ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

Instituto de Ciencias Matemáticas

"DISEÑO DE CONTROLES DE APLICACIÓN GENERALES EN LA IMPLEMENTACIÓN DE SISTEMAS DE INFORMACIÓN"

TESIS DE GRADO

Previa la obtención del título de:

AUDITOR EN CONTROL DE GESTIÓN

Presentada por:

Adriana E. Salvador Guncay

GUAYAQUIL- ECUADOR

AÑO

2009

DEDICATORIA

Dedico este trabajo a mi madre Cecilia Guncay quien fue mi amiga, consejera y ahora es mi ángel guardián que cuida y guía mis pasos desde el cielo.

A Dios por ser mi motor de vida, la fuerza suprema que me anima a seguir cada día.

Y a mis hermanos que me devolvieron las ganas de vivir y de seguir adelante a pesar de las adversidades de la vida. Gracias.

AGRADECIMIENTO

A cada miembro de mi familia, quienes me escuchan, me empujan a seguir adelante y siempre están a mi lado; a mi padre por apoyarme en mi formación académica, a esta prestigiosa institución por acogerme y formarme y a los profesores que me impartieron sus conocimientos. Gracias.

TRIBUNAL DE GRADUACIÓN

Ing. Guillermo Baquerizo	MAE. Alice Naranjo
PRESIDENTE	DIRECTORA DE TESIS
Ing. Miquel Ángel Chang	Ing. Pablo Álvarez
PRIMER VOCAL PRINCIPAL	PRIMER VOCAL ALTERNO

DECLARACIÓN EXPRESA

"La responsabilidad del contenido de esta Tesis de Grado, me corresponde; y el patrimonio intelectual de la misma a la Escuela Superior Politécnica del Litoral".

Adriana E. Salvador Guncay

RESUMEN

El tema “DISEÑO DE CONTROLES DE APLICACIÓN GENERALES EN LA IMPLEMENTACIÓN DE SISTEMAS DE INFORMACIÓN”, consistió en establecer los controles que se requieren en el proceso de implementación de los sistemas de información.

Los sistemas de información son en la actualidad una herramienta que bien implementada se convierte en un arma competitiva en los negocios, así como las empresas buscan diferenciarse de su competencia, los sistemas de información (SI) son una manera de hacerlo.

Se tomaron en cuenta los parámetros que establecen ciertas normas y/o estándares internacionales tales como: COSO, SAC, ISO 17799 y COBIT; y se utilizaron los más aplicables a la implementación de los sistemas de información, luego de la respectiva revisión de cada norma.

De esta manera se pudo establecer cada proceso a seguir, determinando los objetivos de control y las políticas aplicables a los mismos, mediante la elaboración de un manual que debe seguir cada empresa que requiere implementar un sistema de información eficaz y eficiente; determinando los

riesgos que se presentan en el transcurso de la implementación, sabiendo que deben mitigarse mediante la aplicación de los controles establecidos en el manual elaborado; teniendo como referencia los procesos del estándar internacional COBIT.

ÍNDICE GENERAL

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

ABREVIATURAS

AAA American Accounting Association (Asociación Americana de Contabilidad)

AICPA American Institute of Certified Public Accountants (Instituto Americano de Contadores Públicos Certificados)

COSO Comité de Organizaciones Patrocinadoras de la Comisión Treadway.

ERP Enterprise Resource Planning (Planificación de Recursos de la Empresa)

FEI Financial Executive Institute

ISO Organización Internacional de Normalización.

IIA Institute of Internal Auditors (Instituto de Auditores Internos)

IMA Institute of Management Accountants (Instituto de Contadores de Gestión)

PCGA Principios de Contabilidad Generalmente Aceptados

TI Tecnología de Información

INTRODUCCIÓN

En el capítulo I se establecen los antecedentes de los sistemas de información y los riesgos a los que están expuestos los mismos; además se redactan varias definiciones de los sistemas de información realizados por diferentes autores que exponen su diferente punto de vista.

En el capítulo II se redactan los controles necesarios en los sistemas de información, la seguridad que deben tener estos sistemas según la metodología del ciclo de vida, resaltando la fase de implementación.

En el capítulo III se detallan los estándares internacionales y las normativas que se deben seguir y tomar en cuenta en el proceso de la elaboración del manual de controles de aplicación generales en la implementación de los sistemas de información en las empresas.

En el capítulo IV se detallan los parámetros que deben seguirse, estableciendo las responsabilidades, los análisis de riesgo y todos los controles que deben aplicarse en la fase de implementación de los sistemas de información.

CAPÍTULO I

1.0 ANTECEDENTES

1.1. LOS SISTEMAS DE INFORMACIÓN

1.1.1 Definiciones

Sistema de Información

- Según Nolan “Es un grupo de gente, una serie de procedimientos o equipo de procesamiento de datos que escoge, almacenan, procesan y recuperan datos para disminuir la incertidumbre en la toma de decisiones mediante el suministro de información a los niveles gerenciales para que sea utilizada eficientemente”.

- Según James Senn “Es el medio por el cual los datos fluyen de una persona o departamento hacia otros y puede ser cualquier cosa, desde la comunicación interna entre los diferentes componentes de la organización y líneas telefónicas hasta sistemas de cómputo que generan reportes periódicos para varios usuarios”.

- Según la Real Academia de la Lengua “Es un conjunto organizado de cosas o partes interactuantes e interdependientes, que se relacionan formando un todo unitario y complejo”.

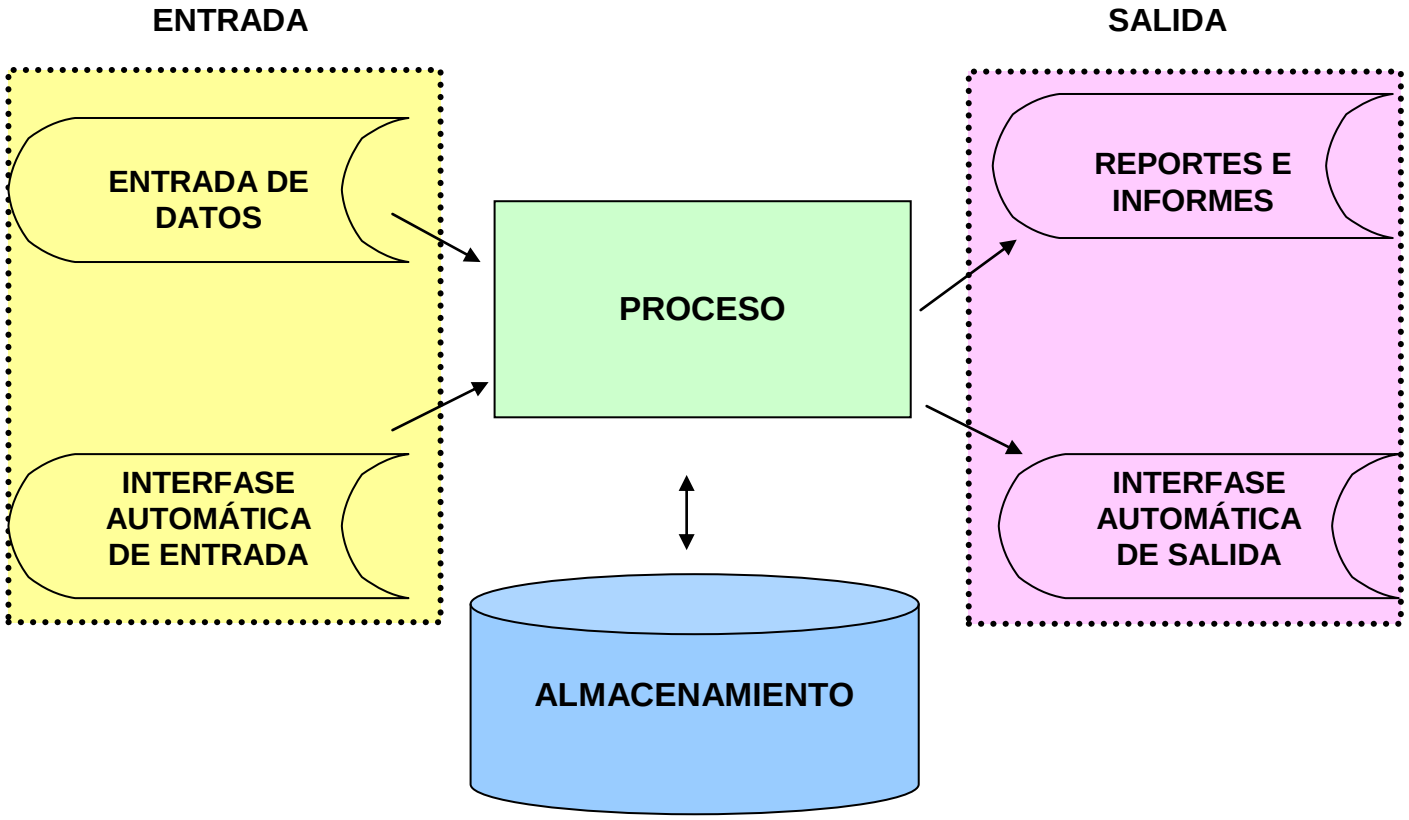
Cabe aclarar que las cosas o partes que componen al sistema, no se refieren al campo físico (objetos), sino más bien al funcional. De este modo las cosas o partes pasan a ser funciones básicas realizadas por el sistema. Podemos enumerarlas en: entradas, procesos, almacenamientos y salidas.

1.1.2 Elementos de un sistema de información

Según Richard Nolan los elementos de un sistema de información son:

1. Entrada de Información
2. Almacenamiento de Información
3. Procesamiento de Información
4. Salida de Información

Figura 1.0 Elementos de un Sistema de Información según Nolan



- **Entrada de Información:**

Es el proceso mediante el cual el Sistema de Información toma los datos que requiere para procesar la información. Las entradas pueden ser manuales o automáticas. Las manuales son aquellas que se proporcionan en forma directa por el usuario, mientras que las automáticas son datos o información que provienen o son tomados de otros sistemas o módulos. Esto último se denomina interfases automáticas.

Las unidades típicas de entrada de datos a las computadoras son las terminales, los CD, los DVD, los PenDrive, las unidades de diskette, los códigos de barras, los escáners, la voz, los monitores sensibles al tacto, el teclado y el mouse, entre otras.

- **Almacenamiento de información:**

El almacenamiento es una de las actividades o capacidades más importantes que tiene una computadora, ya que a través de esta propiedad el sistema puede recordar la información guardada en la sección o proceso anterior. Esta información suele ser almacenada en estructuras de información denominadas archivos. La unidad típica de almacenamiento son los discos magnéticos o discos duros, los discos flexibles o diskettes y los discos compactos (CD-ROM).

- **Procesamiento de Información:**

Es la capacidad del Sistema de Información para efectuar cálculos de acuerdo con una secuencia de operaciones preestablecida. Estos cálculos pueden efectuarse con datos introducidos recientemente en el sistema o bien con datos que están almacenados. Esta característica de los sistemas permite la transformación de datos fuente en información que puede ser

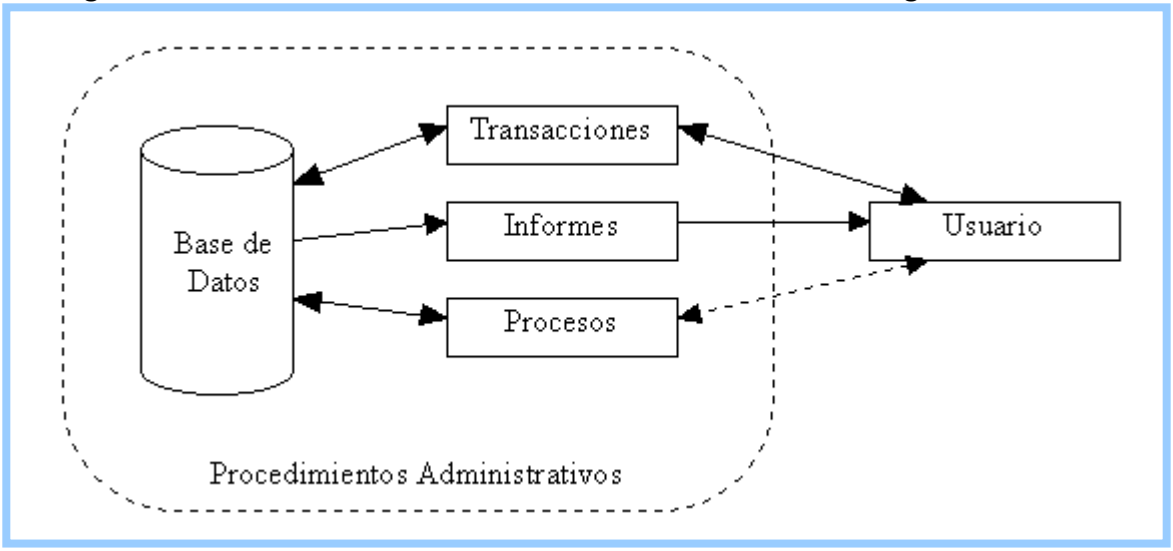
utilizada para la toma de decisiones, lo que hace posible, entre otras cosas, que un tomador de decisiones genere una proyección financiera a partir de los datos que contiene un estado de resultados o un balance general de un año base.

- **Salida de Información:**

La salida es la capacidad de un Sistema de Información para sacar la información procesada o bien datos de entrada al exterior. Las unidades típicas de salida son las impresoras, terminales, diskettes, cintas magnéticas, la voz, los graficadores y los plotters, entre otros. Es importante aclarar que la salida de un Sistema de Información puede constituir la entrada a otro Sistema de Información o módulo. En este caso, también existe una interfase automática de salida. Por ejemplo, el Sistema de Control de Clientes tiene una interfase automática de salida con el Sistema de Contabilidad, ya que genera las pólizas contables de los movimientos procesales de los clientes.

Según James A. Senn un Sistema de Información está compuesto por 6 elementos claramente identificables, tal y como se muestran en la siguiente figura:

Figura 1.1 Elementos de un Sistemas de información según Senn



1. **Base de Datos/Archivos:**

Es donde se almacena toda la información que se requiere para la toma de decisiones. La información se organiza en registros específicos e identificables.

2. **Transacciones:**

Corresponde a todos los elementos de interfaz que permiten al usuario: consultar, agregar, modificar o eliminar un registro específico de Información.

3. **Informes:**

Corresponden a todos los elementos de interfaz mediante los cuales el usuario puede obtener uno o más registros y/o información de tipo estadístico (contar, sumar) de acuerdo a criterios de búsqueda y selección definidos.

4. **Procesos:**

Corresponden a todos aquellos elementos que, de acuerdo a una lógica predefinida, obtienen información de la base de datos y generan nuevos registros de información. Los procesos sólo son controlados por el usuario (de ahí que aparezca en línea de puntos).

5. **Usuario:**

Identifica a todas las personas que interactúan con el sistema, esto incluye desde el máximo nivel ejecutivo que recibe los informes de estadísticas procesadas, hasta el usuario operativo que se encarga de recolectar e ingresar la información al sistema.

