conjuntar información para preparar programas estratégicos, tácticos o de acción.
2. **Logística.** El flujo de información necesario para ligar partes de la organización, para permitir que determinadas acciones ocurran o se detengan.
3. **Control.** La información que es requerida para monitorear el trabajo en la organización, para apuntar a los requisitos para una acción correctiva o para el mejoramiento de la actividad. El control tiene un sentido de monitoreo **no de administración dentro** de la teoría de organizaciones.
4. **Motivación.** La información es utilizada para dar al individuo o al grupo respaldo y motivación. Metas y objetivos, información general sobre la organización son temas de esta categoría.

Si el propósito no es reconocible en primera instancia, como sea, las características de un sistema de información determinan la clase de datos que se manejan y como se manejan. Se debe considerar en primer término el tipo de datos, en segundo el impacto del comportamiento del sistema de información y tercero considerar el objetivo del sistema dentro de la organización.

Un acuerdo o convención que es ventajosa o pertinente para un propósito no lo es tal vez para otro. Lo que es importante para un individuo o departamento , tal vez no lo es para otro, aún objetos contados físicamente. Todo depende de la definición arbitraria del proceso. La creencia que los números son hechos, proviene del uso de la computadora, sin embargo, los números se pueden almacenar de diversas formas y diferentes lugares. Por ello, requerimos de convenciones y controles en el flujo de la información para validar los datos como un hecho.

Frecuentemente, el individuo es afectado por el posible uso de los números para propósitos de control y evaluación. El desempeño de un individuo puede estar por debajo de su potencial, si la organización planea sólo en base a números, en este caso la meta para el individuo es simplemente subsistir en la organización, mientras que la organización cumple con sus objetivos y metas menores.

En lugar de ello, se deberían de hacer dos preguntas claves para el beneficio de la organización y el desempeño de los individuos: ¿Para qué es la información y para quién es la información ?. Estas preguntas nos llevan a considerar los siguientes puntos:

1. **Los grados de exactitud**, el detalle y la urgencia variarán con el propósito. Por ejemplo, una organización multinacional famosa por su sistema de información, el cual, en una cuenta producía 12,000 diagramas que cada mes iban a las gerencias divisionales. Donde la mayoría de los gerentes de producción y ventas encontraron, que se les daba mucha información y demasiado tarde. Estos gerentes, con algo de ingenio, ideaban sus propios sistemas, tal vez inexactos pero en tiempo real y sencillos. El sistema central fue diseñado en el centro y es útil ahí para propósitos de monitoreo.
2. **Quien controla la información en efecto controla la operación.** Si la información es con propósitos de control, los datos generados en territorios de un individuo deben de ser de su posesión, al menos en primera instancia. En una fábrica los datos de análisis de la producción van primero al supervisor responsable, para actuar según el caso. Si no se toma alguna acción correctiva o no se debe entregar algún informe o explicación dicha información será entregada hasta después de transcurrido algún tiempo límite a sus superiores.

Por ejemplo, los gerentes de ventas, quienes producen la primera prueba de los registros de ventas sin notificarlo mensualmente a sus gerentes superiores, indudablemente han incrementado su control, pero han privado de independencia a sus superiores e inferiores y consecuentemente el compromiso, iniciativa e incentivos.

3. Como deben ser los datos recopilados. Particularmente con propósitos de mantenimiento, y frecuentemente de control, debería ser posible definir los datos requeridos que pueden ser recolectados automáticamente y rutinariamente. Las preferencias individuales o errores pueden ser evitados haciendo que los datos sean independientes de los individuos. Las operaciones de nómina, los procedimientos de facturación, las medidas de control las cuales esencialmente apuntan a desviarse de la norma. Como sea, es importante considerar quien debe tener el derecho de modificar o alterar datos en el sistema contra la posibilidad de un fraude o error. Aspectos importantes en la seguridad de datos.

Por último, no es probable que alguien se sienta comprometido con los planes que surgen de otro departamento ajeno excepto por los miembros de ese departamento. Varias buenas ideas pueden ser rechazadas e ignoradas en los departamentos por lo que se conoce como el *síndrome de NIH (No Inventado Aquí, por sus siglas en inglés). Los datos y las ideas son extraños por aquellos quienes las tendrán que llevar a cabo, y son posteriormente rechazadas. La propiedad de los datos no es una característica transferible.

* Charles B. Handy. Understanding Organizations.

3.3 NORMAS Y PROCEDIMIENTOS PARA EL CONTROL EN LAS APLICACIONES

A continuación se mencionan en los puntos generales más importantes del control en los sistemas de información que están en operación dentro de la organización:

❖ **Control de los datos fuente.**

- Procedimientos en la preparación de los datos. (Datos de entrada a un sistema).
- Diseño de documentos fuente. (La fuente donde se toman los datos de entrada).
- Control de los documentos fuente.
- Procedimientos para la autorización de entrada de datos.
- Procedimientos para documentación y control de la operación.
- Vigilancia de los documentos fuente.

❖ **Control de los datos de entrada.**

- Procedimientos de conversión y/o entrada de datos. (Si es requerida una conversión de datos).
- Procedimientos de conversión y/o entrada en línea. (Si es requerida una conversión de datos).
- Validación y edición de datos.
- Manejo de errores en la entrada de datos.

❖ **Control del procedimiento de datos.**

- Integridad en las condiciones iniciales del sistema.
- Integridad del procesamiento de datos.
- Validación y edición en el procesamiento de datos.

Manejo de errores en el procesamiento de datos.

Prohibir la anulación de banderas, etiquetas o errores en dispositivos.

Restringir la intervención de los operadores.

Reporte de los procedimientos de reproceso.

Identificación y seguimiento de errores de procesamiento.

Informes auxiliares de errores por computadora.

Procedimientos de "Stop" y "Restart" en caso de mal funcionamiento del equipo.

Bitácora del sistema.

❖ **Control en la salida de la información.**

Revisión de la salida de datos.

Conciliación y balanceo de resultados.

Distribución de las salidas o resultados. (Flujo de la salida).

Manejo de errores en la salida de datos.

Manejo y retención de la salida de datos.

Medidas de seguridad para los reportes de salida.

3.4 RESUMEN

El control de los sistemas de información en operación (aplicaciones) consiste en verificar los elementos de entrada/salida, los procesos y los procedimientos de control que rodean a un sistema en su funcionamiento. Existe una relación estrecha entre el funcionamiento de un sistema y el departamento en el que opera. Los esquemas de control en el desarrollo de sistemas y en el funcionamiento del sistema, como se ha descrito son totalmente distintos.

El control en este capítulo se refiere a los procedimientos que se tienen en la entrada de datos a los sistemas, los procesos que pueden validarse a través de datos de control en el sistema, la salida de datos del sistema y el flujo de información en toda la empresa. Debemos considerar dos tareas muy importantes de inicio:

1. **Conocer a la organización.** Las funciones y responsabilidades por departamento.
2. **Entender los procedimientos de entrada de datos, salida de datos, procesamiento de datos y los procedimientos de control.**

La naturaleza de una aplicación y el entorno de la función de los sistemas de información involucra más el trabajo de áreas administrativas. Bajo este entorno, los sistemas de información se clasifican de la siguiente forma:

- Sistemas para el procesamiento de transacciones.
- Sistemas de información administrativa.
- Sistemas para el soporte de decisiones.

Cada departamento en la organización tiene sus requerimientos y maneja determinada información, es importante visualizar cuales son los elementos que pueden considerarse generales o comunes para toda la organización y los elementos que son particulares de cada área.

El control del flujo de información debe estar sustentado sobre políticas claras y directas de la Gerencia, y con ello desarrollar normas explícitas considerando eliminar los siguientes puntos:

- Distorsiones en la información que pueda ocasionar un departamento.
- Reglas y regulaciones inventadas por un departamento.
- Canales de información informales.

El flujo de información es el elemento base para el control en los sistemas de información que están operando. Los sistemas de información también se pueden clasificar por su propósito: Planeación, logística, control y/o motivación.

Todos los sistemas de información que estén funcionando en nuestra organización necesitan un esquema de control. Nuestra meta es verificar como esta funcionando el sistema: Los datos de entrada, los procesos y por supuesto la salida de datos. Ya que para la empresa es vital la información generada por las aplicaciones.

CAPITULO 4

EL CONTROL GERENCIAL

- 4.1 LA PLANEACION EN EL AREA DE SISTEMAS DE INFORMACION DENTRO DE LA ORGANIZACION.**
- 4.2 DEFINICION DE POLITICAS, ESTANDARES, NORMAS Y PROCEDIMIENTOS.**
- 4.3 DEFINICION DE RESPONSABILIDADES Y FUNCIONES EN CADA AREA DE LA ORGANIZACION.**
- 4.4 LA ADQUISICION DE EQUIPO Y SERVICIOS.**
- 4.5 REQUERIMIENTOS EXTERNOS.**
- 4.6 NORMAS Y PROCEDIMIENTOS PARA EL CONTROL GERENCIAL.**
- 4.7 RESUMEN.**

**4.1 LA PLANEACION EN EL AREA DE SISTEMAS DE INFORMACION
DENTRO DE LA ORGANIZACION**

Los avances en tecnología presentados en las últimas tres décadas han cambiado la situación de toda gerencia administrativa en una organización. Hoy en día hay que trabajar y desempeñar diversas operaciones utilizando equipo de cómputo, los sistemas de información son muy importantes en las actividades de una empresa.

Una empresa puede ser menos competitiva ante otras, por la falta o inadecuada infraestructura de cómputo y la planeación de los sistemas de información. Además, como toda operación de la empresa debe existir un control para los sistemas de información. En este punto surge una gran incógnita, si la gerencia administrativa y la gerencia de auditoría conocen la importancia de los sistemas de información y su control.

El objetivo más importante del control gerencial es crear el ambiente propicio para que el departamento de sistemas construya la estructura de control en todas las áreas de sistemas de información dentro de la empresa. El departamento de sistemas debe considerar las políticas de la Gerencia como una guía, sin olvidar la función de investigación e innovación.

La planeación en esta área era simplemente técnica en el pasado, enfocándose en el hardware y software. Con el desarrollo de sistemas estratégicos, la planeación ha tomado nuevas dimensiones y requiere de nuevos enlaces con el proceso de planeación de la empresa. La gerencia de la organización tiene que considerar a los sistemas de información y a la tecnología como áreas que pueden proporcionar efectos significativos de competitividad de la compañía.

De hecho tener o no tener una planeación de sistemas de información puede afectar los planes de la empresa y por supuesto no tenemos una base sólida para el esquema de control.

La planeación estratégica se refiere a la planeación de estrategias de la organización para el futuro y cual es la dirección a la que quiere ir la organización. Por otro lado la planeación táctica describe como la organización alcanzará sus objetivos. También existen otras clases de planeación de sistemas de información, la planeación de proyectos que sirve para elaborar el programa de desarrollo de sistemas o para la planeación de presupuestos y adquisiciones.

El enfoque en este punto es resaltar que la gerencia de la organización, el departamento de sistemas y el departamento de auditoría, es decir la organización, debe tener un plan para saber a donde quiere dirigirse en el futuro y considerar fuertemente el papel de los sistemas de información.