6. **Procedimientos Administrativos:**

Corresponde al conjunto de reglas y políticas de la organización, que rigen el comportamiento de los usuarios frente al sistema. Particularmente, debieran

asegurar que nunca, bajo ninguna circunstancia un usuario tenga acceso directo a la Base de Datos ("cocinar datos")...

1.1.3 Actividades que realiza un Sistema de Información

Los Sistemas de Información realizan varios tipos de actividades, según el área en el cual sea usado.

El uso de la información del sistema depende de los requerimientos de los usuarios del mismo.

A continuación se detallan las diferentes actividades que se pueden realizar en un Sistema de Información de Control de Clientes.

Entradas:

- Datos generales del cliente: nombre, dirección, tipo de cliente, etc.
- Políticas de créditos: límite de crédito, plazo de pago, etc.
- Facturas (interfase automática).
- Pagos, depuraciones, etc.

Proceso:

- Cálculo de antigüedad de saldos.
- Cálculo de intereses moratorios.

- Cálculo del saldo de un cliente.

Almacenamiento:

- Movimientos del mes (pagos, depuraciones).
- Catálogo de clientes.
- Facturas.

Salidas:

- Reporte de pagos.
- Estados de cuenta.
- Pólizas contables (interfase automática)
- Consultas de saldos en pantalla de una terminal.

1.1.4 Evolución de los Sistemas de Información

Un sistema de información es un conjunto de elementos que interactúan entre sí con el fin de apoyar las actividades de una empresa o negocio. Estos elementos son de naturaleza diversa y normalmente incluyen:

- El equipo computacional, es decir, el hardware necesario para que el sistema de información pueda operar. Lo constituyen las computadoras y el equipo periférico que puede conectarse a ellas.
- El recurso humano que interactúa con el Sistema de Información, el cual esta formado por las personas que utilizan el sistema, alimentándolo con datos o utilizando los resultados que genere.
- Los datos o información fuente que son introducidos en el sistema; son todas las entradas que necesita el sistema para generar como resultado la información que se desea.
- Los programas que son procesados y producen diferentes tipos de resultados. Los programas son parte del software del sistema de información que hará que los datos de entrada introducidos sean procesados correctamente y generen los resultados que se esperan.

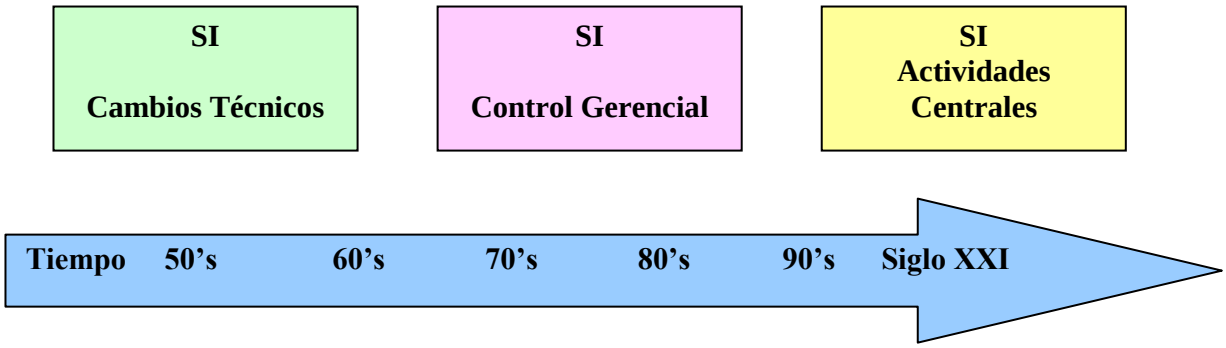
En los años 50 aparecen las primeras computadoras, con esta nueva tendencia los sistemas de información que se realizaban de forma manual en las empresas, empezaron a realizarse de forma automatizada.

En los años 60 por el uso de sistemas de información computacionales sin los controles necesarios, se empezaron a detectar fraudes financieros; como desvíos de dinero en los sistemas financieros informáticos por los que se implementan medidas de control para disminuir este tipo de riesgos.

En los años 80 muchas empresas construyeron sus sistemas de información en forma incremental. Pensaron en soluciones individuales a problemas específicos. Invirtieron con base en necesidades específicas. Se concentraron en resolver problemas inmediatos. Generaron Sistemas de información con capacidades poco coordinadas. Comunicación deficiente entre sistemas. La Gerencia entendía poco, cómo la TI apoyaba metas estratégicas del negocio. No había un plan general para evaluar la TI. No existía visión integrada de los sistemas.

A finales de los años 90 hasta la actualidad se incrementó la implantación de ERP's para simplificar y estandarizar la infraestructura de la información. Surgió la necesidad de acceder a información fiable para mejorar las interacciones y comunicaciones con clientes y proveedores. Se desea mejorar los procesos del negocio gracias a una mejor disponibilidad y calidad de datos e información del funcionamiento de la empresa.

Figura 1.2 Evolución de los sistemas de información



La evolución que tienen los Sistemas de Información en las organizaciones tiene como inicio los Sistemas Transaccionales y, posteriormente, se introducen los Sistemas de Apoyo a las Decisiones. Por último, se desarrollan los Sistemas Estratégicos que dan forma a la estructura competitiva de la empresa.

En la década de los setenta, Richard Nolan, un conocido autor y profesor de la Escuela de Negocios de Harvard, desarrolló una teoría que impactó el proceso de planeación de los recursos y las actividades de la informática.

Según Nolan, “la función de la Informática en las organizaciones evoluciona a través de ciertas etapas de crecimiento”, las cuales se explican a continuación:

1. **Etapa de contagio o expansión. Los aspectos sobresalientes que permiten diagnosticar rápido que una empresa se encuentra en esta etapa son:**

- Se inicia con la implantación exitosa del primer Sistema de Información en la organización. Como consecuencia de lo anterior, el primer ejecutivo usuario se transforma en el paradigma o persona que se habrá que imitar.
- Las aplicaciones que con frecuencia se implantan en esta etapa son el resto de los Sistemas Transaccionales no desarrollados en la etapa de inicio, tales como facturación, inventarios, control de pedidos de clientes y proveedores, cheques, etc.

- El pequeño departamento es promovido a una categoría superior, donde depende de la Gerencia Administrativa o Contraloría.
- El tipo de administración empleado está orientado hacia la venta de aplicaciones a todos los usuarios de la organización; en este punto suele contratarse a un especialista de la función con preparación académica en el área de sistemas.
- Se inicia la contratación de personal especializado y nacen puestos tales como analista de sistemas, analista-programador, programador de sistemas, jefe de desarrollo, jefe de soporte técnico, etc.
- Las aplicaciones desarrolladas carecen de interfases automáticas entre ellas, de tal forma que las salidas que produce un sistema se tienen que alimentar en forma manual a otro sistema, con la consecuente irritación de los usuarios.
- Los gastos por concepto de sistemas empiezan a crecer en forma importante, lo que marca la pauta para iniciar la racionalización en el uso de los recursos computacionales dentro de la empresa. Este problema y el inicio de su solución marcan el paso a la siguiente etapa.

2. **Etapa de control o formalización. Para identificar a una empresa que transita por esta etapa es necesario considerar los siguientes elementos:**

- Esta etapa de evolución de la Informática dentro de las empresas se inicia con la necesidad de controlar el uso de los recursos computacionales a través de las técnicas de presupuestación base cero (partiendo de que no se tiene nada) y la implantación de sistemas de cargos a usuarios (por el servicio que se presta).
- Las aplicaciones están orientadas a facilitar el control de las operaciones del negocio para hacerlas más eficaces, tales como sistemas para control de flujo de fondos, control de órdenes de compra a proveedores, control de inventarios, control y manejo de proyectos, etc.
- El departamento de sistemas de la empresa suele ubicarse en una posición gerencial, dependiendo del organigrama de la Dirección de Administración o Finanzas.
- El tipo de administración empleado dentro del área de Informática se orienta al control administrativo y a la justificación económica de las aplicaciones a desarrollar. Nace la necesidad de establecer criterios para las prioridades en el desarrollo de nuevas aplicaciones. La cartera de aplicaciones pendientes por desarrollar empieza a crecer.
- En esta etapa se inician el desarrollo y la implantación de estándares de trabajo dentro del departamento, tales como: estándares de documentación,

control de proyectos, desarrollo y diseño de sistemas, auditoría de sistemas y programación.

- Se integra a la organización del departamento de sistemas, personal con habilidades administrativas y preparado técnicamente.
- Se inicia el desarrollo de interfases automáticas entre los diferentes sistemas.

3. **Etapa de integración. Las características de esta etapa son las siguientes:**

- La integración de los datos y de los sistemas surge como un resultado directo de la centralización del departamento de sistemas bajo una sola estructura administrativa.
- Las nuevas tecnologías relacionadas con base de datos, sistemas administradores de bases de datos y lenguajes de cuarta generación, hicieron posible la integración.
- En esta etapa surge la primera hoja electrónica de cálculo comercial y los usuarios inician haciendo sus propias aplicaciones. Esta herramienta ayudó mucho a que los usuarios hicieran su propio trabajo y no tuvieran que esperar a que sus propuestas de sistemas fueran cumplidas.
- El costo del equipo y del software disminuyó por lo cual estuvo al alcance de más usuarios.

- En forma paralela a los cambios tecnológicos, cambió el rol del usuario y del departamento de Sistemas de Información. El departamento de sistemas evolucionó hacia una estructura descentralizada, permitiendo al usuario utilizar herramientas para el desarrollo de sistemas.
- Los usuarios y el departamento de sistema iniciaron el desarrollo de nuevos sistemas, reemplazando los sistemas antiguos, en beneficio de la organización.

4. **Etapa de administración de datos. Entre las características que destacan en esta etapa están las siguientes:**

- El departamento de Sistemas de Información reconoce que la información es un recurso muy valioso que debe estar accesible para todos los usuarios.
- Para poder cumplir con lo anterior resulta necesario administrar los datos en forma apropiada, es decir, almacenarlos y mantenerlos en forma adecuada para que los usuarios puedan utilizar y compartir este recurso.
- El usuario de la información adquiere la responsabilidad de la integridad de la misma y debe manejar niveles de acceso diferentes.

5. **Etapa de madurez. Entre los aspectos sobresalientes que indican que una empresa se encuentra en esta etapa, se incluyen los siguientes:**

- Al llegar a esta etapa, la Informática dentro de la organización se encuentra definida como una función básica y se ubica en los primeros niveles del organigrama (dirección).
- Los sistemas que se desarrollan son Sistemas de Manufactura Integrados por Computadora, Sistemas Basados en el Conocimiento y Sistemas Expertos, Sistemas de Soporte a las Decisiones, Sistemas Estratégicos y, en general, aplicaciones que proporcionan información para las decisiones de alta administración y aplicaciones de carácter estratégico.
- En esta etapa se tienen las aplicaciones desarrolladas en la tecnología de base de datos y se logra la integración de redes de comunicaciones con terminales en lugares remotos, a través del uso de recursos computacionales.

Tendencias Futuras de los Sistemas de Información

El uso de la tecnología de información en las empresas se ha incrementado considerablemente y en un futuro será aún mayor. Las principales tendencias respecto a los Sistemas de Información son las siguientes:

- La tecnología de información se usará como parte de la estrategia corporativa, es decir, el uso de los Sistemas de Información que dan ventaja competitiva (sistemas estratégicos) se incrementará. Las empresas de más éxito serán manejadas por personas que sean capaces de desarrollar aplicaciones estratégicas de la tecnología de la Información de manera creativa.
- La tecnología será parte del trabajo en equipo en las empresas. Esta tecnología será usada para reducir el trabajo, mejorar la calidad, dar mejores servicios a los clientes o para cambiar la forma en que ser trabaja. Los trabajadores usarán las computadoras personales conectadas en red, y las fábricas usarán la tecnología para el diseño y control de producción.
- El uso de la tecnología transformará a la organización y cambiará su estructura. Como ejemplo de ello puede verse el uso del correo electrónico, el intercambio electrónico de datos y el acceso a información externa por medio de redes como Internet.
- La tecnología facilitará la creación de las oficinas virtuales para las personas que requieren estar en diferentes localidades, permitiendo el uso del correo electrónico y de conferencias por computadoras y de esta manera facilitar la comunicación global.
- La tecnología de información apoyará de manera importante el rediseño de los procesos de negocios. Las técnicas de reingeniería de procesos continuarán apoyándose en los sistemas de información.

La tecnología de información será más inteligente y reducirá aún más la interacción humana.

1.1.5 Características de los sistemas de información modernos

Los sistemas de información modernos cumplen ciertas características que hacen que el usuario pueda interactuar con ellos con mayor facilidad.

Entre las características más importantes tenemos:

1. Sistemas sencillos sirviendo a funciones y niveles múltiples dentro de la empresa.
2. Acceso inmediato en línea a grandes cantidades de información.
3. Fuerte confiabilidad en la tecnología de telecomunicaciones.
4. Mayor cantidad de inteligencia y conocimientos implícita en los sistemas.
5. La capacidad para combinar datos y gráficas.

- **Sistemas sencillos sirviendo a funciones y niveles múltiples dentro de la empresa**.- Los Sistemas de Información deben ser fáciles de entender, para que los usuarios puedan interactuar con facilidad en el Sistema.

- **Acceso inmediato en línea a grandes cantidades de información.-** La información existente en el sistema deberá tener libre acceso al personal seleccionado, de manera fácil y oportuna según los requerimientos del usuario.

- **Fuerte confiabilidad en la tecnología de telecomunicaciones.-** La tecnología de información utilizada deberá ser confiable para poder cumplir con los controles detallados en el manual de sistemas.

- **Mayor cantidad de inteligencia y conocimientos implícita en los sistemas.-** El sistema de información implantado deberá ser fácil de comprender para usuario, pudiendo interactuar con el mismo.

- **La capacidad para combinar datos y gráficas.-** El sistema deberá ser capaz de combinar tanto datos como gráficos para poder ser más llamativo al usuario.

1.1.6 Usos de los Sistemas de Información

- La principal función de un SI es proporcionar a los encargados de la toma de decisiones, datos oportunos y exactos que les permitan tomar y aplicar las decisiones necesarias que mejoren al máximo la relación que existe entre los recursos de la empresa.
- Este sistema tiene el propósito general de ayudar a los gerentes en la planeación, control y toma de decisiones.
- Asegurar que la información exacta y confiable esté disponible cuando se necesite y que se le presente en forma fácilmente aprovechable.
- Incrementar la productividad operacional.
- Hacer que el proceso de información deje de ser información fragmentada, conjeturas inspiradas en la intuición y solución de problemas aislados.

1.1.7 Tipos de Sistemas de Información

En la década de los noventas, los sistemas de información cumplieron dentro de las organizaciones tres objetivos básicos.