4.1.1 EL CICLO DE PLANEACION

A lo largo del tiempo se han hecho numerosas objeciones a la necesidad de la planeación de los sistemas de información. Principalmente bajo el argumento de que las tecnología cambia rápidamente y así cualquier plan se vuelve obsoleto, esto puede ser un gran problema en el área de sistemas y no es cierto del todo. La mala planeación produce planes de bajo rendimiento, las promesas no cumplidas nos llevan a la pérdida de credibilidad y la pérdida de confianza en la habilidad de la función del departamento de sistemas. El objetivo es hacer crecer la arquitectura de sistemas de información, contar con un esquema de control y todo ello en base a una planeación de calidad.

Una forma típica de planeación y que resuelve el problema de la obsolescencia es **dividir los planes futuros en diversos períodos, por ejemplo:**

- ❖ **Planes a corto plazo.** Por ejemplo: Instalar los proyectos terminados, mejorar los sistemas de administración de los proyectos en desarrollo, iniciar proyectos piloto para explorar nuevas tecnologías, etc.

- ❖ **Planes a medio plazo,** los cuales pueden dividirse aún más. Por ejemplo: Mejorar la metodología de planeación, ya que se puede utilizar la metodología más adecuada para los proyectos por iniciarse.

- ❖ **Planes a largo plazo.** Las compañías pueden planear a este punto en la arquitectura de sistemas y en la infraestructura que necesita la compañía para su operación en el futuro.

4.1.2 EL ENLACE ENTRE LA EMPRESA Y LA PLANEACION

¹“La planeación de sistemas y la planeación de la organización se han enlazado gradualmente para soportar los planes corporativos. Con gran énfasis en el uso de computadoras para tener una ventaja competitiva, los planes de sistemas de información pueden guiar la estrategia del negocio”. Lo importante para la compañía es como puede enlazar la estrategia del negocio con los sistemas de información en forma efectiva. A continuación se mencionarán dos elementos por los cuales se puede llevar a cabo este enlace: Los **comités** y el **acercamiento a una planeación de sistemas.**

¹ Ralph H. Sprague Jr. Information Systems Management in Practice.

LOS COMITES

Los comités de sistemas de información generalmente consisten en gerentes de diversas áreas de la compañía, el trabajo de este grupo consiste en encausar las inversiones en los sistemas en la dirección correcta para beneficio de la organización. De estudios realizados acerca del **funcionamiento de los comités**, se mencionan 4 ventajas que nos pueden ayudar:

1. El comité incrementa la atención de la alta gerencia hacia la computación.
2. Los usuarios se involucran en los sistemas de información.
3. El departamento de sistemas se preocupa de las necesidades de los usuarios.
4. Hay una visión más amplia para la planeación.

Según estos estudios, estas ventajas se pueden obtener, si es que los comités están constituidos con las siguientes características:

- El nivel que en el organigrama tiene los gerentes que participan en el comité.
- La representatividad debe reflejar a los usuarios de los sistemas de información y por supuesto al departamento de sistemas.
- Deben existir reuniones **periódicas**.
- Las decisiones deben ser tomadas por acuerdo, no por imposición.

Como resultado de dicho estudio se concluyo que ninguna estructura de comités alcanzaría todas sus ventajas en teoría, sino se tiene el nivel directivo y la representación en dichos comités, son parámetros determinantes para lograr los

¹ Ralph H. Sprague Jr. Information Systems Management in Practice.

objetivos en la teoría. Así, que parte del éxito de una planeación estratégica en los sistemas de información es involucrar a los gerentes de la organización a través de comités. El otro ingrediente es una metodología de planeación.

ACERCAMIENTO A LA PLANEACION DE SISTEMAS

Debido a la importancia y la dificultad de la planeación de sistemas, es importante tener un marco de trabajo o metodología para guiar el proceso. Se han desarrollado varias metodologías al paso del tiempo para apoyar el trabajo de planeación de los gerentes del departamento de sistemas.

Estos procesos tienen diferentes enfoques en la planeación de los sistemas de información. Unos se concentran en la asimilación de la tecnología que soporta a los sistemas de información en la organización, considerando la adaptabilidad a los cambios tecnológicos. Otros se enfocan a la definición de necesidades de información y otros clasifican las aplicaciones de sistemas. A continuación se mencionan estos 7 procesos o técnicas.

1. Etapas de crecimiento.
2. Factores críticos de éxito.
3. Análisis estratégico de inversión.
4. Creación de panoramas para la planeación.
5. Enlazar la planeación de análisis.
6. Solución creativa de problemas.
7. Modelo de empresa.

Basados en el éxito y fallas en la planeación de los sistemas de información, se ven necesarios dos elementos para una buena planeación estratégica. Ambos tal vez parezcan obvios, sin embargo se mencionarán: Uno de ellos es siempre ver hacia el futuro, la otro es enlazar los planes de los sistemas de información con los sistemas de la organización.

4.2 DEFINICION DE POLITICAS, ESTANDARES, NORMAS Y PROCEDIMIENTOS

Dentro de la organización la Gerencia debe concebir políticas, estándares, normas y procedimientos que sean la base de la planeación, el control y la evaluación gerencial para toda la organización en el área de sistemas de información.

- ❖ **Las políticas** deben desarrollarse y comunicarse a las diversas direcciones acerca de la importancia trabajo del departamento de sistemas de información, y la interdependencia con respecto a los departamentos usuarios.
- ❖ **Los estándares** deben definirse, coordinarse y comunicarse al personal involucrado con el desarrollo de sistemas, la evaluación de las aplicaciones, y la adquisición de los recursos de sistemas de información. La adquisición de recursos, ya sea humanos, software o hardware depende de la actividad desarrollada por el departamento o unidad de computo.
- ❖ **Los procedimientos** se deben establecer, coordinar y comunicar a los departamentos involucrados, los procedimientos describen el método y las responsabilidades en el funcionamiento del departamento de sistemas y de los departamentos usuarios.
- ❖ **Las normas** se deben establecer y comunicar a los departamentos de la organización, las normas describen como se hacen las actividades dentro de la empresa y bajo que estándar de calidad se deben de realizar.

4.2.1 EL DESARROLLO DE POLITICAS

Esta actividad se basa en el aspecto de la gestión de los sistemas de información. Es decir, aunque un sistema puede ser proyectado y planeado técnicamente perfecto, su administración puede hacer inútil los beneficios derivados de la realización. La dirección debe establecer su política con respecto a la protección de los sistemas de información y los datos.

Es la política de la alta Gerencia la que establece los modelos, prácticas y responsabilidades de todas las partes envueltas en el desarrollo de sistemas, el funcionamiento de la unidad de computo y de las aplicaciones en funcionamiento. Sin esta guía, la organización no tiene una buena base para iniciar las medidas de control.

Los contratos que unen a la organización a determinados compañías de servicios deben ser examinados por el departamento de auditoria y el departamento jurídico de la empresa. Todo ello con el propósito de revisar de inicio los contratos de hardware, software, garantías en el equipo, mantenimiento etc. Todos estos necesitan tener sus requisitos establecidos revisados y controlados.

**4.3 DEFINICION DE RESPONSABILIDADES Y FUNCIONES EN CADA AREA
DE LA ORGANIZACION**

La función de los sistemas de información debe ser tan importante dentro de la jerarquía de la organización como para permitir alcanzar todos los objetivos establecidos y tener una independencia relativa con respecto a los departamentos usuarios. Se debe emplear una estructura de administración de personal para fomentar el uso eficiente de los recursos humanos y facilitar la evaluación de control y desempeño de la funciones del área de sistemas de información.

La alta gerencia debe colocar la función de los sistemas de información en un nivel eficientemente alto dentro de la estructura organizacional para garantizar su independencia de los departamentos usuarios. Así como la función del departamento de auditoría de sistemas, sus evaluaciones deben tener peso en la organización.

**4.3.1 DESCRIPCION Y RESPONSABILIDAD DE LA FUNCION DEL
DEPARTAMENTO DE SISTEMAS DE INFORMACION**

La Gerencia debe describir las principales actividades dentro de la toda la estructura de la organización que abarca la función de sistemas de información, con sus responsabilidades bien delineadas y documentadas. En este punto no se pretende que la Gerencia describa actividades de tipo técnico, en cambio, se pretende definir cual es la función y la responsabilidad exacta de nuestro departamento de sistemas.

Para tomar el liderazgo de la función del área de sistemas de información y llevar a la organización a una posición competitiva, el Gerente del área de sistemas tiene que considerar las siguientes responsabilidades primarias:

- ❖ **Entender el negocio.** Particularmente de los mercados en los cuales la empresa negocia sus productos o servicios.
- ❖ **Establecer la credibilidad del departamento de sistemas.** Incrementar la confianza de la alta Gerencia con respecto a las ideas presentadas por la gerencia de sistemas.
- ❖ **Incrementar la madurez tecnológica de la organización.** Hacer más sencillo el trabajo de tomar ventaja y aprovechar las aplicaciones de computo y telecomunicaciones dentro de la organización.
- ❖ **Crear una visión del futuro y venderla.** Establecer objetivos sobre el uso de la tecnología en la organización y vender ese objetivo a la alta dirección y otros departamentos.
- ❖ **Implementar la arquitectura** de sistemas de información que soporte la visión y a la compañía en el futuro. Determinar la plataforma de hardware, la plataforma de software y a la infraestructura de telecomunicaciones. Por ejemplo, necesito una red local (LAN) o de extensión amplia (WAN) o requiero de un equipo mainframe; que tipo de sistema operativo requiero para la red, etc. Preguntas que bajo una metodología de trabajo se irán resolviendo.

Algunas de estas responsabilidades tal vez sean nuevas para algunos gerentes del área de sistemas, ya que cada organización tiene diferentes situaciones. De hecho algunas organizaciones cubren varios de los puntos antes mencionados.

4.3.2 LA ADECUADA SEPARACION DE FUNCIONES

El objetivo de una adecuada separación de funciones, indica la autoridad, responsabilidad y compromiso del personal en el área de sistemas. Por ejemplo, ningún programador debería estar involucrado con el manejo de los datos de entrada de la aplicación o ser usuario de estos datos. Si es posible cada una de las siguientes funciones se efectuará por una persona distinta. Aunque en organizaciones pequeñas esto no es factible, o en las etapas de desarrollo de un sistema donde una sola persona puede llegar a realizar todas las etapas. Uno debe reconocer el peligro que hay, si un sólo individuo asume más de una de estas funciones:

- Diseño de los sistemas de información.
- Programación.
- Mantenimiento de los sistemas de información.
- Administración de las bases de datos.
- Operación de un sistema. Administración de un sistema.
- Operación de un sistema. Captura de datos.
- Operación de un sistema. Salida de datos.
- Distribución de la información.
- Verificaciones y validaciones en las aplicaciones.
- Pruebas en los sistemas y equipos.
- Evaluación de procesos y control.

Un organigrama es una herramienta que puede ayudar a proyectar en forma eficiente y sintetizada las funciones y responsabilidades de departamento de sistemas de información en la organización.

DELIMITACION DE TAREAS

La Gerencia debe disponer la delimitación de tareas dentro de la función de los sistemas de información, las tareas se han delimitado a través de todo este trabajo, tenemos 3 grandes grupos: El desarrollo de sistemas, las tareas del departamento de sistemas o unidad de computo, y la administración de nuestras aplicaciones. Y a su vez, éstas pueden ser delimitadas.