1. Automatización de procesos operativos. (Sistemas transaccionales)
2. Proporcionar información que sirva de apoyo al proceso de la toma de decisiones. (Sistemas de soporte a las decisiones)

3. Lograr ventajas competitivas a través de su implementación y uso.(Sistemas estratégicos)

Los tipos de Sistemas de Información más frecuentemente usados en las organizaciones son:

1.- Sistemas Transaccionales

Sus principales características son:

- A través de éstos suelen lograrse ahorros significativos de mano de obra, debido a que automatizan tareas operativas de la organización.
- Con frecuencia son el primer tipo de Sistemas de Información que se implanta en las organizaciones. Se empieza apoyando las tareas a nivel operativo de la organización.
- Son intensivos en entrada y salida de información; sus cálculos y procesos suelen ser simples y poco sofisticados.
- Tienen la propiedad de ser recolectores de información, es decir, a través de estos sistemas se cargan las grandes bases de información para su explotación posterior.
- Son fáciles de justificar ante la dirección general, ya que sus beneficios son visibles y palpables.

2.- Sistemas de Apoyo de las Decisiones

Las principales características de estos son:

- Suelen introducirse después de haber implantado los Sistemas Transaccionales más relevantes de la empresa, ya que estos últimos constituyen su plataforma de información.
- La información que generan sirve de apoyo a los mandos intermedios y a la alta administración en el proceso de toma de decisiones.
- Suelen ser intensivos en cálculos y escasos en entradas y salidas de información. Así, por ejemplo, un modelo de planeación financiera requiere poca información de entrada, genera poca información como resultado, pero puede realizar muchos cálculos durante su proceso.
- No suelen ahorrar mano de obra. Debido a ello, la justificación económica para el desarrollo de estos sistemas es difícil, ya que no se conocen los ingresos del proyecto de inversión.
- Suelen ser Sistemas de Información interactivos y amigables, con altos estándares de diseño gráfico y visual, ya que están dirigidos al usuario final.
- Apoyan la toma de decisiones que, por su misma naturaleza son repetitivos y de decisiones no estructuradas que no suelen repetirse. Por ejemplo, un Sistema de Compra de Materiales

que indique cuándo debe hacerse un pedido al proveedor o un Sistema de Simulación de Negocios que apoye la decisión de introducir un nuevo producto al mercado.

- Estos sistemas pueden ser desarrollados directamente por el usuario final sin la participación operativa de los analistas y programadores del área de informática.
- Este tipo de sistemas puede incluir la programación de la producción, compra de materiales, flujo de fondos, proyecciones financieras, modelos de simulación de negocios, modelos de inventarios, etc.

3.- Sistemas Estratégicos

Sus principales características son:

- Su función primordial no es apoyar la automatización de procesos operativos ni proporcionar información para apoyar la toma de decisiones.
- Suelen desarrollarse in house, es decir, dentro de la organización, por lo tanto no pueden adaptarse fácilmente a paquetes disponibles en el mercado.

- Típicamente su forma de desarrollo es a base de incrementos y a través de su evolución dentro de la organización. Se inicia con un proceso o función en particular y a partir de ahí se van agregando nuevas funciones o procesos.
- Su función es lograr ventajas que los competidores no posean, tales como ventajas en costos y servicios diferenciados con clientes y proveedores. En este contexto, los Sistema Estratégicos son creadores de barreras de entrada al negocio.
- Apoyan el proceso de innovación de productos y proceso dentro de la empresa debido a que buscan ventajas respecto a los competidores y una forma de hacerlo en innovando o creando productos y procesos.

1.2. RIESGOS EN LOS SISTEMAS DE INFORMACIÓN

Riesgo.- Cualquier evento futuro incierto que puede obstaculizar el logro de los objetivos estratégicos, operativos y/o económicos, financieros de la organización.

Clasificación General

- Riesgo Estratégico
- Riesgo de Mercado
- Riesgo de Liquidez
- Riesgo de Crédito
- Riesgo Legal
- Riesgo Operacional
- Riesgo Reputacional

Principales riesgos de los Sistemas de Información

- Riesgos inherentes
- Riesgos de Control
- Riesgos de Auditoría
- Riesgo Computacional

Riesgos Inherentes

Es propio de la naturaleza del negocio, no es propiamente del departamento de sistemas.

Riesgos de Control

A pesar de que existan controles en los sistemas de información se pueden vulnerar los mismos.

Riesgos de Auditoría

No se pueden detectar todos los riesgos que tienen los sistemas de información a pesar de existir controles de Auditoría.

Riesgo Computacional

Se debe evaluar las aplicaciones y la dependencia del sistema de información, para lo cual es importante considerar responder las siguientes cuatro preguntas:

1. ¿Qué sucedería si no se puede utilizar el sistema?

Si el sistema depende de la aplicación por completo se debe definir el nivel de riesgo. Por ejemplo:

- Un sistema de llamadas de emergencias de un hospital que dependa por completo de un sistema computarizado, es un sistema de alto riesgo.

- Una lista de clientes será de menor riesgo.

Un sistema de contabilidad fuera del tiempo de balance será de menor riesgo.

2. ¿Qué consecuencias traería si es que no se pudiera acceder al sistema? Al considerar esta pregunta se debe cuidar la presencia de manuales de respaldo para emergencias o algún modo de cómo se solucionó este problema en el pasado.

3. ¿Existe un procedimiento alternativo y que problemas ocasionaría? Se debe verificar si el sistema es único o es que existe otro sistema también computarizado de apoyo menor.

4. ¿Qué se ha hecho en casos de emergencia hasta ahora? Para responder esta pregunta se debe considerar al menos las siguientes situaciones, donde se debe rescatar los acontecimientos, las consecuencias y las soluciones tomadas, considerando:

- Que exista un sistema paralelo al menos manual
- Si hay sistemas duplicados en las áreas críticas (tarjetas de red, teclados, monitores, servidores, unidades de disco, aire acondicionado).
- Si hay sistemas de energía ininterrumpida UPS.
- Si las instalaciones eléctricas, telefónicas y de red son adecuadas (se debe contar con el criterio de un experto).

CAPÍTULO II

2.0 MARCO TEÓRICO

2.1. Los controles de los sistemas de Información

Controles

- Planes, políticas y procedimientos que se establecen para prevenir o detectar riesgos que impedirían el cumplimiento de los objetivos de la Organización.

Clasificación de los Controles

Controles Preventivos

Son aquellos que disminuyen la frecuencia con que ocurren las causas del riesgo, permitiendo cierto margen de violaciones. Ejemplo:

- Sistemas de claves de acceso

Controles Detectivos

Son aquellos que no detienen que ocurran causas del riesgo sino que los detecta luego de ocurridos. En cierta forma sirvan para evaluar la eficiencia de los controles preventivos. Ejemplo:

- Procesamiento de Validación

Controles Correctivos

Ayudan a la investigación y corrección de las causas del riesgo. La corrección adecuada puede resultar difícil e ineficiente, siendo necesaria la implantación de controles detectivos sobre los controles correctivos, debido a que la corrección de errores es en sí una actividad altamente propensa a errores. Ejemplo:

- Respaldo de Datos.

Controles Administrativos del área Informática

1.- Controles de Preinstalación

2.- Controles de Organización y Planificación

3.- Controles de Sistemas en Desarrollo y Producción

4.- Controles de Procesamiento

5.- Controles de Operación

6.- Controles de uso de Microcomputadores

1.- Controles de Preinstalación Hacen referencia a procesos y actividades previas a la adquisición e instalación de un equipo de computación y obviamente a la automatización de los sistemas existentes. Objetivos:

- Garantizar que el hardware y software se adquieran siempre y cuando tengan la seguridad de que los sistemas computarizados proporcionaran mayores beneficios que cualquier otra alternativa.
- Garantizar la selección adecuada de equipos y sistemas de computación
- Asegurar la elaboración de un plan de actividades previo a la instalación

2.- Controles de organización y Planificación Se refiere a la definición clara de funciones, línea de autoridad y responsabilidad de las diferentes unidades del área PAD, en labores tales como:

- Diseñar un sistema
- Elaborar los programas
- Operar el sistema
- Control de calidad
- Se debe evitar que una misma persona tenga el control de toda una operación.

3.- Controles de Sistema en Desarrollo y Producción Se debe justificar que los sistemas han sido la mejor opción para la empresa, bajo una relación costo-beneficio que proporcionen oportuna y efectiva información, que los sistemas se han desarrollado bajo un proceso planificado y se encuentren debidamente documentados.

4.- Controles de Procesamiento Los controles de procesamiento se refieren al ciclo que sigue la información desde la entrada hasta la salida de la información, lo que conlleva al establecimiento de una serie de seguridades para:

- Asegurar que todos los datos sean procesados.
- Garantizar la exactitud de los datos procesados.
- Garantizar que se grabe un archivo para uso de la gerencia y con fines de auditoría.
- Asegurar que los resultados sean entregados a los usuarios en forma oportuna y en las mejores condiciones.

5.- Controles de Operación Abarcan todo el ambiente de la operación del equipo central de computación y dispositivos de almacenamiento, la administración de la cintoteca y la operación de terminales y equipos de comunicación por parte de los usuarios de sistemas online.

Los controles tienen como fin:

- Prevenir o detectar errores accidentales que puedan ocurrir en el Centro de Cómputo durante un proceso.
- Garantizar la integridad de los recursos informáticos.
- Asegurar la utilización adecuada de equipos acorde a planes y objetivos.

6.- Controles en el uso del Microcomputador Es la tarea más difícil pues son equipos más vulnerables, de fácil acceso, de fácil explotación pero los controles que se implanten ayudarán a garantizar la integridad y confidencialidad de la información.

2.2. Seguridad de los Sistemas de Información

La seguridad en la informática abarca los conceptos de seguridad física y seguridad lógica:

- La seguridad física, se refiere a la protección del Hardware y de los soportes de datos, así como a la de los edificios e instalaciones que los albergan. Contempla las situaciones de incendios, sabotajes, robos, catástrofes naturales, etc.
- La seguridad lógica, se refiere a la seguridad de uso del software, a la protección de los datos, procesos y programas, así como la del acceso ordenado y autorizado de los usuarios a la información.

Seguridad de un Sistema de Información

Importancia de la Información

Cuando se habla de la función informática generalmente se tiende a hablar de tecnología nueva, de nuevas aplicaciones, nuevos dispositivos de hardware, nuevas formas de elaborar información más consistente, etc.

Sin embargo se suele pasar por alto o se tiene muy implícita la base que hace posible la existencia de los anteriores elementos. Esta base es la información.

Es muy importante conocer su significado dentro la función informática, de forma esencial cuando su manejo está basado en tecnología moderna, para esto se debe conocer que la información:

- Está almacenada y procesada en computadoras
- Puede ser confidencial para algunas personas o a escala institucional
- Puede ser mal utilizada o divulgada
- Puede estar sujeta a robos, sabotaje o fraudes

Los primeros puntos nos muestran que la información está centralizada y que puede tener un alto valor y los últimos puntos nos muestran que se puede provocar la destrucción total o parcial de la información, que incurre directamente en su disponibilidad que puede causar retrasos de alto costo.

Pensemos por un momento que ahí se sufre un accidente en el centro de computo o el lugar donde se almacena la información. Ahora preguntémonos: ¿Cuánto tiempo pasaría para que la organización este nuevamente en operación?

Es necesario tener presente que el lugar donde se centraliza la información, con frecuencia el centro de cómputo, puede ser el activo más valioso y al mismo tiempo el más vulnerable.

Lo antes descrito nos conduce a pensar en riesgo y seguridad.

- **Riesgo.-** Proximidad o posibilidad de un daño, peligro, etc.

Cada uno de los imprevistos, hechos desafortunados, etc., que puede cubrir un seguro.

Sinónimos: amenaza, contingencia, emergencia, urgencia, apuro.

- **Seguridad.**- Cualidad o estado de seguro**.** Garantía o conjunto de garantías que se da a alguien sobre el cumplimiento de algo.

Ejemplo: Seguridad Social Conjunto de organismos, medios, medidas, etc., de la administración estatal para prevenir o remediar los posibles riesgos, problemas y necesidades de los trabajadores, como enfermedad, accidentes laborales, incapacidad, maternidad o jubilación; se financia con aportaciones del Estado, trabajadores y empresarios.

Se dice también de todos aquellos objetos, dispositivos, medidas, etc., que contribuyen a hacer más seguro el funcionamiento o el uso de una cosa: cierre de seguridad, cinturón de seguridad.

Delitos accidentales e incidentales

Los delitos cometidos utilizando la computadora han crecido en tamaño, forma y variedad.

En la actualidad los delitos cometidos tienen la peculiaridad de ser descubiertos en un 95% de forma casual. Podemos citar a los principales delitos hechos por computadora o por medio de computadoras, éstos son:

- Fraudes
- Falsificación
- Venta de información

Entre los hechos criminales más famosos en los E.E.U.U. están:

- El caso del Banco Wells Fargo donde se evidenció que la protección de archivos era inadecuada, cuyo error costo USD 21.3 millones.
- El caso de la NASA donde dos alemanes ingresaron en archivos confidenciales.
- El caso de un muchacho de 15 años que entrando a la computadora de la Universidad de Berkeley en California destruyó gran cantidad de archivos.
- También se menciona el caso de un estudiante de una escuela que ingresó a una red canadiense con un procedimiento de admirable

sencillez, otorgándose una identificación como un usuario de alta prioridad, y tomo el control de una embotelladora de Canadá.

- También el caso del empleado que vendió la lista de clientes de una compañía de venta de libros, lo que causo una pérdida de USD 3 millones.

Estos hechos y otros nos muestran claramente que los componentes del sistema de información no presentaban un adecuado nivel de seguridad. Ya que el delito se cometió con y sin intención. Donde se logró penetrar en el sistema de información, por ello es importante establecer seguridad en los sistemas de información.

Seguridades de los SI ante Virus Informático

Definición: El virus informático es un programa elaborado accidental o intencionadamente, que se introduce y se transmite a través de diskettes o de la red telefónica de comunicación entre ordenadores, causando diversos tipos de daños a los sistemas computarizados. Ejemplo: el virus llamado viernes trece o Jerusalén, que desactivó el conjunto de ordenadores de la defensa de Israel y que actualmente se ha extendido a todo el mundo.

Históricamente los virus informáticos fueron descubiertos por la prensa el 12 de octubre de 1985, con una publicación del New York Times que hablaba

de un virus que se distribuyó desde y aparentemente era para optimizar los sistemas IBM basados en tarjeta gráfica, pero al ejecutarlo salía la presentación pero al mismo tiempo borraba todos los archivos del disco duro, con un mensaje al finalizar que decía "Caíste".

Bueno en realidad éste fue el nacimiento de su nombre, ya que los programas con código integrado, diseñados para hacer cosas inesperadas han existido desde que existen las computadoras. Y ha sido siempre la obra de algún programador delgado de ojos de loco.

Pero las primeras referencias de virus con fines intencionales surgieron en 1983 cuando Digital Equipament Corporation (DEC) empleó una subrutina para proteger su famoso procesador de textos Decmate II, que el 1 de abril de 1983 en caso de ser copia ilegal borraba todos los archivos de su unidad de disco.

Los principales casos de crímenes cometidos empleando virus informáticos son:

- 12 de diciembre de 1987. El virus de Navidad

Una tarjeta navideña digital enviada por medio de un BBS de IBM atascó las instalaciones en los EE.UU. por 90 minutos. Cuando se ejecutaba el virus este tomaba los Address Book del usuario y se retransmitía

automáticamente, además que luego colgaba el ordenador anfitrión. Esto causó un desbordamiento de datos en la red.

- 10 de enero de 1988. El virus Jerusalén

Se ejecuta en una universidad hebrea y tiene como fecha límite el primer viernes 13 del año, como no pudieron pararlo se sufría una disminución de la velocidad cada viernes 13.

- 20 de septiembre de 1988

En Fort Worth, Texas, Donald Gene un programador de 39 años será sometido a juicio el 11 de julio por cargos delictivos de que intencionadamente contaminó el sistema informático de la empresa por ser despedido, con un virus informático el año 85. Fue la primera persona juzgada con la ley de sabotaje que entró en vigor el 1 de septiembre de 1985. El juicio duró 3 semanas y el programador fue declarado culpable y condenado a siete años de libertad condicional y a pagar USD. $12.000. Su empresa que se dedicaba a la bolsa sufrió el borrado de datos, aproximadamente 168000 registros.

- 4 de noviembre de 1988

Un virus invade miles de computadoras basadas en Unix en universidades e instalaciones de investigación militares, donde las velocidades fueron reducidas y en otros casos paradas. También el virus se propagó a escala internacional.

Se estableció que la infección no fue realizada por un virus sino por un programa gusano, diseñado para reproducirse así mismo indefinidamente y no para eliminar datos. El programa se difundió a través de un corrector de errores para correo electrónico, que se movió principalmente en Internet (Arpanet) y contaminó miles de computadoras en todo el mundo contando 6000 computadoras en centros militares en los EE.UU. , incluyendo la NASA, la Fuerza Aérea, el MIT, las universidades de Berkeley, Illinois, Boston, Stanford, Harvard, Princeton, Columbia y otras. En general se determinó que la infección se propagó en las computadoras VAX de DEC (Digital Equipament Corp) y las fabricadas por Sun Microsystems, que empleaban Unix.

Se halla al culpable Robert Morris, estudiante de 23 años, que declara haber cometido un error al propagar el gusano. Morris era el hijo de un experto en seguridad informática del gobierno.

El caso fue investigado por el FBI. Se sentenció a Morris por 5 años de prisión y una multa USD. $250.000.

- 23 de marzo del 89

Virus ataca sistemas informáticos de hospitales, variando la lectura de informes de laboratorio.

Y los últimos pero recordados vaccina, hacker, cpw543, natas, antiexe, etc.

Estos casos y muchos otros nos muestran que al realizar la auditoría se debe estudiar con mucho cuidado lo que significan los virus. Y conocer los diferentes tipos como ser: caballo de troya, gusano, trampilla, bomba de tiempo, bomba lógica y los recientes macro virus.

Pero como principal punto de partida se debe observar que el sistema:

- No tenga copias ilegales o piratas
- Que no exista la posibilidad de transmisión de virus al realizar conexiones remotas o de redes
- El acceso de unidades de disco flexible sea restringido solo a quienes las necesitan

Es muy importante manejar con discreción los resultados que se obtengan de los aspectos de seguridad, pues su mala difusión podría causar daños mayores. La información resultante de una auditoría no debe ser divulgada y se la debe mantener como reservada.

Ambiente propicio para el cultivo del crimen

En la actualidad se nota que los fraudes crecen en forma rápida, incluso mayor que los sistemas de seguridad. Se sabe que en los EE.UU. se cometen crímenes computarizados denunciados o no por más de 3 mil millones de dólares.)

Es importante para el auditor conocer las causas para que se cometan delitos, ya que una vez encontrado el problema se debe observar la raíz para sugerir su solución, entre las causas podemos citar, dos grupos:

Mayor riesgo

- Beneficio personal
- Síndrome de Robin Hood
- Odio a la organización
- Mentalidad turbada
- Equivocación de ego
- Deshonestidad del departamento
- Problemas financieros de algún individuo
- Fácil modo de desfalco

Menor riesgo

- Beneficio de la organización
- Jugando a jugar

Al ingresar al área de seguridad se debe contemplar muy estrechamente las relaciones que hay entre los aspectos: tecnológicos, humano - sociales y administrativos.

Paradigmas Organizacionales en Cuanto a Seguridad

Paradigma: Modelo o ejemplo de algo, En filosofía: Conjunto de ideas filosóficas, teorías científicas y normas metodológicas que influyen en la forma de resolver los problemas en una determinada tradición científica.

Sinónimo: prototipo, muestra, canon.

Los paradigmas desempeñan un papel importante en la actual filosofía de la ciencia, a partir de la obra de Thomas S. Kuhn "La estructura de las revoluciones científicas" (1962).

Del paradigma se desprenden las reglas que rigen las investigaciones. Cuando dentro de un paradigma aparecen anomalías excesivas, se produce una revolución científica que consiste precisamente en el cambio de paradigma.

Es muy importante que el auditor conozca los paradigmas que existen en las organizaciones sobre la seguridad, para no encontrarse con un contrincante desconocido.

Entre los principales paradigmas que se pueden encontrar veamos los siguientes:

- Generalmente se tiene la idea que los procedimientos de auditoría es responsabilidad del personal del centro de cómputo, pero se debe cambiar este paradigma y conocer que estas son responsabilidades del usuario y del departamento de auditoría interna.
- También muchas compañías cuentan con dispositivos de seguridad física para los computadores y se tiene la idea que los sistemas no pueden ser violados si no se ingresa al centro de cómputo, ya que no se considera el uso terminales y de sistemas remotos.
- Se piensa también que los casos de seguridad que tratan de seguridad de incendio o robo que "eso no me puede suceder a mí" o "es poco probable que suceda".
- También se cree que los computadores y los programas son tan complejos que nadie fuera de su organización los va a entender y no les van a servir, ignorando las personas que puedan captar y usarla para otros fines.

- Los sistemas de seguridad generalmente no consideran la posibilidad de fraude interno que es cometido por el mismo personal en el desarrollo de sus funciones.
- Generalmente se piensa que la seguridad por clave de acceso es inviolable pero no se considera a los delincuentes sofisticados.
- Se suele suponer que los defectos y errores son inevitables.
- También se cree que se hallan fallas porque nada es perfecto.
- Y la creencia que la seguridad se aumenta solo con la inspección.

Se deben analizar estos y otros paradigmas de la organización, también es muy importante que el auditor enfrente y evalúe primero sus propios paradigmas y sus paradigmas académicos.

Consideraciones Inmediatas para la Auditoría de la Seguridad

A continuación se citarán las consideraciones inmediatas que se deben tener para elaborar la evaluación de la seguridad, pero luego se tratarán las áreas específicas con mucho mayor detalle.

- Uso de la Computadora

Se debe observar el uso adecuado de la computadora y su software ya que puede ser susceptible a:

1. Tiempo de máquina para uso ajeno
2. Copia de programas de la organización para fines de comercialización (copia pirata)
3. Acceso directo o telefónico a bases de datos con fines fraudulentos

- Sistema de Acceso

Para evitar los fraudes computarizados se debe contemplar de forma clara los accesos a las computadoras de acuerdo a:

1. Nivel de seguridad de acceso
2. Empleo de las claves de acceso
3. Evaluar la seguridad contemplando la relación costo, ya que a mayor tecnología de acceso mayor costo

- Cantidad y Tipo de Información

El tipo y la cantidad de información que se introduce en las computadoras debe considerarse como un factor de alto riesgo ya que podrían producir que:

1. La información esté en manos de algunas personas
2. La alta dependencia en caso de pérdida de datos

- Control de Programación

Se debe conocer que el delito más común está presente en el momento de la programación, ya que puede ser cometido intencionalmente o no, para lo cual se debe controlar que:

1. Los programas no contengan bombas lógicas
2. Los programas deben contar con fuentes y sus últimas actualizaciones
3. Los programas deben contar con documentación técnica, operativa y de emergencia

- Personal

Se debe observar este punto con mucho cuidado, ya que hablamos de las personas que están ligadas al sistema de información de forma directa y se deberá contemplar principalmente:

1. La dependencia del sistema a nivel operativo y técnico
2. Evaluación del grado de capacitación operativa y técnica
3. Contemplar la cantidad de personas con acceso operativo y administrativo
4. Conocer la capacitación del personal en situaciones de emergencia

- Medios de Control

Se debe contemplar la existencia de medios de control para conocer cuando se produce un cambio o un fraude en el sistema.

También se debe observar con detalle el sistema ya que podría generar indicadores que pueden actuar como elementos de auditoría inmediata, aunque ésta no sea una especificación del sistema.

- Rasgos del Personal

Se debe ver muy cuidadosamente el carácter del personal relacionado con el sistema, ya que pueden surgir:

1. Malos manejos de administración
2. Malos manejos por negligencia
3. Malos manejos por ataques deliberados

- Instalaciones

Es muy importante no olvidar las instalaciones físicas y de servicios, que significan un alto grado de riesgo. Para lo cual se debe verificar:

1. La continuidad del flujo eléctrico
2. Efectos del flujo eléctrico sobre el software y hardware
3. Evaluar las conexiones con los sistemas eléctrico, telefónico, cable, etc.
4. Verificar si existen un diseño, especificación técnica, manual o algún tipo de documentación sobre las instalaciones

- Control de Residuos

Observar como se maneja la basura de los departamentos de mayor importancia, donde se almacena y quien la maneja.

1. Determinar y verificar que la basura se deposite en los lugares correspondientes
2. Verificar quién y cuándo desechó la basura.

Establecer las Áreas y Grados de Riesgo

Es muy importante el crear una conciencia en los usuarios de la organización sobre el riesgo que corre la información y hacerles comprender que la seguridad es parte de su trabajo. Para esto se deben conocer los principales riesgos que acechan a la función informática y los medios de prevención que se deben tener, para lo cual se debe:

Establecer el Costo del Sistema de Seguridad

Este estudio se realiza considerando el costo que se presenta cuando se pierde la información vs. el costo de un sistema de seguridad.

Para realizar este estudio se debe considerar lo siguiente:

1. Clasificar la instalación en términos de riesgo (alto, mediano, pequeño)
2. Identificar las aplicaciones que tengan alto riesgo
3. Cuantificar el impacto en el caso de suspensión del servicio aquellas aplicaciones con un alto riesgo
4. Formular las medidas de seguridad necesarias dependiendo del nivel de seguridad que se requiera
5. La justificación del costo de implantar las medidas de seguridad

2.3. Metodología del ciclo de vida: La implementación de sistemas

CICLO DE VIDA DE UN SISTEMA DE INFORMACIÓN

El ciclo de vida de un sistema de información es un enfoque por fases del análisis y diseño que sostiene que los sistemas son desarrollados de mejor manera mediante el uso de un ciclo específico de actividades del analista y del usuario.

Según James Senn, existen tres estrategias para el desarrollo de sistemas: el método clásico del ciclo de vida de desarrollo de sistemas, el método de desarrollo por análisis estructurado y el método de construcción de prototipos de sistemas. Cada una de estas estrategias tienen un uso amplio

en cada una de los diversos tipos de empresas que existen, y resultan efectivas si son aplicadas de manera adecuada.

Un sistema de información es el conjunto de recursos que permiten recoger, gestionar, controlar y difundir la información de toda una empresa u organización.

Desde los años setenta, los sistemas de bases de datos han ido reemplazando a los sistemas de ficheros en los sistemas de información de las empresas. Al mismo tiempo, se ha ido reconociendo la gran importancia que tienen los datos que éstas manejan, convirtiéndose en uno de sus recursos más importantes. Esto ha hecho que muchas empresas tengan departamentos que se encarguen de gestionar toda su información, que estará almacenada en una base de datos. Aparecen los papeles de administrador de datos y administrador de la base de datos, que son las personas encargadas de supervisar y controlar todas las actividades relacionadas con los datos de la empresa y con el ciclo de vida de las aplicaciones de bases de datos, respectivamente.

Un sistema de información está formado por los siguientes componentes:

- La base de datos.
- Los programas de aplicación.
- Los dispositivos físicos (ordenadores, dispositivos de almacenamiento, etc.).

- El personal que utiliza y que desarrolla el sistema.

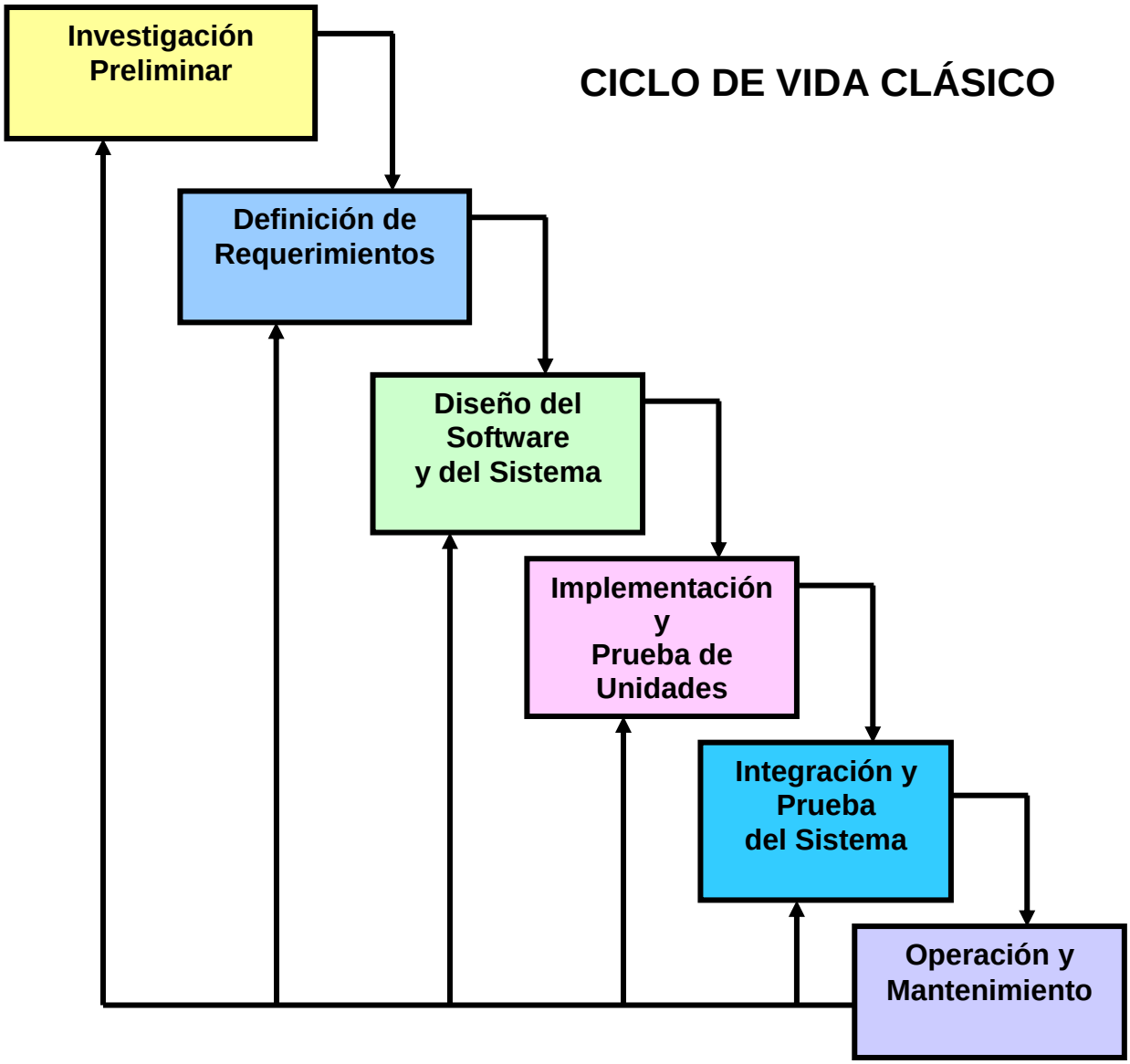
La base de datos es un componente fundamental de un sistema de información. El ciclo de vida de un sistema de información está ligado al ciclo de vida del sistema de base de datos sobre el que se apoya. Al ciclo de vida de los sistemas de información también se le denomina ciclo de vida de desarrollo del software. Las etapas típicas del ciclo de vida de desarrollo del software son: planificación, recolección y análisis de los requisitos, diseño (incluyendo el diseño de la base de datos), creación de prototipos, implementación, prueba, conversión y mantenimiento. Este ciclo de vida hace énfasis en la identificación de las funciones que realiza la empresa y en el desarrollo de las aplicaciones que lleven a cabo estas funciones. Se dice que el ciclo de vida de desarrollo del software sigue un enfoque orientado a funciones, ya que los sistemas se ven desde el punto de vista de las funciones que llevan a cabo. Por esta razón, el análisis estructurado hace énfasis en los diagramas de flujo de datos, siguiendo el movimiento de los datos a través de una secuencia de transformaciones, y refinando éstas a través de una serie de niveles. Lo mismo ocurre en el diseño estructurado, que ve a un sistema como una función que se descompone sucesivamente en niveles o subfunciones.