DESCRIPCION DE PUESTOS EN LOS SISTEMAS DE INFORMACION

Las descripciones de puestos en los sistemas de información deben presentarse por escrito, ser claras en la delegación de autoridad y responsabilidad, mantenerse actualizadas, ir acompañadas de definiciones de las habilidades técnicas necesarias y utilizarse como base para la evaluación del control y desempeño.

4.3.3 SELECCION DE PERSONAL

Las prácticas de reclutamiento y promoción de personal deben basarse en criterios objetivos y bajo la política de la Gerencia, en el presente trabajo se menciona la relación que existe entre la contratación de personal y las actividades de la unidad de computo.

El personal del departamento de sistemas de información debe estar unido a la organización no sólo por situaciones económicas, la gerencia debe promover mecanismos con el departamento de administración para unir al personal a la empresa en más de un aspecto, dígame becas, prestaciones, etc.

PROCEDIMIENTOS PARA LA TERMINACION DE LA RELACION LABORAL

Los procedimientos para la terminación de la relación laboral del personal de sistemas de información deben proteger los recursos de hardware, los recursos de software, y la información de la empresa. El procedimiento debe estar bien definido y considerar diversos aspectos legales para ser aplicado por el departamento jurídico de la organización.

4.3.4 LA CAPACITACION DEL PERSONAL

Los empleados deben ser orientados a una capacitación continua que ayude a mantener su conocimiento técnico, sus destrezas y sus habilidades. El problema en este punto es que la Gerencia debe invertir en empleados que pueden irse a otra empresa ya que fueron entrenados. Si pueden perderse empleados, pero como ya se menciono debemos tener mecanismos que ligen a nuestros empleados a la empresa, y contemplar no sólo características a favor del empleado, también características a favor de la empresa.

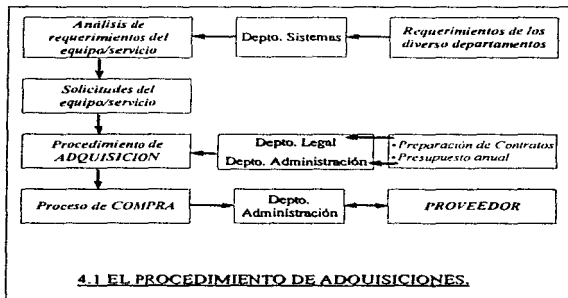
Capacitación en control de sistemas de información. El programa de capacitación debe considerar a las áreas de control, evaluación del control (auditoría de sistemas), determinadas áreas de sistemas y hasta la Gerencia, para formar y actualizar conocimientos sobre control y tecnología de sistemas de información.

La evaluación del desempeño es un resultado, el cual debe permitir a la Gerencia tomar decisiones, existe toda una infraestructura de control, y antes un desarrollo de políticas, programas y planes que generan procedimientos, etc. Todo ello debe en teoría, producir reportes de evaluación precisos y fidedignos, ya que la Gerencia tomará decisiones basada en estos reportes.

4.4 LA ADQUISICION DE EQUIPO Y SERVICIOS

“Se entiende que la adquisición de bienes y servicios es tomar la propiedad de un bien o tener el derecho a recibir un servicio de calidad”. En el proceso que se sigue para adquirir los bienes y servicios necesarios para la operación en el área de sistemas, deben intervenir diversas áreas, desde las que tienen la necesidad del bien o servicio hasta las que efectúan la compra y las que realizan el pago respectivo.

En términos generales las áreas a las que se ha hecho referencia, deben seguir la programación y presupuesto planeado para el periodo. Las adquisiciones además deben cumplir con un estudio previo del área que quiere pedir el bien o servicio, deben tomarse en consideración aspectos de rentabilidad, control de calidad, evaluación técnica, evaluación económica y contabilidad.



³ IMCP. Normas y Procedimientos de Auditoría.

4.4.1 LA IMPORTANCIA DEL CONTROL EN LAS ADQUISICIONES

La organización debe establecer comités que tendrán por objetivo determinar las acciones tendientes a la optimización de recursos que se destinen a las adquisiciones, arrendamientos y servicios, es decir seguir las políticas sobre la adquisición de bienes y servicios de la empresa. Los procedimientos y normas en la adquisición de bienes y servicios, y no sólo la adquisición, también la función debería de verse como una ley, ya que existe una gran inversión en este rubro, el objetivo es disminuir el riesgo de pérdidas en una actividad donde se maneja una gran cantidad de recursos monetarios, y no importante el tamaño de la empresa, lo que se invierte en bienes y servicios de computo siempre es un porcentaje considerable para la empresa.

4.4.2 LA FUNCION DE LOS COMITES

No en todas las organizaciones deben establecerse dichos comités salvo por la naturaleza de la empresa o que no se pueda implementar ningún otro mecanismo de control en las adquisiciones. Por supuesto también depende de la magnitud de las operaciones.

En los casos en que sea factible el establecimiento de los comités, éstos tendrán las siguientes funciones:

- ❖ Revisar los programas y el presupuestos de adquisiciones, arrendamientos y servicios de computo.

- ❖ En el caso de organizaciones gubernamentales **dictaminar** sobre si procede celebrar licitaciones públicas. Así, como los casos que no se celebren por encontrarse en algún supuesto de excepción que marca la Ley.

- ❖ **Proponer** las políticas internas en la materia adquisiciones, así como **autorizar** los supuestos no previstos, y por supuesto **informando** a la Gerencia sobre estas propuestas y que esta haciendo el comité.

- ❖ **Analizar** las diversas disposiciones legales que debe cumplir la organización para celebrar contratos de bienes y servicios y todo lo relacionado con sanciones a proveedores.

- ❖ **Analizar** exclusivamente para su opinión, cuando se le solicite, los dictámenes y fallos emitidos. Es decir, en algún punto la Gerencia quiere saber que ocurrió con determinado proceso de adquisición.

4.5 REQUERIMIENTOS EXTERNOS

En la planeación de la organización y la función del departamento de sistemas, se deben tomar en cuenta los requisitos o características externas relacionados con prácticas y controles en los sistemas de información, el requerimiento que consideramos más importante en este punto, es el legal.

4.5.1 EL DERECHO DE AUTOR Y LOS SISTEMAS DE INFORMACION

En el derecho de autor, la admisión de los programas de software se contemplan en la categoría de obras protegidas, aunque los programas de software parecían no considerarse en el ámbito de la propiedad intelectual, en poco tiempo, la tecnología digital se ha ido perfilando como una de las formas de explotación más relevantes de las obras intelectuales en un futuro no lejano.

“La tecnología digital ha ingresado a la disciplina del derecho de autor de la mano del software, antes que se produzca el gran desafío de la aplicación de ese avance fenomenal de la técnica, a la explotación de las obras en los soportes multimedia y en la supercarretera de la información”.

LA NECESIDAD DE ENCONTRAR SOLUCIONES PARA LA CONCESION DE LICENCIAS EN LA TECNOLOGIA DIGITAL

Hoy en día las leyes se encuentran obligados a responder a la exigencia de los autores, la industria de software y tecnología digital requiere y demanda la protección de lo que se puede denominar como obras artísticas. Como van a poder

* Santiago Schuster V. La Tecnología y los Derechos de los Autores.

gozar de las licencias de derechos de autor correspondientes, para que puedan satisfacer las demandas de sus clientes o usuarios que desean acceder a la entrega digital de tales obras.

Las preguntas que debemos formular son en apariencia sencillas, a pesar de lo complejo del fenómeno de la tecnología digital, con toda su terminología repleta de siglas que representan cada una diferentes cosas.

En efecto, el asunto consiste en resolver si será posible a los autores continuar gozando de sus derechos exclusivos de autorizar el uso de sus obras, sea bajo la forma de gestión individual o colectiva y, de ser ello posible, que condiciones nuevas se deberán satisfacer para que ello tenga lugar.

LA OBRA COMO DATO AFECTADA POR NUEVAS EXPLOTACIONES

Se deben delimitar cuáles serán los derechos de los autores, que están involucrados en estas nuevas explotaciones, y como se resolverá la concesión de las licencias los límites de los usos autorizados, donde estará centrada la negociación de las condiciones económicas que deberán establecerse por el uso de las obras.

En esta necesidad de definir los modos de licenciamiento, distinguimos las posibles nuevas utilidades de las obras en medios digitales:

1. En las bases de datos.
2. Transmisión en redes de telecomunicación.
3. Utilización por el usuario final de las bases de datos
4. Utilización secundaria, extraída de las bases de datos.

Es preciso asegurar para la organización un examen para conocer que derechos de explotación tenemos al contratar un producto o licencia. Se debe tener presente el principio general del derecho de autor de la independencia de las explotaciones.

4.5.2 EL USO DE SOFTWARE ILEGAL

Todos necesitamos utilizar programas de cómputo, pero desgraciadamente no todos los usuarios respetan las leyes de derecho de autor, y la piratería es una práctica que consiste en copiar ilegalmente programas protegidos por las leyes de derecho de autor para evadir erogaciones.

“La ley de propiedad intelectual establece que un programa original para computadora es propiedad intelectual de la persona o empresa que lo creó. De esta manera, al adquirir un programa, no se adquieren los derechos sobre éste, sino solamente una licencia para su uso en una computadora, o a veces en dos, y que esto se permita en la licencia”.

Una licencia especifica las condiciones bajo las cuales el software puede utilizarse. Siempre que se adquiere un programa, es preciso leer la licencia de utilización del mismo.

⁵ Eduardo Peñalosa, Thaís Rezende. La Piratería de Software: Riesgos y Alternativas.

En nuestro país se considera según ANPICO (Asociación Nacional de la Industria de Programas para Computadoras) que algunas conductas ilegales son:

- Copiar o distribuir software o su documentación sin permiso del autor.
- Ejecutar un programa en dos o más computadoras simultáneamente, a no ser que esté permitido en la licencia.
- Estimular, permitir, obligar o presionar a los empleados en las empresas a hacer o utilizar copias no autorizadas.
- Infringir las leyes sobre copias no autorizadas porque alguien lo pida o lo exija.
- Prestar los programas para que sean copiados o copiar aquéllos que se han pedido en préstamo.
- Fabricar, importar, poseer o negociar con artículos que faciliten la copia de programas.

LOS RIESGOS

Por una parte, existen los riesgos impuestos por la ley (en México), que consisten en:

- **Sanciones económicas.** En este sentido, la ley impone multas hasta por 20,000 salarios mínimos.
- **Confiscaciones.** En los sitios donde se encontrara software ilegal, puede confiscarse el equipo de cómputo en el que se utilice, así como los medios de almacenamiento (discos, cd's u otros) en los que se encuentren las copias ilegales.
- **Clausuras.** Los negocios que se sorprendan (en estas actividades, pueden ser clausurados temporal o definitivamente).

Por otro lado, al utilizar copias de software pirata de dudosa procedencia se incrementa sensiblemente la probabilidad de que los equipos de cómputo se infecten con virus, que alteren o destruyan la información almacenada.

Los virus pueden extenderse fácilmente en una organización, ya sea a través de discos que se comparten o incluso a través de una red de computadoras. Otras desventajas inherentes a la piratería son:

- Fallas en el software.
- Falta de garantía.
- No se tiene derecho a soporte técnico.
- No se tiene derecho a actualizaciones.
- No se tiene acceso a documentación.