Concentrándose en las funciones se infravaloran los datos y, en especial, la estructura de los datos que son manipulados por las funciones. El resultado es que estos sistemas tienen valor durante poco tiempo en relación con las

necesidades de los usuarios a largo plazo. Esto sucede debido a que al poco tiempo de haber instalado un sistema, las funciones implementadas son en realidad un subconjunto de las funciones que los usuarios realmente desean. Casi inmediatamente, los usuarios descubren una gran variedad de servicios adicionales que quisieran incorporar al sistema. Estas necesidades causan problemas a los sistemas obtenidos con un diseño orientado a funciones, puesto que este diseño puede requerir una revisión importante para acomodar las funciones adicionales.

En contraste, el enfoque orientado a datos centra el foco de atención en el análisis de los datos utilizados por las funciones. Esto tiene dos ventajas. La primera es que los datos son una parte considerablemente más estable que las funciones. La segunda ventaja es que la propia estructura de un esquema de base de datos requiere de un análisis sofisticado de los datos y de sus relaciones. Una vez que se haya construido un esquema para la base de datos que sea lógico, podrían diseñarse tantas funciones como fuera necesario para sacar provecho del mismo. Sin embargo, sin un esquema tal, la base de datos sólo podría ser útil para una única aplicación. Por lo tanto, el enfoque orientado a funciones puede ser bueno para el desarrollo a corto plazo, pero pierde su valor real a largo plazo. Usando un enfoque orientado a datos, los datos pasan a ser los cimientos sobre los cuales se puede construir una gran variedad de funciones diferentes.

Figura 2.0 CICLO DE VIDA CLÁSICO DEL DESARROLLO DE SISTEMAS



El método de ciclo de vida para el desarrollo de sistemas es el conjunto de actividades que los analistas, diseñadores y usuarios realizan para desarrollar e implantar un sistema de información. El método del ciclo de vida para el desarrollo de sistemas consta de 6 fases:

1). Investigación Preliminar: La solicitud para recibir ayuda de un sistema de información puede originarse por varias razones: sin importar cuales sean estas, el proceso se inicia siempre con la petición de una persona.

2). Determinación de los requerimientos del sistema: El aspecto fundamental del análisis de sistemas es comprender todas las facetas importantes de la parte de la empresa que se encuentra bajo estudio. Los analistas, al trabajar con los empleados y administradores, deben estudiar los procesos de una empresa para dar respuesta a las siguientes preguntas clave:

¿Qué es lo que hace?

¿Cómo se hace?

¿Con qué frecuencia se presenta?

¿Qué tan grande es el volumen de transacciones o decisiones?

¿Cuál es el grado de eficiencia con el que se efectúan las tareas?

¿Existe algún problema? ¿Qué tan serio es? ¿Cuál es la causa que lo origina?

3). Diseño del sistema: El diseño de un sistema de información produce los detalles que establecen la forma en la que el sistema cumplirá con los requerimientos identificados durante la fase de análisis. Los especialistas en

sistemas se refieren, con frecuencia, a esta etapa como diseño lógico en contraste con la del desarrollo del software, a la que denominan diseño físico.

4). Desarrollo del software: Los encargados de desarrollar software pueden instalar software comprobando a terceros o escribir programas diseñados a la medida del solicitante. La elección depende del costo de cada alternativa, del tiempo disponible para escribir el software y de la disponibilidad de los programadores.

Por lo general, los programadores que trabajan en las grandes organizaciones pertenecen a un grupo permanente de profesionales.

5). Prueba de sistemas: Durante la prueba de sistemas, el sistema se emplea de manera experimental para asegurarse de que el software no tenga fallas, es decir, que funciona de acuerdo con las especificaciones y en la forma en que los usuarios esperan que lo haga.

Se alimentan como entradas un conjunto de datos de prueba para su procesamiento y después se examinan los resultados.

6). Implantación y evaluación: La implantación es el proceso de verificar e instalar nuevo equipo, entrenar a los usuarios, instalar la aplicación y construir todos los archivos de datos necesarios para utilizarla. Una vez instaladas, las aplicaciones se emplean durante muchos años. Sin embargo,

las organizaciones y los usuarios cambian con el paso del tiempo, incluso el ambiente es diferente con el paso de las semanas y los meses.

Por consiguiente, es indudable que debe darse mantenimiento a las aplicaciones. La evaluación de un sistema se lleva a cabo para identificar puntos débiles y fuertes. La evaluación ocurre a lo largo de cualquiera de las siguientes dimensiones:

- Evaluación operacional: Valoración de la forma en que funciona el sistema, incluyendo su facilidad de uso, tiempo de respuesta, lo adecuado de los formatos de información, confiabilidad global y nivel de utilización.
- Impacto organizacional: Identificación y medición de los beneficios para la organización en áreas tales como finanzas, eficiencia operacional e impacto competitivo. También se incluye el impacto sobre el flujo de información externo e interno.
- Opinión de los administradores: evaluación de las actividades de directivos y administradores dentro de la organización así como de los usuarios finales.
- Desempeño del desarrollo: La evaluación de proceso de desarrollo de acuerdo con criterios tales como tiempo y esfuerzo de desarrollo, concuerdan con presupuestos y estándares, y otros criterios de administración de proyectos. También se incluye la valoración de los métodos y herramientas utilizados en el desarrollo.

MÉTODO DE DESARROLLO POR ANÁLISIS ESTRUCTURADO

Muchos especialistas en sistemas de información reconocen la dificultad de comprender de manera completa sistemas grandes y complejos. El método de desarrollo del análisis estructurado tiene como finalidad superar esta dificultad por medio de:

1). La división del sistema en componentes

2). La construcción de un modelo del sistema.

El análisis estructurado se concentra en especificar lo que se requiere que haga el sistema o la aplicación. Permite que las personas observen los elementos lógicos (lo que hará el sistema) separados de los componentes físicos (computadora, terminales, sistemas de almacenamiento, etc.). Después de esto se puede desarrollar un diseño físico eficiente para la situación donde será utilizado.

El análisis estructurado es un método para el análisis de sistemas manuales o automatizados, que conduce al desarrollo de especificaciones para sistemas nuevos o para efectuar modificaciones a los ya existentes. Este análisis permite al analista conocer un sistema o proceso en una forma lógica y manejable al mismo tiempo que proporciona la base para asegurar que no se omite ningún detalle pertinente.

Componentes

- Símbolos gráficos
- Diccionario de datos
- Descripciones de procesos y procedimientos
- Reglas
- Diseño Estructurado

El objetivo del Diseño Estructurado es tener programas formados por módulos independientes unos de otros desde el punto de vista funcional.

La herramienta fundamental del Diseño Estructurado es el diagrama estructurado que es de naturaleza gráfica y evitan cualquier referencia relacionada con el hardware o detalles físicos. Su finalidad no es mostrar la lógica de los programas (que es la tarea de los diagramas de flujo).

Los Diagramas Estructurados describen la interacción entre módulos independientes junto con los datos que un módulo pasa a otro cuando interacciona con él.

Análisis de flujo de datos.

Estudia el empleo de los datos para llevar a cabo procesos específicos de la empresa dentro del ámbito de una investigación de sistemas usa los diagrama de flujos de datos y los diccionarios de datos.

Herramientas

Las herramientas muestran todas las características esenciales del sistema y la forma en que se ajustan entre sí, como es muy difícil entender todo un proceso de la empresa en forma verbal, las herramientas ayudan a ilustrar los componentes esenciales de un sistema, junto con sus acciones.

Diagrama de flujo de datos

Es el modelo del sistema. Es la herramienta más importante y la base sobre la cual se desarrollan otros componentes.

El modelo original se detalla en diagramas de bajo nivel que muestran características adicionales del sistema. Cada proceso puede desglosarse en diagramas de flujos de datos cada vez más detallados. Repitiéndose esta secuencia hasta que se obtienen suficientes detalles para que el analista comprenda la parte del sistema que se encuentra bajo investigación.

El diagrama físico de datos da un panorama del sistema en uso, dependiente de la implantación, mostrando cuales tareas se hacen y como son hechas. Incluyen nombres de personas, nombres o números de formato y documento, nombres de departamentos, archivos maestro y de transacciones, equipo y dispositivos utilizados, ubicaciones, nombres de procedimientos.

El diagrama lógico de datos da un panorama del sistema, pero a diferencia del físico es independiente de la implantación, que se centra en el flujo de datos entre los procesos, sin considerar los dispositivos específicos y la localización de los almacenes de datos o personas en el sistema. Sin indicarse las características físicas.

Notaciones: son cuatro símbolos, que fueron desarrollados y promovidos al mismo tiempo por dos organizaciones: Yourdon y Gane y Sarson.

Flujo de datos: son movimientos de datos en una determinada dirección, desde un origen hasta un destino. Es un paquete de datos.

MÉTODO DEL PROTOTIPO DE SISTEMAS

La construcción de prototipos representa una estrategia de desarrollo, cuando no es posible determinar todos los requerimientos del usuario. Es por ello que incluye el desarrollo interactivo o en continua evolución, donde el usuario participa de forma directa en el proceso.

Este método contiene condiciones únicas de aplicación, en donde los encargados del desarrollo tienen poca experiencia o información, o donde los costos y riesgos de que se cometa un error pueden ser altos.

Así mismo este método resulta útil para probar la facilidad del sistema e identificar los requerimientos del usuario, evaluar el diseño de un sistema o examinar el uso de una aplicación. El método del prototipo de sistemas consta de 5 etapas:

1). Identificación de requerimientos conocidos: La determinación de los requerimientos de una aplicación es tan importante para el desarrollo de prototipos como lo es para el ciclo de desarrollo de sistemas o análisis estructurado. Por consiguiente, antes de crear un prototipo, los analistas y usuario deben de trabajar juntos para identificar los requerimientos conocidos que tienen que satisfacer.

2). Desarrollo de un modelo de trabajo: Es fácil comenzar el proceso de construcción del prototipo con el desarrollo de un plan general que permita a los usuarios conocer lo que se espera de ellas y del proceso de desarrollo. Un cronograma para el inicio y el fin de la primera interacción es de gran ayuda. En el desarrollo del prototipo se preparan los siguientes componentes:

- El lenguaje para el diálogo o conversación entre el usuario y el sistema.
- Pantallas y formatos para la entrada de datos.
- Módulos esenciales de procesamiento.
- Salida del sistema

3). Utilización del prototipo: Es responsabilidad del usuario trabajar con el prototipo y evaluar sus características y operación. La experiencia del sistema bajo condiciones reales permite obtener la familiaridad indispensable para determinar los cambios o mejoras que sean necesarios, así como las características inadecuadas

4). Revisión del prototipo: Durante la evaluación los analistas de sistemas desean capturar información sobre los que les gusta y lo que les desagrada a los usuarios.

Los cambios al prototipo son planificados con los usuarios antes de llevarlos a cabo, sin embargo es el analista responsable de tales modificaciones.

5). Repetición del proceso las veces que sean necesarias: El proceso antes descrito se repite varias veces, el proceso finaliza cuando los usuarios y analistas están de acuerdo en que el sistema ha evolucionado lo suficiente como para incluir todas las características necesarias.

2.4. Tipos de implementación de sistemas

Existen diferentes tipos de implementar un Sistema de Información, entre los más importantes tenemos:

1. Sistemas de Paralelos
2. Conversión Directa

3. Enfoque Piloto
4. Por etapas

1. - Sistemas de Paralelos.- Es cuando el sistema anterior se opera junto con el sistema nuevo.

Ventaja: Se puede recurrir al sistema anterior si se hallan errores en el nuevo o si ocurren problemas en el uso.

Desventaja: Duplica los costos de operación.

2.- Conversión Directa.- El sistema anterior se reemplaza por el nuevo. La organización confía completamente en el nuevo sistema.

Ventaja: Hay beneficios inmediatos de los nuevos controles. Obliga a los usuarios a que hagan trabajar el nuevo sistema.

Desventaja: No hay otro sistema al cual recurrir si surgen dificultades con el nuevo sistema. Requiere de la más cuidadosa planeación.

3.- Enfoque Piloto.- Se implanta una versión de trabajo del sistema en una parte de la organización. Con base en la retroalimentación, se hacen

cambios y el sistema se instala en el resto de la organización mediante uno de los demás tipos de implementación.

Ventaja: Proporciona experiencia y prueba directa antes de la implantación.

Desventaja: Puede dar la impresión de que el nuevo sistema no es confiable, ni está libre de errores.

4.- Por etapas.- Se implanta el sistema de manera gradual a todos los usuarios.

Ventaja: Permite a los primeros usuarios aprovechar las ventajas del sistema. Permite la capacitación y la instalación sin uso innecesario de recursos.

Desventaja: Un largo período de instalación provoca la deuda en el usuario de si el proyecto marcha bien (demasiado entusiasmo) o mal (resistencia y falta de un juicio justo) .

IMPLEMENTACIÓN Y EVALUACIÓN DE UN NUEVO SISTEMA

REVISIÓN DEL SISTEMA

La revisión de los sistemas tiene la finalidad de detectar su comportamiento y consistencia mediante la aplicación de técnicas adecuadas, que permitan observar si el sistema se está ajustando a las necesidades.

Mediante la revisión de los sistemas se implica el proceso de medir y verificar principios para determinar si el plan, la política y el sistema son los mejores.

Con las revisiones al sistema implantado se determinarán los puntos de posible peligro, si se ha dado cumplimiento o no a los procedimientos instalados últimamente o a los que ya tienen cierta antigüedad, y si su consistencia se mantiene o no.

El analista detectará las deficiencias y errores que se deben corregir, y que pueden ser los siguientes:

1. Desviación del sistema implantado.
2. Aumento de operaciones de la empresa.
3. Cambio de políticas que afecten directa o indirectamente el sistema.
4. Discrepancia en las operaciones.

5. Cambio de condiciones en las que se ejecutaba o realizaba el sistema.

Para comprender mejor estas deficiencias, se explicará brevemente a que se refiere cada una de ellas:

1.- Desviación del sistema implantado

El sistema puede haberse desvirtuado o salido de los lineamientos en que fue fijado. A los primeros indicios, se deberá efectuar la revisión para fijar los controles necesarios que lo devuelvan a su curso normal.

2.- Aumento de operaciones en la empresa

El crecimiento de las operaciones trae ajustes a los sistemas, o bien un nuevo diseño, por lo que también deberá efectuarse una revisión que proponga mejoras o sistemas que realicen con fluidez y con beneficios las operaciones.

3.- Cambio de políticas que afecten directa o indirectamente

Cuando hay cambios de políticas que hacen la operación diferente respecto a como se manejaba anteriormente, y esto afecta a los sistemas y procedimientos, es sumamente indispensable efectuar una revisión que restablezca el control.

4.- Discrepancia en las operaciones

Cuando hay dificultad en las operaciones que se llevan, o duplicidad de funciones en una misma operación, es conveniente efectuar la revisión que detectó las fallas con exactitud.

5.- Cambio de condiciones en las que se ejecutaba o realizaba el sistema

Cuando ha variado la índole o naturaleza del sistema, se debe efectuar una revisión que marque el nuevo sistema, o las modificaciones para ajustarse a las nuevas condiciones del trabajo

Razones para Implementar Sistemas de Información

Las aplicaciones de sistemas de información tienen su origen en casi todas las áreas de una empresa y están relacionadas con todos los problemas de la organización.

Para alcanzar los objetivos, las empresas emprenden proyectos de desarrollo de sistemas de Información por una o más de las siguientes razones:

Las 5 letras "C":

Capacidad

- Mayor velocidad de Procesamiento.
- Incremento en el Volumen.
- Recuperación más rápida de la información.

Control

- Mayor exactitud y mejora en consistencia.

Comunicación:

- Mejora en la comunicación.

- Integración de áreas de la Empresa.

Costos

- Monitoreo de costos.
- Reducción de costos.

Competitividad

- Atraer clientes.
- Dejar fuera a la competencia.
- Mejores acuerdos con los proveedores.
- Desarrollo de nuevos productos.

2.5. Controles de implementación

Los controles de implementación son factores frecuentes claves de éxito para la operación de un nuevo sistema, entre los elementos más importantes que hay que considerar tenemos:

- Procedimientos de emergencia que describan las acciones a emprender una vez ocurrido un incidente que ponga en peligro las operaciones de la empresa.

- Procedimientos de emergencia (fallback) que describan las acciones a emprender para el traslado de actividades esenciales de la empresa o de servicios de soporte a ubicaciones transitorias alternativas.

- Procedimientos de recuperación que describan las acciones a emprender para establecer las operaciones normales de la empresa.

- Un cronograma de mantenimiento que especifique cómo y cuándo será probado el plan, y el proceso para el mantenimiento del mismo.

- Actividades de concientización e instrucción que estén diseñadas para propiciar la comprensión de los procesos de continuidad del negocio y garantizar que los procesos sigan siendo eficaces.

- Las responsabilidades de las personas, describiendo los responsables de la ejecución de cada uno de los componentes del plan.

- Cada plan debe tener un propietario específico.

- Pruebas de discusión de diversos escenarios (discutiendo medidas para la recuperación del negocio utilizando ejemplo de interrupciones)

- Simulaciones (especialmente para entrenar al personal en el desempeño de sus roles de gestión posterior a incidentes o crisis)

- Pruebas de recuperación técnica (garantizando que los sistemas de información puedan ser restablecidos con eficacia)

- Pruebas de recuperación en un sitio alternativo (ejecutando procesos de negocio en paralelo, con operaciones de recuperación fuera del sitio principal)

- Pruebas de instalaciones y servicios de proveedores (garantizando que los productos y servicios de proveedores externos cumplan con el compromiso contraído)

- Ensayos completos (probando que la organización, el personal, el equipamiento, las instalaciones y los procesos pueden afrontar interrupciones

2.6. Definiciones conceptuales

- Análisis y Diseño de Sistemas de Información: (James A. Senn) Conjunto de datos que dentro de contexto significativo y útil, ésta se comunica a un receptor, quien la utiliza para tomar decisiones.

- Administradores: son los que tienen que ver con la asignación de recursos al proyecto y su supervisión. Suelen conformar un comité directivo que velará por que el proyecto se desarrolle dentro de los márgenes y los requerimientos establecidos en la documentación aprobada.

- Analista de Sistemas: Es el papel o rol que jugará usted. Es responsable de determinar y especificar los requerimientos del sistema a construir desde los usuarios.

- Comunicación. Es el proceso mediante el cual un conjunto de signos y/o señales salen y llegan desde un emisor a un receptor.

- Datos: Es un conjunto de señales o signos con un significado particular. Diccionario de datos: descripción de todos los datos usados en el sistema. Puede ser manual o automatizado.

- Descripciones de procesos y procedimientos: declaraciones formales que usan técnicas y lenguajes que permiten a los analistas describir actividades importantes que forman parte del sistema.

- Diseño Estructurado: El diseño Estructurado es otro elemento del Método de Desarrollo por Análisis Estructurado que emplea la descripción gráfica, se enfoca en el desarrollo de especificaciones del software.

- Diseño de Sistemas de Información (Burch-Grudnitski:) La información la componen datos que se han colocado en un contexto significativo y útil y se ha comunicado a un receptor, quien la utiliza para tomar decisiones

- Diseñador de sistemas: es el responsable de especificar las características de la arquitectura del sistema y que servirá de base para el trabajo de los programadores. En muchos casos, el analista y el diseñador son la misma persona.

- Información. La información la componen datos que se han colocado en un contexto significativo y útil y se ha comunicado a un receptor, quien la utiliza para tomar decisiones.

- Información.- Datos procesados por un receptor para quien tienen sentido, y que le da el valor de información.

- Programador: es la persona responsable de pasar a un lenguaje de programación de aplicaciones las características de diseño del sistema especificadas por el diseñador. A menudo es el que descubre errores y ambigüedades en la propuesta de requerimientos entregada por el analista.

- Reglas: estándares para describir y documentar el sistema en forma correcta y completa.

- Símbolos gráficos: Íconos y convenciones para identificar y describir los componentes de un sistema junto con las relaciones entre estos componentes.

- Sistema.- Conjunto de entidades u objetos relacionados entre si, conformando una estructura, y que tienen un fin común.

- Sistemas de Información.- Sistema manual, automatizado o mixto que procesa datos de entrada y entrega información de salida de interés para los usuarios.

- Sistemas On-Line: aquel que acepta datos de entrada directamente del área donde se crea. También es el sistema en el que la información de salida se devuelve directamente a donde es requerida.

- Sistemas de Soporte a las Decisiones (DSS): son sistemas que ayudan a los funcionarios y ejecutivos de las organizaciones a tomar decisiones inteligentes y documentadas acerca de los diversos aspectos críticos de gran impacto sobre los objetivos de la organización. Su característica principal es la recuperación y exhibición de datos consolidados en diversas formas (reportes en tablas y/o gráficos), posibilitando una variedad de análisis de datos, ya sea matemático o estadístico.

- Sistemas basados en el Conocimiento: contienen grandes cantidades de diversos conocimientos que se emplean en el desempeño de una tarea

dada. Los sistemas expertos son una especie de sistema basado en el conocimiento, aunque ambos términos a menudo se utilizan indistintamente. Los sistemas expertos se construyen de tal manera que sean capaces de explicar las líneas de razonamiento que llevan a los responsables a tomar las decisiones.

- Usuarios: Son aquellos que utilizan y se benefician directamente del sistema o para quienes se construye el sistema. Usuario es la persona a la que se tendrá que entrevistar, a menudo con gran detalle, a fin de conocer sus requerimientos para el nuevo sistema. También se les suele denominar clientes internos.

CAPÍTULO III

3.0 FUNDAMENTACIÓN NORMATIVA Y/O ESTÁNDARES INTERNACIONALES

3.1. Fundamentación Normativa

3.1.1. Normas de control interno COSO

ANTECEDENTES

Algunos grupos de interés de países como: Canadá, Estados Unidos, Reino Unido, Francia, Nueva Zelanda entre otros integraron la (Comisión Treadway), quienes realizaron muchos esfuerzos para definir formalmente el Modelo de Control Interno COSO, que contiene objetivos y elementos del control interno, así mismo establecieron los roles de todos los interesados incluyendo la Junta Directiva, los directivos, los jefes de mandos medios, los supervisores y empleados.

DEFINICIÓN Y OBJETIVOS

El Control Interno es un proceso integrado a los procesos, y no un conjunto de pesados mecanismos burocráticos añadidos a los mismos, efectuado por

el consejo de la administración, la dirección y el resto del personal de una entidad, diseñado con el objeto de proporcionar una garantía razonable para el logro de objetivos incluidos en las siguientes categorías:

- Eficacia y eficiencia de las operaciones.
- Confiabilidad de la información financiera.
- Cumplimiento de las leyes, reglamentos y políticas.
- Completan la definición algunos conceptos fundamentales:
- Lo llevan a cabo las personas que actúan en todos los niveles, no se trata solamente de manuales de organización y procedimientos.
- Sólo puede aportar un grado de seguridad razonable, no la seguridad total, a la conducción.

COMPONENTES

El marco integrado de control que plantea el informe COSO consta de cinco componentes interrelacionados, derivados del estilo de la dirección, e integrados al proceso de gestión:

- Ambiente de control
- Evaluación de riesgos
- Actividades de control
- Información y comunicación

- Supervisión

AMBIENTE DE CONTROL

El ambiente de control define al conjunto de circunstancias que enmarcan el accionar de una entidad desde la perspectiva del control interno y que son por lo tanto determinantes del grado en que los principios de este último imperan sobre las conductas y los procedimientos organizacionales.

Los principales factores del ambiente de control son:

- La filosofía y estilo de la dirección y la gerencia.
- La estructura, el plan organizacional, los reglamentos y los manuales de procedimiento.
- La integridad, los valores éticos, la competencia profesional y el compromiso de todos los componentes de la organización, así como su adhesión a las políticas y objetivos establecidos.

EVALUACIÓN DE RIESGOS

El control interno ha sido pensado esencialmente para limitar los riesgos que afectan las actividades de las organizaciones. A través de la investigación y análisis de los riesgos relevantes y el punto hasta el cual el control vigente los neutraliza se evalúa la vulnerabilidad del sistema. Para ello debe adquirirse un conocimiento práctico de la entidad y sus componentes de manera de identificar los puntos débiles, enfocando los riesgos tanto a los niveles internos y externos de la como de la actividad.

El análisis de los riesgos incluirá:

- Una estimación de su importancia / trascendencia.
- Una evaluación de la probabilidad / frecuencia.
- Una definición del modo en que habrán de manejarse.

ACTIVIDADES DE CONTROL

Las actividades de control se ejecutan en todos los niveles de la organización y en cada una de las etapas de la gestión, partiendo de la elaboración de un mapa de riesgos según lo expresado en el punto anterior: conociendo los riesgos, se disponen los controles destinados a evitarlos o

minimizarlos, los cuales pueden agruparse en tres categorías, según el objetivo de la entidad con el que estén relacionados:

- Las operaciones
- La confiabilidad de la información financiera
- El cumplimiento de leyes y reglamentos

A su vez en cada categoría existen diversos tipos de control:

- Preventivo / Correctivos
- Manuales / Automatizados o informáticos
- Gerenciales

En todos los niveles de la organización existen responsabilidades de control, y es preciso que los agentes conozcan individualmente cuales son las que les competen, debiéndose para ello explicitar claramente tales funciones.

INFORMACIÓN Y COMUNICACIÓN

La información relevante debe ser captada, procesada y transmitida de tal modo que llegue oportunamente a todos los sectores permitiendo asumir las responsabilidades individuales.

La información operacional, financiera y de cumplimiento conforma un sistema para posibilitar la dirección, ejecución y control de las operaciones.

La comunicación es inherente a los sistemas de información. Las personas deben conocer a tiempo las cuestiones relativas a sus responsabilidades de gestión y control. Cada función ha de especificarse con claridad, entendiendo en ello los aspectos relativos a la responsabilidad de los individuos dentro del sistema de control interno.

Los informes deben transferirse adecuadamente a través de una comunicación eficaz. Esto es, en el más amplio sentido, incluyendo una circulación multidireccional de la información: ascendente, descendente y transversal.

La existencia de líneas abiertas de comunicación y una clara voluntad de escuchar por parte de los directivos resultan vitales.

SUPERVISIÓN

El objetivo es asegurar que el control interno funciona adecuadamente, a través de dos modalidades de supervisión: actividades continuas o evaluaciones puntuales.

Las primeras son aquellas incorporadas a las actividades normales y recurrentes que, ejecutándose en tiempo real y arraigadas a la gestión, generan respuestas dinámicas a las circunstancias sobrevinientes.

En cuanto a las evaluaciones puntuales, corresponden las siguientes consideraciones:

a) Su alcance y frecuencia están determinados por la naturaleza e importancia de los cambios y riesgos que éstos conllevan, la competencia y experiencia de quienes aplican los controles, y los resultados de la supervisión continuada.

b) Son ejecutados por los propios responsables de las áreas de gestión (auto evaluación), la auditoría interna (incluidas en el planeamiento o solicitadas especialmente por la dirección), y los auditores externos.

c) Constituyen en sí todo un proceso dentro del cual, aunque los enfoques y técnicas varíen, priman una disciplina apropiada y principios insoslayables.

La tarea del evaluador es averiguar el funcionamiento real del sistema: que los controles existan y estén formalizados, que se apliquen cotidianamente como una rutina incorporada a los hábitos, y que resulten aptos para los fines perseguidos.

d) Responden a una determinada metodología, con técnicas y herramientas para medir la eficacia directamente o a través de la comparación con otros sistemas de control probadamente buenos.

Las deficiencias o debilidades del sistema de control interno detectadas a través de los diferentes procedimientos de supervisión deben ser comunicadas a efectos de que se adopten las medidas de ajuste correspondientes.

Según el impacto de las deficiencias, los destinatarios de la información pueden ser tanto las personas responsables de la función o actividad implicada como las autoridades superiores.