ALTERNATIVAS

Por supuesto, la alternativa es adquirir software con licencias, por los beneficios que esto implica. Una de las soluciones se ha realizado por parte de las empresas que arman computadoras (las de marca), hoy en día incluyen software preinstalado, con todas las garantías legales.

Estas facilidades en el equipo ofrecido por las empresas de software y hardware han hecho decrecer el número de copias pirata, ya que la mayoría de los usuarios tiene suficiente con un conjunto de aplicaciones, y si éstas vienen preinstaladas en el equipo, se cuenta con la solución completa.

Por otra parte, empresas de software han lanzado programas que permiten la adquisición a precios accesibles de software en sectores con bajo poder adquisitivo como el académico, en el que ofrecen descuentos. Esto garantizará un incremento en el uso de software legal.

ESTADISTICAS SOBRE PIRATERIA

*Las siguientes estadísticas son una recopilación de la Asociación Nacional de la Industria de Programas para Computadoras, ANPICO.

- Posiblemente sólo 2 de cada 10 programas instalados en computadoras personales cuentan con una licencia que avale su legalidad.
- En México la proporción de software pirata es de 78% contra 22% con licencia. Hace algunos años el software con licencia apenas alcanzaba cerca de 10%.
- En otros países se presenta una proporción más favorable para el software con licencia. En Europa el software pirata sólo asciende a 35%, y en EU es menor.
- En Latinoamérica el porcentaje de software pirata es del 82% aproximadamente. En México, en 1992 y 1993, se incrementó la piratería, por los precios elevados del software, pero en 1994 empezó a decrecer, debido a las medidas de venta y distribución de las compañías.
- En México, se pierden al año 250 millones de dólares, y 1,500 millones en América Latina, por lo cual asociaciones como ANPICO y el IMPI (Instituto Mexicano de la Propiedad Industrial), han pugnado por hacer respetar la ley de protección a los derechos de autor.

* Eduardo Peñalosa, Thais Rezende. *La Piratería de Software: Riesgos y Alternativas.*

7En la era digital los **derechos de los autores** sólo encontrarán enormes ventajas, si se logran establecer los siguientes escenarios:

- ❖ Los autores mantienen sus derechos sobre sus obras, y no sucumben a las presiones de cederlos íntegra e indefinidamente, venciendo la pretensión casi natural de las grandes empresas de telecomunicaciones de adquirir la titularidad total del contenido de sus bases de datos. Los autores, por tanto, ejercen como herramientas insustituibles las licencias de explotación, perpetuando su derecho a aprovechar del éxito de su obra, lo que al mismo tiempo aleja la amenaza de las licencias legales.

- ❖ Los autores hacen valer el principio de la independencia de los derechos, de modo tal que la incorporación de las obras para su utilización a través de bases de datos, se canaliza a través de formas contractuales que impiden un vaciado de los datos/obras que pueden ser explotadas indiscriminadamente, sin límite alguno.

- ❖ Los autores conducen a sus sociedades de gestión a nuevas modalidades de gestión colectiva, satisfaciendo un mercado que requiere grandes volúmenes de obras donde, paradójicamente, será posible dar cabida en mejores términos a una administración más individualizada del autor y de su obra.

⁷ Santiago Schuster V. *La Tecnología y los Derechos de los Autores*.

4.6 NORMAS Y PROCEDIMIENTOS PARA EL CONTROL GERENCIAL

A continuación mencionamos los aspectos generales que se deben cubrir en el control gerencial. La filosofía del capítulo es mostrar los puntos claves de trabajo para llevar a cabo el control gerencial:

❖ **Planeación para la organización y para los sistemas de información.**

Planeación a corto plazo para la organización y en los sistemas de información.

Planeación a mediano plazo para la organización y en los sistemas de información.

Planeación a largo plazo en la organización y en los sistemas de información.

El comité de planeación y supervisión de los sistemas de información.

Revisión de la planeación para la organización y en los sistemas de información.

❖ **Políticas, estándares, normas y procedimientos.**

Desarrollo de Políticas, Estándares, Normas y Procedimientos de control.

❖ **Responsabilidades en la organización y administración de personal.**

Ubicación en el organigrama de la empresa del departamento de sistemas de información.

Descripción y responsabilidades de la función del departamento de sistemas de información.

Delimitación de tareas.

Descripción de puestos en el departamento de sistemas de información.

Selección de personal.

Procedimientos de terminación laboral.

Capacitación de personal.

Capacitación sobre el control de sistemas de información, en todas las áreas de control.

Evaluación del desempeño de los empleados.

❖ **Control de calidad de los sistemas de Información.**

La responsabilidad del control de calidad.

Aspectos organizacionales de la función de control de calidad.

Avance de objetivos de los sistemas de información.

Revisión del cumplimiento de los estándares en los sistemas de información.

Revisión de los controles de los sistemas de información.

Informes de la revisión del control de calidad.

❖ **Auditoría Interna**

Organigrama de la Auditoría Interna.

Responsabilidad de la función de la Auditoría Interna.

❖ **Requisitos Externos**

Requisitos legales relacionados con prácticas contables y controles en los sistemas de información.

Leyes de exclusividad en un ambiente de cómputo.

Por último, el siguiente cuadro es un resumen de los controles Gerenciales que se han descrito.

4.2 LOS CONTROLES GERENCIALES.

LA PLANEACION REQUIERE DEL TRABAJO DE LA ALTA GERENCIA, EL DEPARTAMENTO DE SISTEMAS Y EL DEPARTAMENTO DE AUDITORIA INTERNA.

DEFINIR RESPONSABILIDADES Y FUNCIONES DEL DEPARTAMENTO DE SISTEMAS DE INFORMACION.

PRODUCIR LAS POLITICAS, ESTANDARES, NORMAS Y PROCEDIMIENTOS RELACIONADOS CON TODAS LAS FUNCIONES Y ACTIVIDADES DE SISTEMAS.

ESTABLECER UN ESTRICTO CONTROL DE CALIDAD EN LOS SISTEMAS DE INFORMACION.

DEFINIR LAS FUNCIONES DE LA AUDITORIA INTERNA.

CONSIDERAR LOS FACTORES EXTERNOS QUE AFECTEN LA ACTIVIDAD DE SISTEMAS DE INFORMACION.

4.7 RESUMEN

Dentro del trabajo de la Gerencia en el área de sistemas de información definimos claramente dos conjuntos de tareas, uno de ellos desarrollado por la alta Gerencia de la organización y el otro desarrollado por la Gerencia del departamento de sistemas de información.

Con respecto a las tareas de la Gerencia de la organización le corresponde establecer el siguiente entorno:

1. Producir las políticas, establecer los estándares, normas y procedimientos de control con los que se trabajará en área de sistemas de información.
2. Establecer la independencia del departamento de computo con respecto a los demás departamentos. Con el objetivo de definir las funciones y responsabilidades del departamento de sistemas de información.
3. Definir los criterios y el entorno del plan de presupuestos y adquisiciones dentro de la compañía.
4. Considerar como afectará a la compañía los requerimientos externos. Sobre todo lo que se refiere a los aspectos legales dentro de los sistemas de información y la infraestructura de computo.
5. Definir las funciones y responsabilidades del departamento de auditoría interna.

Por la otra parte, la Gerencia del departamento de sistemas de información debe enfocarse en dos puntos muy importantes para su funcionamiento:

1. Realizar la planeación de los sistemas de información considerando lo que se puede realizar a corto, mediano y largo plazo dentro del ámbito de la organización. La planeación debe considerar cual es el objetivo de la organización y cual es el funcionamiento de esta.
2. Considerar como afecta al departamento de sistemas las disposiciones de la alta Gerencia. El departamento de sistemas debe construir una gran confiabilidad acerca de su trabajo ante la alta Gerencia, y proponer los planes y proyectos de la forma que la alta Gerencia los considere factibles de llevar a cabo desde la primera impresión, y evidentemente deben ser los mejores planes y proyectos para la organización.

Este conjunto de tareas nos encamina directamente a establecer una base para el control dentro de la organización, este papel corresponde a la Alta Gerencia encabezarlo con el apoyo del departamento de auditoría y del departamento de sistemas de información.

CAPITULO 5
EL VALOR AGREGADO DE LA INFORMACION

5.1 EL VALOR DE LA INFORMACION.

5.2 LA ADMINISTRACION DE LAS FUENTES DE INFORMACION.

5.3 LOS INFORMES.

5.4 RESUMEN.

5.1 EL VALOR DE LA INFORMACION

Nuestro punto de partida es revisar la diferencia entre el concepto de dato e información. Los datos son símbolos que por sí mismos tienen un valor, pueden formar parte de una palabra, un número, etc. Si estos datos son interpretados bajo un determinado entorno de referencia, éstos datos se pueden considerar como información. Consideremos las siguientes definiciones:

- ❖ **Dato** como: "Cualquier representación de hechos, conceptos e/o instrucciones cuya significación es o puede ser asignada cuando sea procesada correctamente por medios humanos o automáticos".
- ❖ **Información** como: "El sentido que un individuo asigna a los datos por medio de convenciones aplicadas a esos datos".

El valor de la información está dado por el contexto donde será utilizada. La información proporcionada debe contar con dos características muy importantes:

1. **Precisión.** La información debe evidenciar los hechos en forma clara y precisa dentro de nuestro contexto.
2. **Oportunidad.** Es decir, debe estar disponible a tiempo.

A la información se le puede agregar un valor aún mayor, que a continuación revisaremos. La información es intangible, pero tiene un valor enorme para la empresa.

¹ William C. Mair, et. al. Control y Auditoría del Computador.

² *ibíd.*

LA INFORMACION

Dicen los expertos que quien es dueño de la información es dueño del mundo. Esta aseveración, justa y razonable, es la que ha hecho que algunas empresas sean líderes en su mercado al estar en la vanguardia de todos los sucesos relacionados con su materia, que les permite tomar decisiones orientadas a que sus empresas mantengan la excelencia en su campo de acción.

La información precisa y oportuna es importante para la correcta toma de decisiones. Sin embargo, no basta que tengan esas dos características, sino que también deberá ser significativa, relevante e imparcial.

El empresario moderno cuenta con un torrente de información, que tiene que analizar y sintetizar. Es recomendable el auxilio de personal experto que depure, analice y sintetice información, de tal suerte que el empresario sólo se entera de lo relevante y significativo para poder elegir con mayor seguridad.

La información como recurso, es un medio del que se vale la empresa para adecuarse con mejor visión a los cambios. Constituye un elemento vital de decisión. "El éxito de este recurso consiste en generar una serie de reportes que muestren lo verdaderamente representativo, no lo usual y trillado. Algunas empresas han invertido más tiempo en el diseño de la información que en la obtención de la misma; el resultado ha sido que obtienen, en menos tiempo, una información sustanciosa, certera y adecuada".

³ Carlos Prieto S., Carlos Suárez O. Introducción a los Negocios.

“El recurso material es importante; el recurso financiero es básico para la seguridad y oportunidad; el elemento humano es esencial; la tecnología es un marco de supervivencia y la información un recurso para nuestras correctas decisiones”. Ninguno de estos elementos en forma aislada, nos dará como resultado una empresa integrada. La mezcla correcta de todos ellos, dará como resultado un balance de eficiencia que demandan las organizaciones de hoy en día.

El objetivo principal considerando que estamos conscientes del valor de la información, es poder crear la estructura de sistemas de información que nos proporcione la confiabilidad en la información que interviene en nuestra organización. El siguiente apartado tiene el propósito de describir como podemos alcanzar este objetivo.

5.2 LA ADMINISTRACION DE LAS FUENTES DE INFORMACION

Las fuentes de información internas y externas disponibles para una organización se han incrementado debido a los avances tecnológicos. El almacenamiento de información a bajo costo, una mayor velocidad procesamiento y una mayor capacidad de comunicación están haciendo posible que una mayor cantidad de información interna esté disponible. La tecnología digital de voz, video e imágenes han incrementado los formatos en los que se presenta la información. Al mismo tiempo, los datos externos, tanto información en medios magnéticos como información en libros han incrementado su disponibilidad mediante las bases de datos públicas y servicios similares.

Debido al crecimiento de las fuentes de información, varias compañías aún están luchando para tener sus datos internos bajo control. La era de las bases de datos ha traído beneficios y ventajas incluyendo la separación de programas y datos, reducción en la redundancia de datos, y un acceso más sencillo a datos para la solución de problemas y la toma de decisiones. Como sea, en el área de sistemas "El progreso todavía está por hacerse en la organización y el manejo de las fuentes de información". Para una organización, la estrategia para el manejo de la información como una fuente corporativa de datos se divide en 4 puntos:

1. Identificar los **problemas en la administración de datos**.
2. La evolución de los **sistemas de administración de base de datos**.
3. La necesidad del manejo de **datos distribuidos**.
4. Los **tipos de información** que una compañía debe manejar para que ésta sea una fuente de información organizacional.

⁵ Ralph H. Sprague Jr. Information Systems Management in Practice.

5.2.1 LOS PROBLEMAS EN LA ADMINISTRACION DE DATOS

Los intentos de la organización para tener bajo control los datos inician con el uso de los Sistemas Administradores de Base de Datos (DBMS, por sus siglas en inglés), a finales de los años 60 e inicio de los 70. Estos productos de software han incrementado la funcionalidad desde aquellos tiempos. La función de un administrador de base de datos involucra el manejo de toda la fuente de datos de la organización.

El primer problema a enfrentar es la incompatibilidad en la definición de datos de una aplicación a otra, de un departamento a otro, de un lugar a otro. Ya que para desarrollar y poner en funcionamiento los sistemas rápidamente, los diseñadores han visto la necesidad de que los datos fuente se obtengan de una fuente barata. Esto significa utilizar datos de archivos existentes y adicionar nuevos datos, sin analizar las normas de control de información. El resultado ha sido almacenar los mismos datos en diferentes archivos, con nombres diferentes para el mismo elemento; el mismo nombre para distintos elementos de datos y los mismos datos en diferentes archivos con diferentes ciclos de almacenamiento.

La administración gerencial no puede obtener una visión consistente a través de la organización bajo estas circunstancias. Además, los cambios en los programas de software y datos son difíciles de llevar a cabo. Las estructuras de control necesitan una fuente de datos consistente y bien definida.

En lugar de tener una aplicación funcionando lo antes posible se podría pensar en un esquema distinto. Primero identificar todos los tipos de datos en los cuales la empresa está interesada, luego identificar una fuente de datos única a través de las

de los departamentos de la organización que generan los datos. Finalmente, un sistema de transacciones será desarrollado para coleccionar y almacenar los datos, sólo después, todo usuario autorizado y aplicación tendrán acceso al conjunto de datos.

Este procedimiento no resulta, por lo que pudiese pensarse, en una enorme base de datos para ser utilizada por toda la empresa. Pero si requiere de un control administrativo sobre toda la información, así como un diseño de base de datos para atender a los usuarios de la organización, comenzando con:

- La descripción de los datos que requiere la organización.
- Seleccionar el método para proporcionar los datos que mejor mantenga el balance en los plazos de tiempo y las metas de la administración de datos.

EL PAPEL DE LA ADMINISTRACION DE DATOS

El uso de sistemas de administración de base de datos (DBMS) ha incrementado el problema de inconsistencia y redundancia de datos. No sólo por instalar un DBMS, significa que es suficiente para la administración de información en forma corporativa. Existen dos puntos fundamentales para promover la administración de datos en la empresa:

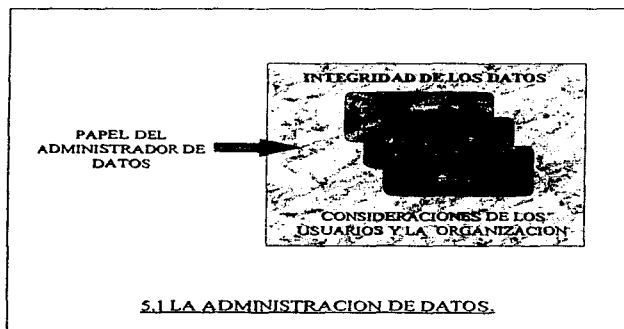
1. **El papel de la administración de datos.** La administración de datos es una tarea muy amplia, donde uno de sus principales propósitos es determinar que datos serán utilizados fuera del departamento de la organización que los genera y como deben ser definidos y estandarizados bajo la administración de datos.

2. **El uso efectivo del diccionario de datos.** El diccionario de datos es la herramienta principal para el administrador de datos, para que controle las definiciones del estándar de datos. Toda nueva definición y todas las peticiones de cambio deben reflejarse en el diccionario de datos, para asegurar que todas las políticas de la organización se estén siguiendo.

Y en donde la administración de datos contempla las siguientes funciones:

- ❖ **Establecer la definición de datos.** El administrador de datos necesita tener la responsabilidad y autoridad para asegurar la compatibilidad de datos e información en la organización mediante la eliminación de redundancias e inconsistencia de datos. El papel de la administración es diseñar los estándares en la definición de datos, diseñar el diccionario de datos y el diseño de la base de datos para conciliar las necesidades del usuario, sin olvidar la integridad de datos. Finalmente entrenar a los usuarios en el manejo apropiado de los datos. Sin embargo, los usuarios no intervienen en la definición de datos.
- ❖ **Controlar los datos compartidos.** Esta es un área controversial, por un lado se dice que todos los datos deben estar bajo control de la administración de datos, sean o no utilizados a lo largo de la organización, pueden ser utilizados en el futuro. El otro punto de vista es que cada departamento puede controlar sus datos; sólo los datos que fluyen hacia otros departamentos deben ser estandarizados, puede ser impráctico el tratar de estandarizar todo. Sin embargo los administradores de datos tienen que confrontar estas perspectivas y decidir que tan amplia o estrechamente se definirán los datos compartidos dentro de la empresa. Todos los programas que requieran cambios deben ser identificados antes de ser aprobados y requieren ser notificados a los usuarios.

- ❖ **Manejar datos distribuidos.** Por otro lado, los datos distribuidos son datos geográficamente dispersos, también quizá cruzaran niveles jerárquicos en la organización. La administración de datos en un ámbito distribuido, con diversos niveles de detalle, presenta un gran reto para el administrador, especialmente con las características de procesos corporativos y portabilidad.
- ❖ **Mantener la calidad de los datos.** Mantener íntegra la definición de datos, y otras importantes funciones de la administración de datos, esta tarea puede ser inútil al menos que las políticas gerenciales y procedimientos sean desarrollados para mantener la calidad de los datos. Los lineamientos desarrollados deben descentralizar o distribuir esta función, colocar a los dueños de los datos a cargo de editar y verificar la exactitud y calidad de los datos, y requiere resolver la incógnita de quién es el dueño de la información.



LA IMPORTANCIA DEL DICCIONARIO DE DATOS

El diccionario de datos son sistemas y procedimientos automatizados o manuales para manejar y almacenar las definiciones de datos de la organización. El propósito es eliminar errores de comprensión, ambigüedades y dificultades en la interpretación de datos.

Idealmente, el diccionario de datos debe seguir la siguiente secuencia:

1. **Establecer las funciones** de la administración de datos.
2. **Desarrollar los estándares** de datos.
3. **Adquirir e instalar** el DBMS.
4. **Instalar el diccionario de datos** como la primer aplicación.

Si el sistema administrador de bases de datos (DBMS), tiene como una de sus características la creación de un diccionario de datos para las aplicaciones que desarrollarán, esta función es una ventaja para la empresa. Sin embargo, la empresa que adquiere un DBMS y tiene en operación ya varias aplicaciones, requerirá de un mayor esfuerzo y tiempo para la creación y utilización exitosa de un diccionario de datos.

5.2.2 LA EVOLUCION DE LOS SISTEMAS ADMINISTRADORES DE BASE DE DATOS

Una de las áreas más activas del desarrollo de software ha sido la referente a los sistemas administradores de bases de datos. Los conceptos fundamentales de este desarrollo han sido:

1. Los niveles en la administración de datos.
2. Las diversas alternativas de modelos para la organización de datos.

EL MODELO GENERICO DE 3 NIVELES DE UNA BASE DE DATOS

Este concepto se deriva del trabajo de James Bradley sobre la tecnología de datos en los años 70, y que era parte de ANSI (American National Standard Institute). La mayoría de los DBMS han adoptado este concepto que a continuación se describe brevemente:

- ❖ **Nivel 1.** Llamado nivel local, externo o conceptual. Este nivel contiene varias *ideas* de los usuarios acerca de los datos utilizados por las aplicaciones. Este nivel no relaciona como se almacenan físicamente los datos o que datos están siendo utilizados por cada aplicación.
- ❖ **Nivel 2.** Llamado lógico o nivel de datos de la empresa. Se encarga de tomar todos los datos relevantes de la organización y tenerlos bajo control del administrador de datos.

- ❖ **Nivel 3.** Llamado nivel de almacenamiento físico. Este especifica la forma en que los datos son almacenados físicamente. Un registro de datos consiste en uno o más campos de datos, así como cierta implementación, ya sea apuntadores y/o banderas. Para el usuario final esta implementación no es vista y sólo es utilizada por el DBMS.

La ventaja de este modelo de 3 niveles es que los datos lógicos pueden separarse del método de almacenamiento físico.

LOS MODELOS TRADICIONALES DE DATOS

El segundo mayor concepto en la administración de bases de datos es la de definir las relaciones entre los datos y el sistema administrador de la base de datos. Estos modelos de datos son los medios por los cuales se realizan las representaciones de problemas y la forma en que los datos son accedados. Existen varios modelos en uso, pero los más utilizados desde la década de los 70 son el jerárquico, el modelo de red y el relacional.

- ❖ **El modelo jerárquico.** Estructura los datos de tal manera que cada elemento es subordinado a otro en una forma jerárquica estricta. Este modelo utiliza los términos padre e hijo para representar las relaciones.
- ❖ **El modelo de red.** Permite que cada modelo tenga más de un padre. Una lista de partes ensambladas ilustra esta estructura, donde una parte puede utilizarse en más de un ensamblado. En el caso del modelo jerárquico como en el de red, las relaciones de datos son explícitas, generalmente por apuntadores. Estos apuntadores se utilizan para acceder los registros de datos.

- ❖ **El modelo relacional.** Este sistema propuesto por Edgar F. Codd de IBM en 1970. Es el más reciente de los tres modelos. Este sistema ha traído consigo el debate de cual modelo es el mejor. En el modelo relacional, las relaciones entre elementos de datos no son expresadas por medio de apuntadores a los datos. En su lugar, el DBMS se encarga de buscar los elementos relacionados, basado en los valores de campos de datos específicos.