3.1.2.Normas de control interno SAC

El informe de la SAC define el sistema de mando interior, describe sus componentes, proporciona varias clasificaciones de mandos, describe objetivos del mando y riesgos, y define el papel del auditor interno. El informe proporciona la guía en usar, manejando, y protegiendo los recursos de tecnología de información.

La definición: El informe de SAC define un sistema de mando interior como: un juego de procesos, funciones, actividades, subsistemas, y las personas que se agrupan para asegurar el logro eficaz de los objetivos y metas.

El informe da énfasis al papel e impacto de sistemas de información informatizado en el sistema de mandos interiores. Enfatiza la necesidad de evaluar los riesgos, establecer los costos y beneficios, y para construir los mandos en el sistema en lugar de agregarlos después de la aplicación.

Los componentes: El sistema de mando interior consiste en tres componentes:

- el ambiente del mando,
- el manual y sistema automatizado, y
- procedimientos del mando.

El ambiente del mando incluye la estructura de la organización, armazón del mando, las políticas y procedimientos, y las influencias externas. Los sistemas automatizados consisten en los sistemas y la aplicación del software.

Las clasificaciones: La SAC proporciona una clasificación de cinco planes para los controles internos en el sistema de información:

- preventivo, detectivo, y correctivo,
- discrecional,

- voluntario y obligatorio,
- el manual automatizado, y
- la aplicación y los controles generales.

Estos planes se ponen en marcha cuando los controles son aplicados, y si estos controles no son aplicados se realizan las siguientes preguntas, quién impone la necesidad por el control, cómo el control se lleva a cabo, y donde en el software el control es implementado.

Objetivos de Control y Riesgos: Los riesgos incluyen el fraude, errores, interrupciones en los negocios, y el uso ineficaz de recursos. Los objetivos de control reducen estos riesgos y aseguran integridad de la información. La integridad de información es resguardada en la entrada, proceso, rendimiento, y controles de calidad del software. Las medidas de Seguridad incluyen datos, y controles de seguridad de programa. Los controles de complacencia aseguran la conformidad con las leyes y regulaciones, la contabilidad y estándares en la auditoría, políticas interiores y procedimientos.

3.2 Estándares Internacionales

3.2.1 Estándar de Control de Sistemas COBIT

Antecedentes

COBIT se fundamenta en los Objetivos de Control existentes de la Information Systems Audit and Control Foundation (ISACF), mejorados a partir de estándares internacionales técnicos, profesionales, regulatorios y específicos para la industria, tanto existentes como en surgimiento.

Se determinó que las mejoras a los objetivos de control originales debería consistir en:

- El desarrollo de un marco referencial para control en TI como fundamento para los objetivos de control en TI y como una guía para la investigación consistente en auditoría y control de TI;
- Una alineación del marco referencial general y de los objetivos de control individuales, con estándares y regulaciones internacionales existentes de hecho y de derecho.

Generalidades

COBIT es una herramienta para la administración y operación a un nivel superior a los estándares de tecnología para la administración de sistemas de información.

El objetivo principal de COBIT es el desarrollo de políticas claras y buenas prácticas para la seguridad y el control de Tecnología de Información, con el fin de obtener la aprobación y el apoyo de las entidades comerciales, gubernamentales y profesionales en todo el mundo.

Dominios y Procedimientos de Control COBIT

- **Planeación y Organización**

Este dominio cubre la estrategia y las tácticas y se refiere a la identificación de la forma en que la tecnología de información puede contribuir de la mejor manera al logro de los objetivos del negocio. Además, la consecución de la visión estratégica necesita ser planeada, comunicada y administrada desde diferentes perspectivas. Finalmente, deberán establecerse una organización y una infraestructura tecnológica apropiadas.

- **Adquisición e Implementación**

Para llevar a cabo la estrategia de TI, las soluciones de TI deben ser identificadas, desarrolladas o adquiridas, así como implementadas e integradas dentro del proceso del negocio. Además, este dominio cubre los cambios y el mantenimiento realizados a sistemas existentes.

- **Entrega y Soporte**

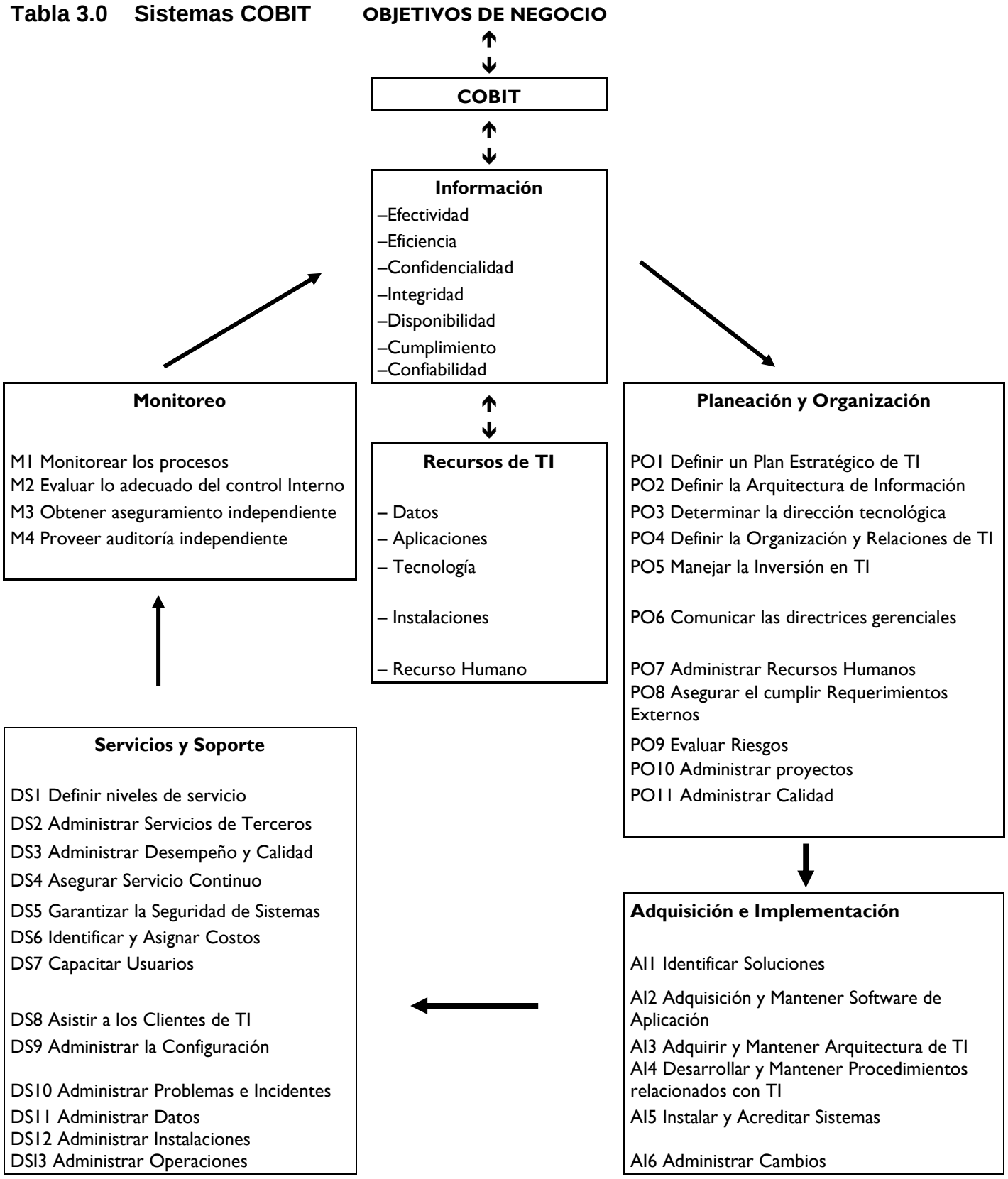
En este dominio se hace referencia a la entrega de los servicios requeridos, que abarca desde las operaciones tradicionales hasta el entrenamiento, pasando por seguridad y aspectos de continuidad. Con el fin de proveer servicios, deberán establecerse los procesos de soporte necesarios. Este dominio incluye el procesamiento de los datos por sistemas de aplicación, frecuentemente clasificados como controles de aplicación.

- **Monitoreo**

Todos los procesos necesitan ser evaluados regularmente a través del tiempo para verificar su calidad y suficiencia en cuanto a los requerimientos de control.

Para obtener una comprensión de los procesos que integran el estándar COBIT describo una tabla condensada a continuación:

Tabla 3.0 Sistemas COBIT



Definiciones

- **Control**.- Son políticas, procedimientos, prácticas y estructuras organizacionales diseñadas para garantizar razonablemente que los objetivos del negocio serán alcanzados y que eventos no deseables serán prevenidos o detectados y corregidos.

- **Objetivo de control**.- se define como el resultado o propósito que se desea alcanzar implementando procedimientos de control en una actividad del Sistema de Información.

- **Efectividad.-** Se refiere a que la información relevante sea pertinente para el proceso del negocio, así como a que su entrega sea oportuna, correcta, consistente y de manera utilizable.

- **Eficiencia.-** Se refiere a la provisión de información a través de la utilización óptima de recursos.

- **Confidencialidad.-** Se refiere a la protección de información sensible contra divulgación no autorizada.

- **Integridad**.- Se refiere a la precisión y suficiencia de la información, así como a su validez de acuerdo con los valores y expectativas del negocio.

3.2.2. ISO 17799

La ISO (International Organization for Standardization) es la entidad internacional encargada de favorecer la normalización en el mundo. La finalidad principal de las normas ISO es orientar, coordinar, simplificar y unificar los usos para conseguir menores costos y efectividad.

Este estándar internacional de alto nivel para la administración de la seguridad de la información, fue publicado por la ISO (International Organization for Standardization) en diciembre de 2000 con el objeto de desarrollar un marco de seguridad sobre el cual trabajen las organizaciones.

El ISO 17799, se orienta a preservar los siguientes principios de la seguridad informática:

- **Confidencialidad**.- Asegurar que únicamente personal autorizado tenga acceso a la información.

- **Integridad**.- Garantizar que la información no será alterada, eliminada o destruida por entidades no autorizadas.
- **Disponibilidad**.- Asegurar que los usuarios autorizados tendrán acceso a la información cuando la requieran.

El objetivo de la seguridad de los datos es asegurar la continuidad de las operaciones de la organización, reducir al mínimo los daños causados por una contingencia, así como optimizar la inversión en tecnologías de seguridad.

El objetivo principal de la ISO 17799 es proporcionar un conjunto de normas comunes de seguridad de información reconocidas globalmente, y ser una práctica eficaz de la gestión de la seguridad capaz de someterse a auditorías independientes.

Estructura

La norma ISO 17799:2002 establece diez dominios de control que cubren todos los aspectos fundamentales aplicables a la seguridad en el manejo de la información:

- Política de seguridad
- Aspectos organizativos para la seguridad
- Clasificación y control de activos

- Seguridad ligada al personal
- Seguridad física y del entorno
- Gestión de comunicaciones y operaciones
- Control de accesos
- Desarrollo y mantenimiento de sistemas
- Administración de la continuidad del negocio
- Conformidad con la legislación

Figura 3.0. Dominios de control ISO 17799

Objetivos de control en ISO 17799

Aspectos organizativos para la seguridad

Dentro de los aspectos organizativos podemos encontrar aspectos referentes a la infraestructura de seguridad de la información, seguridad

frente al acceso de terceros y la tercerización. Se profundizará en el segundo punto, cuyo objetivo es mantener la seguridad de las instalaciones de procesamiento de información y de los recursos de información de la organización a los que acceden terceras partes.

Seguridad del personal

La norma considera dentro de la seguridad del personal, la respuesta a incidentes y anomalías, en este caso se ampliará el tema sobre la comunicación de anomalías del software.

Comunicación de anomalías del software

Se deben considerar las siguientes acciones:

a) Deben advertirse y registrarse los síntomas del problema y los mensajes que aparecen en pantalla.
b) La computadora debe ser aislada, si es posible, y debe detenerse el uso de la misma. Se debe alertar de inmediato a la persona pertinente (contacto). Si se ha de examinar el equipo, éste debe ser desconectado de las redes de la organización antes de ser activado nuevamente. Los disquetes no deben transferirse a otras computadoras.
c) El asunto debe ser comunicado inmediatamente al gerente de seguridad de la información.

Los usuarios no deben quitar el software que supuestamente tiene una anomalía, a menos que estén autorizados a hacerlo. La recuperación debe ser realizada por personal adecuadamente capacitado y experimentado.

Controles de acceso físico

Las áreas protegidas deben ser resguardadas por adecuados controles de acceso que permitan garantizar que sólo se permite el acceso de personal autorizado. Deben tenerse en cuenta los siguientes controles:

a) Los visitantes de áreas protegidas deben ser supervisados o inspeccionados y la fecha y horario de su ingreso y egreso deben ser registrados. Sólo se debe permitir el acceso a los mismos con propósitos específicos y autorizados, instruyéndose en dicho momento al visitante sobre los requerimientos de seguridad del área y los procedimientos de emergencia.

b) El acceso a la información sensible, y a las instalaciones de procesamiento de información, debe ser controlado y limitado exclusivamente a las personas autorizadas. Se deben utilizar controles de autenticación, por ej. Tarjeta y número de identificación personal (PIN), para autorizar y validar todos los accesos. Debe mantenerse una pista protegida que permita auditar todos los accesos.

c) Se debe requerir que todo el personal exhiba alguna forma de identificación visible y se lo debe alentar a cuestionar la presencia de desconocidos no escoltados y a cualquier persona que no exhiba una identificación visible.
d) Se deben revisar y actualizar periódicamente los derechos de acceso a las áreas protegidas.

Gestión de comunicaciones y operaciones

Tiene como objetivo garantizar el funcionamiento correcto y seguro de las instalaciones de procesamiento de información. Para el caso de estudio, se explicará sobre la planificación y aprobación del sistema.

Se deben establecer criterios de aprobación para nuevos sistemas de información, actualizaciones y nuevas versiones, y se deben llevar a cabo adecuadas pruebas de los sistemas antes de su aprobación. Los gerentes deben garantizar que los requerimientos y criterios de aprobación de nuevos sistemas sean claramente definidos, acordados, documentados y probados. Se deben considerar los siguientes puntos:

a) desempeño y requerimientos de capacidad de las computadoras;
b) recuperación ante errores y procedimientos de reinicio, y planes de contingencia;
c) preparación y prueba de procedimientos operativos de rutina según estándares definidos

d) conjunto acordado de controles de seguridad implementados
e) procedimientos manuales eficaces;
f) disposiciones relativas a la continuidad de los negocios,
g) evidencia que la instalación del nuevo sistema no afectará negativamente los sistemas existentes, especialmente en los períodos pico de procesamiento, como durante los últimos días del mes
h) evidencia de que se ha tomado en cuenta el efecto que tiene el nuevo sistema en la seguridad global de la organización
i) entrenamiento en la operación o uso de nuevos sistemas.

Para los principales nuevos desarrollos, las funciones y usuarios de operaciones deben ser consultados en todas las etapas del proceso de desarrollo para garantizar la eficiencia operativa del diseño propuesto del sistema. Deben llevarse a cabo pruebas apropiadas para constatar el cumplimiento cabal de todos los criterios de aprobación.