Los sistemas relacionales no son tan eficientes como el jerárquico o el modelo de red, pero ya que permite crear relaciones entre datos al momento en que surge una consulta, los sistemas de bases de datos relacionales son mucho más flexibles. Esta característica incrementa la capacidad de los grandes sistemas en línea. Por lo que, se ha convertido en la tecnología elegida hoy en día.

LA PROXIMA GENERACION DE SISTEMAS ADMINISTRADORES DE BASES DE DATOS

La próxima generación sistemas de administración de base de datos, de acuerdo a R. H. Sprague son los DBMS orientados a objetos o también llamados DBMS relacionales extendidos. Estos sistemas son diseñados para ampliar el uso de bases de datos a nuevas áreas para su aplicación: CASE, CAD, medicina, automatización de oficinas y representación de reglas para los sistemas de inteligencia artificial.

Estos sistemas estarán basados en las técnicas de hoy en día, pero incluirán dos conceptos muy importantes. Uno de ellos, es el manejo ya sea de objetos como datos, el manejo de multimedia y procedimientos. El segundo concepto, es el manejo de reglas, es decir la administración de reglas complejas para mantener la integridad de los datos. La siguiente generación de DBMS administrará datos, objetos y reglas.

SISTEMAS DE BASES DE DATOS ORIENTADOS A OBJETOS

Existe un gran crecimiento en el uso de tecnología orientada a objetos, en diversas áreas de computo. Una de esas áreas es la administración de bases de datos. El modelo de datos más reciente es el orientado a objetos. El avance de la tecnología orientada a objetos, es que ésta, expande la visión del almacenamiento de datos hacia el almacenamiento y administración de objetos, que consisten en:

- Un dato.
- Métodos, procedimientos que puedan desempeñar una tarea sobre los datos.
- Atributos que describen los datos.
- Relaciones entre un objeto y los demás.

Los objetos son importantes porque el concepto consiste en que pueden ser datos, hojas de cálculo, video, voz, imágenes, etc. Una colección de objetos es llamada "base de datos objeto" o con diversos nombres similares depende del fabricante del sistema, el propósito es resaltar la relación entre una base de datos objeto y un administrador de base de datos.

Aunque este modelo no reemplazará a los tres modelos tradicionales (jerárquico, red y relacional). Estos modelos **adicionarán** a sus características un almacenamiento de nuevas clases de datos. El trabajo de hoy y el futuro requiere de la administración de datos, objetos y reglas.

HACIA EL FUTURO

Los parámetros que conducen la tecnología de bases de datos y sus necesidades de investigación, según Silberschatz, Stonebraker y Ullman, se muestran en los siguientes puntos:

- ❖ La tecnología del siguiente siglo requerirá nuevas tecnologías de bases de datos.
- ❖ Las nuevas aplicaciones deben manejar diversas clase de datos, soporte de multimedia, objetos, reglas y almacenamiento de archivos.
- ❖ Entre los departamentos de una organización se requerirá del uso de bases de datos distribuidas.

En resumen, “El reto hacia las bases de datos es desarrollar la próxima generación de sistemas administradores de bases de datos y desarrollar sistemas distribuidos y heterogéneos de base de datos”.

Finalmente, la seguridad es un problema en los sistemas administradores de base de datos actuales, donde la distribución de datos y la heterogeneidad de las bases de datos sólo acentúan el problema. En las organizaciones se requiere, permitir el acceso sólo a una parte de la base de datos. Esto requiere de una autenticación confiable, al menos que la seguridad e integridad se refuercen vía programación, la Gerencia y los usuarios no pueden confiar en estos sistemas.

* Ralph H. Sprague Jr. *Information Systems Management in Practice*.

5.2.3 LOS DATOS DISTRIBUIDOS

El segundo gran reto que presenta la administración de datos, además del desarrollo de la próxima generación de Sistemas Administradores de Bases de Datos, son los datos distribuidos. Pocas son las organizaciones, y las cuales se enfrentan a varios problemas, aunque los beneficios que promete una base de datos distribuida son:

- ❖ Menor costo, al llevar procesos de base de datos a equipos menos costosos.
- ❖ Bajar los costos de telecomunicaciones, al acercar las bases de datos a los usuarios.
- ❖ Disminuir la dependencia de un sólo fabricante de computadoras, teniendo varios DBMS interoperando.
- ❖ Mover el manejo de datos a los generadores de los datos.
- ❖ Incrementar diferentes tipos de datos a los DBMS, y entonces ligarlos en las estaciones de trabajo.
- ❖ Permitir el almacenamiento y coordinación de varias clases de datos multimedia.

Esta tecnología no está aún disponible con todas estas características para que una compañía las utilice, pero es la tendencia en la administración de datos.

BASES DE DATOS DISTRIBUIDAS

Existe una gran controversia en el desarrollo de bases de datos distribuidas y no sólo en el campo de la investigación, a continuación se describen las gúfas sobre lo que debe ser una verdadera base de datos distribuida.

Guía de principios. Chris Date del Grupo de consultoría Code & Date formuló 12 reglas para las bases de datos distribuidas y estas se han convertido en la definición de bases de datos distribuidas:

1. Autonomía local de los datos.
2. No confiar en un centro maestro de procesamiento.
3. Operación continua, las instalaciones de software no deben afectar a terceros.
4. Independencia de la localización, no se necesita conocer donde se almacenan los datos físicamente.
5. Independencia de la fragmentación, las relaciones de los datos pueden ser fragmentadas por la localización física, pero los usuarios pueden continuar con su trabajo como si no hubiese ninguna fragmentación.
6. Independencia de los duplicados, las relaciones y fragmentos pueden ser copias o replicas de diferentes lugares, todo ello transparente para el usuario.
7. Procesamiento distribuido de consultas, se considera poder optimizar una consulta, ya sea local o global.
8. Administración de las transacciones distribuidas. Las transacciones se ejecutan provocando actualizaciones en múltiples lugares.
9. Independencia de hardware, se debe poder funcionar en diferentes clases de equipo.
10. Independencia de los sistemas operativos, los sistemas administradores de bases de datos deben correr sobre distintos sistemas operativos.
11. Independencia de la red de trabajo.
12. Independencia de la base de datos, los sistemas distribuidos son capaces de construirse en diferentes tipos de bases de datos, proporcionadas las mismas interfaces.

Transparencia. Existen 7 tipos de transparencia formuladas por M. Stonebraker, los cuales omitiremos. El propósito es mencionar que los 12 principios anteriores describen un sistema que cumple con el concepto de transparencia, lo cual significa que una base de datos distribuida se percibe como una base de datos no distribuida ante un usuario.

Estos dos grupos de definiciones se han convertido en los principios operativos en el campo de las bases de datos distribuidas. Aunque no se menciona en forma explícita las bases de datos **dependen** de que éstas sean **bases de datos relacionales**.

ELEMENTOS TÉCNICOS EN LA DISTRIBUCION DE DATOS

Entre los retos técnicos que enfrentan los desarrolladores de sistemas de bases de datos distribuidas, destacan 3 tipos de problemas técnicos. Hasta poder resolver estos problemas, los datos distribuidos no serán una solución práctica para aplicaciones en línea:

1. **Seleccionar un lenguaje estándar para el acceso a datos.** El estándar actual en el campo de bases de datos es SQL, que fue desarrollado por IBM a mediados de la década de los 70, se ha convertido en un estándar para acceder bases de datos relacionales y distribuidas. SQL no es un lenguaje de desarrollo de aplicaciones y tampoco una herramienta de consulta para usuarios finales. Puede definirse como un lenguaje de manipulación y consulta de datos sobre bases de datos relacionales. Aunque cada fabricante implementa su propia versión de SQL, existen dos estándares sobre los que surgen estas versiones ANSI SQL y IBM SQL.

- 2. La sincronía en las bases de datos distribuidas.** Mantener la integridad de los datos, asegurando que los datos sean los mismos aún en un esquema distribuido, este es uno de los retos técnicos más serios. Requiere que las bases de datos permanezcan sincronizadas y sean modificados en grupo. El objetivo es implementar un procedimiento en las bases de datos, no en las aplicaciones, de tal forma que los programadores no tengan que hacerlo. Esta característica se ha adicionado gradualmente a los DBMS.
- 3. La optimización de consultas.** Otro de los grandes retos técnicos en las bases de datos distribuidas es determinar los pasos más rápidos y eficientes para realizar una consulta. Por ejemplo, supongamos que una consulta requiere una operación entre una tabla de 250,000 registros en un nodo remoto y una tabla de 1,000 registros en una PC. Sería más eficiente mover los 1,000 registros al nodo remoto. Esto es optimizar consultas, y requiere que el optimizador de consultas conozca el tamaño de las tablas en las bases de datos, la capacidad del equipo, y demás características.

ALTERNATIVAS DE UNA VERDADERA BASE DE DATOS DISTRIBUIDA

Es evidente que varias bases de datos no son completamente distribuidas, ciertas alternativas funcionan cumpliendo bien este propósito:

- ❖ **Cargando archivos de datos.** Enviar datos de un equipo mainframe o mini a una PC es muy común. De hecho, es el método más popular de distribución de datos. En algunos casos, archivos de reportes son distribuidos en lugar de reportes impresos. Los usuarios finales pueden hacer peticiones de archivos selectivamente. Las compañías que no permiten que se carguen archivos desde

la PC temen que la integridad de los datos se vea comprometida. En su lugar, los datos son extraídos de los archivos de producción y son colocados en archivos especiales o en bases de datos para tal propósito.

- ❖ **Copia de datos en nodos.** Un segundo acercamiento a bases de datos distribuidas es el colocar copias de los datos de trabajo en diversos nodos. Estos archivos son accedados por usuarios remotos para consulta y algunas veces para actualizaciones. Este método proporciona una respuesta rápida en consultas y ayuda a la actividad de procesamiento del cliente durante el día de trabajo. Los archivos maestros residen en uno o más centros de cómputo y la actualización oficial de los archivos se hace en estos centros, usualmente de noche.

- ❖ **Bases de datos no sincronizadas totalmente.** No siempre es necesario tener bases de datos distribuidas en todos los puntos todo el tiempo, **siempre y cuando** los errores puedan ser localizados y arreglados fácilmente. Donde esta alternativa sea posible que funcione, se debe considerar como una solución robusta y sencilla.

- ❖ **Bases de datos Cliente/Servidor.** Existen diferencias significativas entre una base de datos distribuida y una base de datos cliente/servidor. La diferencia estriba en el concepto de transparencia de la localización. En una verdadera base de datos distribuida, cada nodo tiene una copia del DBMS y del diccionario de datos; así que, la aplicación debe conocer la localización de los datos porque el nodo puede determinar la estrategia de acceso.

7"En los sistemas cliente/servidor, por otro lado, sólo algunos nodos corren el DBMS, de tal forma que las aplicaciones deben conocer donde se localizan los datos. De tal forma que estos sistemas no soportan el concepto de transparencia de localización". Sin embargo, estos son muy apropiados para los procesamientos de transacción de alto rendimiento. Existen fabricantes como Oracle, Sybase, Gupta Technologies, Digital, Ingres e Informix.

- ❖ **Bases de datos ligadas.** Los investigadores creen que las compañías les agrada la idea de tener bases de datos ligadas en lugar de distribuidas. Es decir, que las bases de datos existentes retienen su autonomía, los datos siguen definiéndose independientemente, y los DBMS seguirán funcionando aisladamente, mientras se crean reglas para que otros accesen los datos. Cuando bases de datos incompatibles son accedidas por una aplicación, estas bases de datos se dejan intactas. La aplicación recolecta la información en una estación de trabajo, la aplicación despliega los datos de cada base de datos en diferentes ventanas, y en el formato requerido. Para el manejo de datos no compatibles este es el método que las compañías toman.

⁷ Ralph H. Sprague Jr. *Information Systems Management in Practice*.

5.2.4 LA ADMINISTRACION DE LA INFORMACION

La preocupación de los gerentes de sistemas de información principalmente es la implementación de base de datos, y aunque intentan crear y administrar una fuente de datos corporativa, varias organizaciones no tienen bajo control sus bases de datos. Las tecnologías de información han ampliado las fuentes de datos. Este contexto requiere una administración de la información, incluyendo documentos, textos no estructurados, voz, diagramas, imágenes y cuadros estadísticos.

Las organizaciones plantean que no existe ningún progreso mientras no esté en funcionamiento todo el sistema de procesamiento de transacciones. Sin embargo, los gerentes del departamento de sistemas no pueden darse el lujo de sólo realizar una tarea a la vez. La administración de sistemas de procesamiento debe iniciar ahora, aunque la administración de datos que es sumamente importante aún no este bajo control.

CUATRO TIPOS DE INFORMACION

Para considerar todo el espectro de la información y explorarlo, como base consideramos que existen dos tipos de información generada y administrada internamente en una organización:

1. Información basada en registros, encontrados en una base de datos.
2. Información basada en documentos como reportes, opiniones, diagramas, etc.

El primer tipo de información interna pertenece principalmente a entidades, como transacciones, empleados, etc. Los registros de datos bien estructurados son

utilizados para mantener los atributos de una entidad. La segunda categoría de información pertenece principalmente a conceptos, ideas, opiniones, etc. Documentos menos estructurados y con una gran variedad de formas de información.

El mismo tipo de información es generado externamente. Hay información externa, así como información basada en documentos como reportes, periódicos, etc.

La información interna basada en registros ha tenido la atención de los sistemas de información debido a que es el tipo de información generado y administrado mediante software fácilmente. La información externa basada en registros es muy popular hoy en día debido a su forma de bases de datos públicas, bajo el esquema de Internet. Generalmente los gerentes de sistemas de información ponen poca atención a la información basada en documentos, ya sea interna o externa, estas áreas deberían ser la responsabilidad de un área especial del departamento de sistemas.

INFORMACION INTERNA BASADA EN REGISTROS

Los modelos dominantes en la administración de este tipo de información, como mencionamos son: el modelo jerárquico, el de red y el modelo relacional. Con la administración de datos orientados a objetos prometiendo jugar un papel muy importante en el futuro.

Además las técnicas están evolucionando hacia la administración de datos distribuidos. Cabe hacer notar que esta tecnología trata principalmente con datos de registros internos. Esta tecnología tiende a expandir su medio hacia la

administración de información basada en registros externos, documentos internos y documentos externos, es decir tecnología orientada a objetos.

INFORMACION INTERNA BASADA EN DOCUMENTOS

El manejo de este tipo de información ha recaído en la mayoría de las compañías en los departamentos de administración. Pero con la evolución de los procesadores de texto y demás paquetes, la supervisión ha ido cambiando. Sin embargo, el responsable en la mayoría de la compañías es el departamento de administración.

La administración de documentos es uno de los puntos cruciales que enfrenta una Gerencia actualmente. Se debe buscar la tecnología para el manejo de documentos. La administración de documentos electrónicos se puede manejar a través de diversas tecnologías, como procesadores de texto, procesadores de imágenes, hipertexto, multimedia, etc. Y hasta métodos tradicionales como microfichas, acetatos etc.

La administración de datos y la administración de documentos forman la fuente total de recursos de información dentro de la organización. El administrador de sistemas de información debe planear como unificar estas fuentes. *"A pesar de los adelantos tecnológicos en 40 años, las compañías manejan grandes cantidades de papeles de trabajo para realizar las tareas del negocio. Y a pesar de los 20 años en la administración de sistemas de información, sistemas para el soporte de decisiones, y sistemas de información gerencial. Hasta ahora se ha valorado la importancia de la información incluida en documentos, particularmente las de fuentes externas".*

^a Ralph H. Sprague Jr. *Information Systems Management in Practice.*

INFORMACION EXTERNA BASADA EN REGISTROS

Generalmente los usuarios, y no el departamento de sistemas, son los que han manejado la adquisición de información de fuentes externas. Con el crecimiento de los negocios, las compañías requieren combinar de estos servicios externos. Así como de combinar información interna y externa para un mejor entendimiento del negocio o la industria.

INFORMACION BASADA EN DOCUMENTOS EXTERNOS

Los gerentes de sistemas de información han considerado probablemente a la información basada en documentos externos la fuente menos manejable. La responsabilidad se le encomienda generalmente a la biblioteca de la compañía, si es que existe. A medida que ha crecido esta fuente de información, y más de ella es obtenida por medios electrónicos, su importancia ha crecido para ser considerada dentro de la responsabilidad del departamento de sistemas.

En resumen, los gerentes de sistemas de información necesitan expandir el panorama de la administración de información, si se planea manejar la información como un recurso corporativo. La siguiente tabla muestra las cuatro categorías de información dentro de un típico marco corporativo con fuentes de información y ejemplos de tecnología para su uso.

TABLA 5.1: LAS CATEGORÍAS DE INFORMACION.

Tipo de Información	Actividad típica corporativa	Fuentes de información	Tecnologías utilizadas
Interna basada en registros.	Depto. de sistemas de información.	Deptos. de Administración y procesamiento de transacciones.	DBMS, Diccionarios de datos, Técnicas de análisis de datos.
Interna basada en documentos.	Administración de la organización, Centro de procesamiento de documentos.	Memos, cartas, reportes, formas corporativas, etc.	Procesadores de texto, paquetes de graficación, hojas de cálculo, etc.
Externa basada en registros.	La Gerencia, los usuarios finales, mercadotecnia, etc.	Bases de Datos públicas.	Servicios de red, redes públicas, Internet.
Externa basada en documentos.	Bibliotecas.	Literatura pública, servicios de noticias, periódicos, revistas, etc.	Servicios de red, redes públicas, Internet.

5.3 LOS INFORMES

Como punto final del valor de la información y la administración de las fuentes de información. Podemos mencionar que al obtener la información, necesitamos mostrarla, darle una buena presentación y de calidad. La siguiente frase expresa esto con respecto a los informes. “Recibir informes, rendir informes y ser breves al respecto”.

Los reportes deben reflejar siempre una información clara y objetiva, el entorno de la empresa y la situación de ésta no debe ser un pretexto para modificar la información tendenciosamente, y mucho menos si son informes a toda la empresa.

Un buen gerente procura, primero, mantenerse informado en todo momento, y luego asegurarse de que su gente reciba información lo más rápido posible. Si la empresa produce un informe escrito, bien; lo usará para complementar su propio informe. El gerente sabe lo que le interesa a su gente y le proporciona información sobre esos temas. Después del informe, la anima para que formule preguntas, y si él no sabe algunas respuestas va a buscarla. Aunque el informe de la empresa podría hacer referencia a una disposición excepcional, el gerente sabe que clase de información prefiere su gente.

El gerente procura que sus informes sean breves. Estos son siempre pertinentes, los hace personalmente y con frecuencia. El gerente siempre concede tiempo para que se hagan preguntas, informa con regularidad, y reúne a su gente de improviso para darle información, siempre que es necesario.

* David Freemantle. *El superjefe*.

5.4 RESUMEN

El valor de la información está dado por dos características esenciales: **Precisión y oportunidad**. Estas características son muy importantes para la correcta toma de decisiones. Además podemos agregar valor a esta información, si ésta es también **significativa, relevante e imparcial**.

El segundo apartado de este capítulo explora la evolución de la **administración de la información** como un recurso corporativo, con el objetivo de establecer un ambiente de sistemas de información confiable y eficiente. Comienza con una revisión a la administración de datos con el objetivo de evitar la inconsistencia, redundancia e inaccesibilidad a los equipos de cómputo. La principal herramienta para lograr una buena administración de datos son los sistemas administradores de bases de datos. El reto es la administración de datos distribuidos. Finalmente, la tendencia hacia la administración de información, teniendo un contexto muy amplio, reconociendo cuatro tipos de información y enfocándose en sus características.

La organización necesita establecer una coordinación entre los documentos y registros externos e internos, la definición de datos dentro de la empresa, proporcionando a los usuarios un mejor acceso a los datos, y si es posible en una arquitectura de datos distribuidos.

Finalmente, toda información recabada a través del sistema de información organizacional, que va a ser utilizada para realizar un informe, presentación, reporte, etc. Debe ser elaborado con gran **calidad y objetividad**.

CONCLUSIONES

El objetivo de establecer una estructura de control en los sistemas de información, es que el área de sistemas de la organización funcione adecuada y eficientemente. Estas características deben ser consecuencia del control que se integra a las actividades de sistemas, las actividades y proyectos de sistemas deben ser realizados dentro del tiempo planificado, bajo el presupuesto establecido y el resultado debe ser un producto o actividad de alta calidad, ese es nuestro objetivo.

Este trabajo estudia una estructura de control dividida en 4 áreas, partiendo de la base de que la organización esta interesada en establecer una **eficiente administración de la información**.

- ❖ El control en el desarrollo de sistemas dentro de la organización.
- ❖ El control en las actividades y funcionamiento del departamento de sistemas.
- ❖ El control en las aplicaciones o sistemas en operación.
- ❖ El control Gerencial.

Para poder crear esta estructura de control la Gerencia corporativa debe ser la promotora de políticas y la interesada en que el área de sistemas no sólo funcione, sino que funcione bien. El departamento de sistemas es el responsable de toda nuestra arquitectura de sistemas de información y tecnología, y el departamento de auditoría es responsable de las revisiones.

Si la Gerencia corporativa no se ha dado cuenta de la importancia del control en los sistemas de información. Es un deber de la Gerencia de sistemas demostrar la importancia de la administración de las fuentes de información y de la creación de una estructura de control en los sistemas de información. Aunque desarrollar estas tareas nos puede llevar mucho trabajo, en un futuro, la organización ahorrará dinero, tiempos de producción y la calidad del trabajo será mayor ante la competencia.

Dentro de la empresa visualizamos 3 departamentos que conjuntamente pueden establecer adecuadamente esta estructura de control:

- ❖ **La Gerencia corporativa.** Es el departamento encargado de producir las políticas, y respaldar éstas a través de programas y planes anuales. Sobre todo la Gerencia debe estar interesada en el control, conocer y apoyar el trabajo de los departamentos de sistemas y de auditoría de sistemas.
- ❖ **El departamento de sistemas.** Es el encargado de crear e integrar la estructura de control a todo el entorno de sistemas de información, y establecer el ambiente de administración de información que permita una fácil integración.
- ❖ **El departamento de auditoría.** La supervisión periódica de los controles en cada área corresponde realizarla a este departamento, y en su caso proponer mejoras.

También, es muy importante tomar en cuenta la evaluación costo/beneficio, la relación entre el control y el riesgo de ocurrencia. El objetivo es establecer el control necesario para evitar al máximo los riesgos, no se pretende colocar controles en todos los puntos de cada actividad, requerimos optimizar los recursos en nuestra estructura de control.

SOBRE EL CONTROL EN EL DESARROLLO DE SISTEMAS

El modelo de Ingeniería de Software para el desarrollo de sistemas no será el mismo en todos los proyectos, el departamento de sistemas debe elegir el mejor modelo que se adapte a las características del proyecto. Además, el jefe del proyecto debe coordinar y definir claramente los aspectos de ingeniería de software con los aspectos administrativos. Si podemos conjugar estas tareas, los proyectos culminarán bajo los estándares de la compañía indudablemente.

En cuanto al entorno de todo proyecto tenemos que considerar varios puntos:

- ❖ El nivel que tiene la compañía en cuanto a la de administración de las **fuentes de información corporativas**.
- ❖ La **arquitectura tecnológica** de la organización y hacia donde se dirige la compañía.
- ❖ Los requerimientos y las expectativas de los **usuarios finales**.

Un proyecto bien ejecutado produce el resultado esperado, más aún, bajo las expectativas de la empresa. Tenemos 3 parámetros que cumplir en todo proyecto: **tiempo, costo y calidad**. Tal vez la Gerencia corporativa no conozca todos los avances del departamento de sistemas, pero si los proyectos se realizan bajo estos parámetros, estaremos demostrando nuestro estándar de trabajo, y adquiriendo la confianza de los usuarios y la Gerencia.

El objetivo de la estructura de control en el desarrollo de sistemas es que se realicen aplicaciones considerando las normas, procedimientos y estándares de calidad de la organización.

SOBRE EL CONTROL EN LA UNIDAD DE COMPUTO

Los controles considerados en la unidad de computo o departamento de sistemas, están integrados en diversas funciones, el control se construye alrededor de éstas:

- ❖ Las políticas de la Gerencia sobre tecnología son sólo una guía para el departamento de sistemas. El responsable de la evolución tecnológica de la empresa es el departamento de sistemas. **Primero**, debemos conocer el entorno de la empresa y hacia donde quiere ir. **Segundo**, analizar y seleccionar la mejor alternativa tecnológica en diverso plazos de tiempo. Y **tercero** proponer y saber proponer las ideas a la empresa.

- ❖ La seguridad en los sistemas de información es un punto de gran interés para la compañía. El departamento de sistemas debe analizar todo avance sobre seguridad y dejar claro ante la Gerencia que las funciones desempeñadas en esta área son eficientes y estrictas.

- ❖ Establecer el plan de contingencia y restablecimiento, donde todo punto de este plan debe estar **verificado y probado**. Debemos encontrar alternativas a todos los procedimientos normales, medidas de respaldo de datos, y describir exactamente **que hacer ante cualquier circunstancia**. Desde circunstancias en las que tenemos que continuar la operación de la empresa, hasta circunstancias catastróficas.

- ❖ El inventario de recursos y el respaldo de información. El inventario de recursos tiene más de un objetivo, primero saber donde está ubicado todo nuestro equipo de cómputo, segundo la evaluación del equipo nos conduce hacia el análisis de riesgos y la implantación de controles. Por otra parte el respaldo de información requiere de aspectos de seguridad y recuperación, debemos poder garantizar esto ante la Gerencia.

- ❖ La administración de los recursos humanos. El objetivo no es sólo saber administrar los recursos humanos, sino estar involucrados desde el reclutamiento hasta la contratación.

La Gerencia y el departamento de auditoría deben estar interesados e involucrados en la estructura de control alrededor del departamento de sistemas, ya que éste es el elemento principal de la administración de los sistemas de información y de la evolución de la arquitectura tecnológica en la organización.

SOBRE EL CONTROL EN LAS APLICACIONES

El control en las aplicaciones comprende básicamente que se cumpla toda la normatividad y procedimientos en el uso de los sistemas en operación. No tiene sentido establecer toda una **administración de las fuentes de información corporativas y de control**, si las normatividades y procedimientos no se cumplen.

La Gerencia debe proporcionar el peso suficiente al departamento de auditoría en todas las áreas de control, aunque es más notorio el trabajo sobre el control en las aplicaciones. Esta revisión sobre las aplicaciones nos ayuda a corroborar el manejo de los datos de entrada, que procesos automáticos se aplican, y el manejo de datos de salida.

Debemos analizar las recomendaciones del departamento de auditoría en todas las áreas de sistemas, aunque en esta área (control en las aplicaciones), podemos **descubrir y corregir errores** que no se habían detectado antes. Y sobre todo eliminar prácticas negativas en el uso de nuestros sistemas de información.

SOBRE EL CONTROL GERENCIAL Y EL VALOR DE LA INFORMACION

El trabajo de la Gerencia corporativa en el área de sistemas de información consiste en la producir políticas que apoyen la evolución tecnológica de la compañía, la creación de una estructura de control y transmitir al departamento de sistemas que requiere la compañía. Las tareas generales de la Gerencia son las siguientes:

- ❖ **Producir** las políticas que el departamento de sistemas pueda utilizar para establecer estándares, normas y procedimientos de control.
- ❖ **Definir** las funciones y responsabilidades del departamento de sistemas de información y del departamento de auditoría.
- ❖ **Definir** los criterios para el plan de presupuestos y adquisiciones dentro de la compañía.
- ❖ **Considerar** los requerimientos externos que afectan a la compañía. Sobre todo lo que se refiere a los aspectos legales que involucran a los sistemas de información.

Por otro lado la Gerencia del departamento de sistemas tiene dos tareas esenciales en su relación con la Gerencia de la compañía:

- ❖ **La planeación** de los sistemas de información a corto, mediano y largo plazo. La planeación debe considerar cual es el objetivo de la organización, y como está funcionando la empresa.

- ❖ Considerar como afecta al departamento de sistemas las disposiciones de la Gerencia. El departamento de sistemas debe construir una gran **confiabilidad** acerca de su trabajo ante alta Gerencia. Proponer los planes y proyectos de tal forma, que el objetivo este claro y se consideren factibles de llevar a cabo desde la primera impresión ante la Gerencia.

El **valor** de la información puede ser incrementado por la empresa en la forma en que ésta visualice la importancia del entorno de sistemas y tecnología alrededor de nuestras **fuentes de información y control**.

La alta Gerencia tiene una visión administrativa de la estructura de control, para construir este esquema de control se requiere de una visión técnica alrededor de la información, integrar ambas perspectivas es función del departamento de sistemas. De este modo, no sólo es importante conocer porque la información es valiosa corporativamente, sino como vamos a utilizar la tecnología para cumplir con nuestro objetivo.

Sabremos que el objetivo se ha logra, si podemos afirmar que la información obtenida a través del sistema de información de la organización es confiable, eficiente, que el canal de acceso es único, y que existe una arquitectura tecnológica y una estructura de control que **respalda cada dato obtenido**. Para ello cada elemento de la empresa sabe cual es su función y trabaja para ello en la empresa.

Establecer el **control** y la administración de la información dentro de la organización, es una tarea que corresponde a la Gerencia corporativa encabezarlo con el apoyo del departamento de auditoría y del departamento de sistemas de información.



BIBLIOGRAFIA

1. **Charette, Robert N.** Software Engineering Environments, Concepts and Technology. New York, U.S.A. ed. Intertext Publications Inc., McGraw-Hill Book Company. 1986. 407 pp.
2. **Sommerville, Ian.** Software Engineering. 4ª Edición. ed. Addison Wesley. 1992. 649 pp.
3. **Haynes, Marion E.,** Administración de Proyectos, Desde la Idea Hasta la Implantación. tr. Tejera, Hector G. ed. Grupo Editorial Iberoamericana S. A. de C. V. México. 1992. 85 pp.
4. **Li, David H.** Auditoría en Centros de Computo: Objetivos, Lineamientos y Procedimientos. 1ª Edición. tr. Pérez Moreno, Laura. ed. Trillas. México. 1989. 165 pp.
5. **Mair, William C.; Wood, Donald R.; Davis, Keagle W.** Control y Auditoría del Computador. 1ª Edición. tr. C.P. Ortega de Casso, Beatriz E.; C.P. Minvielle Mendez, Luis. ed. Instituto Mexicano de Contadores Públicos A. C. México. 1980. 608 pp.

6. **Stallings, William.** Network and Internetwork Security. Principles and Practice. ed. Prentice-Hall. Englewood Cliffs, New Jersey. 1995. 462 pp.
7. **Kaufman, Charlie; Perlman, Radia; Speciner, Mike.** Network Security. Private Communications in a Public World. ed. Prentice-Hall, Series in Computer Networking and Distributed Systems. Englewood Cliffs, New Jersey. 1995. 462 PP.
8. **Fischer, Royal P.** Seguridad en los Sistemas Informáticos. tr. Fernández Sánchez, Encarnación; Fernández Sánchez Carlos; ed. Diaz Santos S. A. Madrid, España. 1988. 264 pp.
9. **Katzan Jr., Harry.** The Standard Data Encryption Algorithm. 1ª Edición. ed. Petrocelli Book. New York, U.S. 1977. 134 pp.
10. **Handy, Charles B.** Understanding Organizations. 3ª Edición. ed. Penguin Business. England. 1985. 487 pp.
11. **Senn, James A.** Análisis y Diseño de Sistemas de Información. tr. Urbina Medal, Edmundo; Palmas Velasco, Oscar. Naucalpan de Juaréz, México. 1992. 942 pp.
12. **Olle, Willian; et. al.** Information Systems Methodologies: A Framework for Understanding. ed. Addison-Wesley Publishing Company. Great Britain. 1991. 401 pp.

13. **Sprague, Jr. Ralph; McNurlin Barbara C.** Information Systems Management in Practice. 3ª Edición. ed. Prentice-Hall. Englewood Cliffs, New Jersey. 1993. 554 pp.
14. **Instituto Mexicano de Contadores Públicos.** Normas y Procedimientos de Auditoría; Tomo I. ed. IMCP A. C. 11ª Edición. México. 439 pp.
15. **Prieto Sierra, Carlos; Suárez Obregón, Carlos.** Introducción a los Negocios. Operación de la Empresa. ed. Banca y Comercio. 4ª Edición. Cd. de México. 1996. 235 pp.
16. **Freemantle, David.** El Superjefe, Como Dirigir con Exito. tr. W. De Rosas, Gisela. ed. Norma. Colombia. 1986. 275 pp.
17. **Pfaffenberger, Bryan.** Diccionario para Usuarios de Computadoras. tr. Ibarra Mercado, Victor Hugo; Ocampo Rivera Alfredo. ed. Prentice-Hall Hispanoamericana S. A. 3ª Edición. México 1993. 378 pp.
18. **Peñalosa, Eduardo; Rezende, Thais.** La Piratería de Software: Riesgos y Alternativas. El Economista. Año I, Numero XXI. 21 de Octubre de 1996. 2 pp.
19. **Schuster Vergara, Santiago.** La Tecnología y los Derechos de los Autores. Simposio de la OMPI Sobre los Derechos de Autor en la Infraestructura Global de la Información. Cd. de México, 22 a 24 de mayo de 1995. pp. 259-275.