CAPÍTULO IV

4.0 MANUAL DE CONTROLES DE IMPLEMENTACION DE SISTEMAS

4.1. INFORMACIÓN PRELIMINAR

4.1.1. INTRODUCCIÓN

La elaboración de un manual en el cual se establezcan los controles de implementación de los sistemas de información, es muy necesario en las empresas modernas y competitivas ya que mediante la utilización del mismo los gerentes e implementadores podrán tener una idea clara de cómo se debe instalar y dejar en funcionamiento del sistema, tomando en cuenta los controles que se requieren para salvaguardar la información de dicho sistema.

4.1. INFORMACIÓN PRELIMINAR

4.1.2 OBJETIVOS

- Establecer los controles preventivos, detectivos y correctivos mínimos que se deben aplicar en la implementación de Sistemas de Información.
- Ayudar a incrementar la efectividad de los Sistemas de Información en la operación de la empresa mediante el establecimiento de controles.
- Reducir o eliminar los riesgos a los que está expuesta la información del sistema mediante la correcta utilización de controles.

4.1. INFORMACIÓN PRELIMINAR

4.1.3. ALCANCE

Este Manual debe ser usado exclusivamente por todo el personal que labora en el Departamento de Sistemas, sea éste personal interno o externo con la finalidad de brindar un grado de seguridad razonable a los dueños de procesos y a toda la organización.

4.1. INFORMACIÓN PRELIMINAR

4.1.4. RESPONSABILIDADES

- **Alta Gerencia.-** Deberá dar apoyo a todo proyecto de implantación del sistema de información.
- **Gerencia de Nivel Medio.-** Deberá velar por el cumplimiento de los controles que se detallan en el manual de implementación.
- **Implementadores.-** Deberá aplicar todos los controles que se detallan en esta manual.

4.1. INFORMACIÓN PRELIMINAR

4.1.5. DEFINICIONES BÁSICAS

Análisis de riesgos

Uso sistemático de la información para identificar fuentes y estimar el riesgo.

Confidencialidad

Acceso a la información por parte únicamente de quienes estén autorizados.

Control

Las políticas, los procedimientos, las prácticas y las estructuras organizativas concebidas para brindar una garantía razonable o suficiente de que se lograrán los objetivos de negocio detendrán o corregirán.

Control detectivo

Control que detecta la aparición de un riesgo, error, omisión o acto deliberado. Supone que la amenaza ya se ha materializado pero por sí mismo no la corrige.

Control correctivo

Control que corrige un riesgo, error, omisión o acto deliberado antes de que produzca pérdidas. Supone que la amenaza ya se ha materializado pero que se corrige.

4.1. INFORMACIÓN PRELIMINAR

4.1.5. DEFINICIONES BÁSICAS

Control preventivo

Control que evita que se produzca un riesgo, error, omisión o acto deliberado. Impide que una amenaza llegue siquiera a materializarse.

.

Desastre

Cualquier evento accidental, natural o malintencionado que representa una amenaza, para o interrumpe las operaciones o servicios habituales durante el tiempo suficiente para afectar de manera significativa a la organización o causar un fallo en la misma.

Disponibilidad

Acceso a la información y los sistemas de tratamiento de la misma por parte de los usuarios autorizados cuando lo requieran.

Evaluación de riesgos

Proceso de comparación de los riesgos estimados con unos criterios dados de riesgo para determinar la importancia del riesgo.

Objetivo

Declaración del resultado o fin que se desea lograr mediante la implementación de procedimientos de control en una actividad de TI determinada.

4.1. INFORMACIÓN PRELIMINAR

4.1.5. DEFINICIONES BÁSICAS

Política de seguridad

Documento que establece el compromiso de la Dirección y el enfoque de la organización en la gestión de la seguridad de la información.

Riesgo

Posibilidad de que una amenaza concreta pueda explotar una vulnerabilidad para causar una pérdida o daño en un activo de información.

Seguridad de la información

Preservación de la confidencialidad, integridad y disponibilidad de la información y los sistemas de tratamiento de la misma.

4.1. INFORMACIÓN PRELIMINAR

4.1.6. ETAPAS DE LA IMPLEMENTACIÓN

Para implementar un Sistemas de Información existen varias etapas que deben realizarse.

Entre las etapas más importantes tenemos:

1. Capacitación
2. Conversión de datos
3. Plan de implementación y pruebas de aceptación
4. Revisión post-implementación

4.1. INFORMACIÓN PRELIMINAR

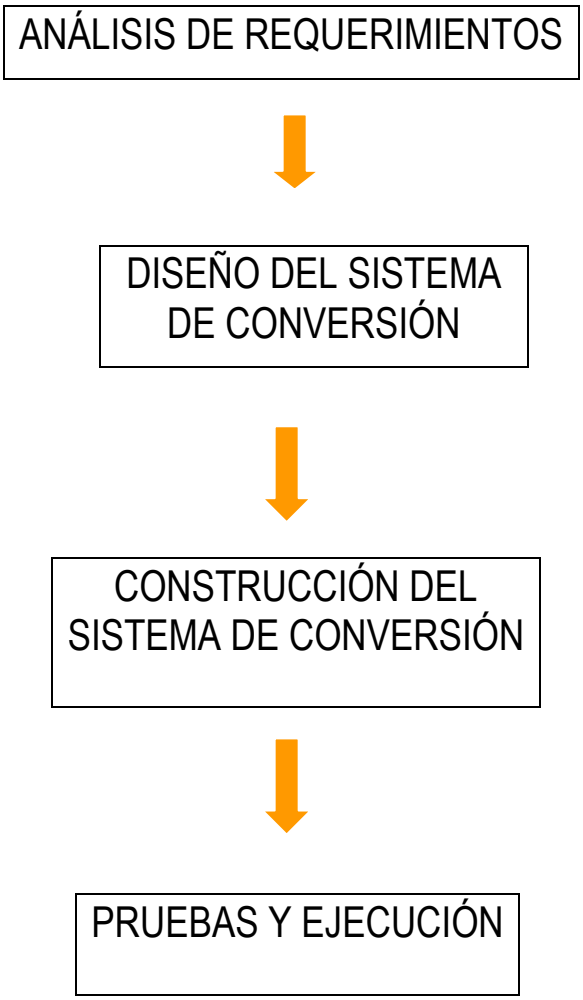
4.1.6. ETAPAS DE LA IMPLEMENTACIÓN

Capacitación:

4.1. INFORMACIÓN PRELIMINAR

4.1.6. ETAPAS DE LA IMPLEMENTACIÓN

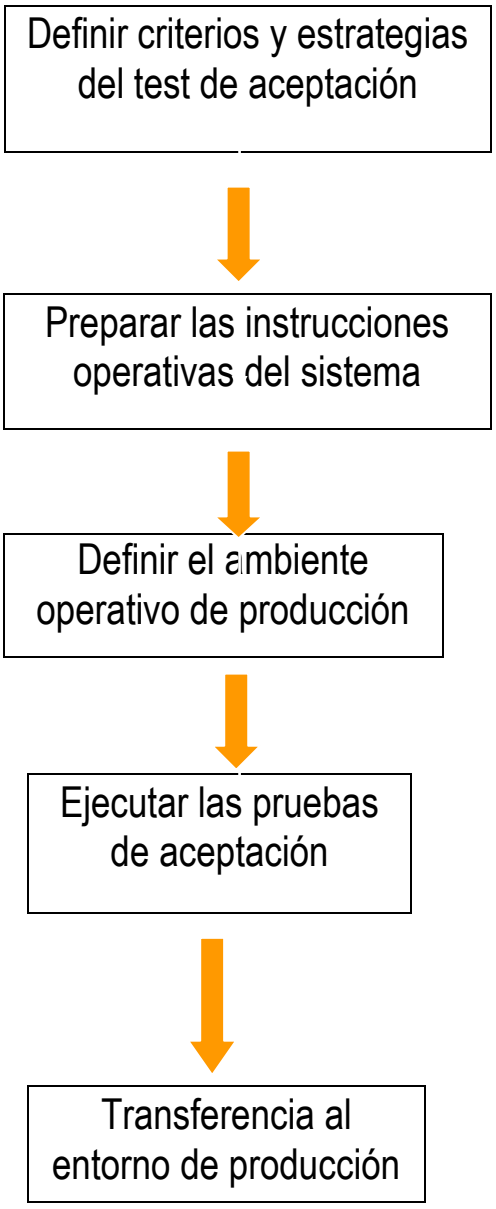
Conversión de Datos:



4.1. INFORMACIÓN PRELIMINAR

4.1.6. ETAPAS DE LA IMPLEMENTACIÓN

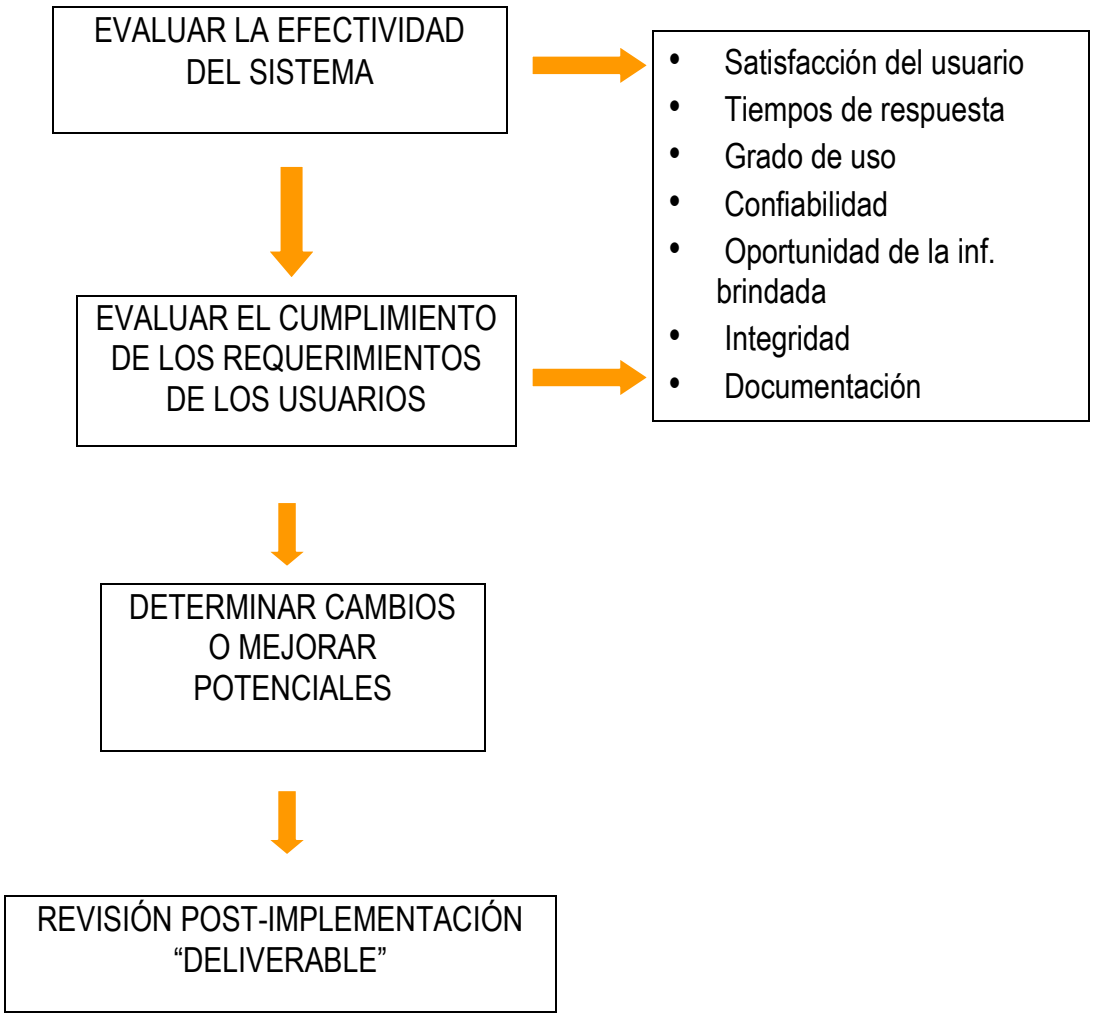
Implantación / Pruebas de Aceptación:



4.1. INFORMACIÓN PRELIMINAR

4.1.6. ETAPAS DE LA IMPLEMENTACIÓN

Revisión Post-implementación:



4.2. ANÁLISIS DE RIESGOS

4.2.1. RIESGOS DE LA ORGANIZACIÓN DE LA IMPLEMENTACIÓN

1. Resistencia por el cambio en el patrón de hábitos que les proporciona el sistema antiguo por los hábitos del nuevo sistema.

2. Que los usuarios ejerzan presión y no permitan llevar a la práctica todos los trabajos que con anterioridad se desarrollaron para la implementación.

3, Presencia de eventos o sucesos inesperados que impidan su implementación.

4. Afectación a los sistemas o recursos de la información de una organización, dados por el procesamiento erróneo o ineficiente de la información.

5. Que los usuarios principales o gerentes no tengan el perfil y autoridad necesaria para vencer la resistencia natural al cambio por parte de los usuarios.

6. Que no exista un plan y cronograma de implementación.

4.2. ANÁLISIS DE RIESGOS

4.2.2. RIESGOS ADMINISTRATIVOS

1. Inadecuada definición de puestos.

2. Falta de determinación de la sensibilidad del puesto

3. Inadecuada selección de la persona para cada puesto

4. Falta total o parcial de entrenamiento inicial y continuo del empleado

4.2. ANÁLISIS DE RIESGOS

4.2.3. RIESGOS DE ACCESO

1.- Terceras personas puedan afectar a la confidencialidad, integridad y disponibilidad de la información del sistema al obtener acceso físico - lógico.

2.- Pobre diseño de password o contraseñas de los usuarios que pueda ser vulnerado por hackers, crackers o phreakers.

3.- Los privilegios de acceso no estén relacionados a las responsabilidades propias del trabajo particular de cada uno.

4.- Inadecuado acceso a datos sensibles y confidenciales .

5.- Acceso no autorizado a la Base de Datos y/o archivos.

4.2. ANÁLISIS DE RIESGOS

4.2.4. RIESGOS DE CONVERSIÓN

1. Pocos procesos de limpieza de los datos antes de la conversión, no aseguran que todos los datos a convertir sean precisos, válidos y estén actualizados.

2. Inexistencia de procedimientos de reconciliación y validación de todos los datos.

3. El personal ajeno a la empresa puede acceder a los datos, y cualquier dato que introduzcan puede que no sean sometidos a una validación extraordinaria.

4. Insuficiente planeación para la conversión y migración de datos.

4.2. ANÁLISIS DE RIESGOS

4.2.5. RIESGOS DE PRUEBA

1. Inexistencia de documentación (de los programas, el manual del usuario y el manual de operación) antes de ejecutar una prueba de aceptación

2. Pruebas de aceptación con fallas por parte del usuario con la firma del usuario en el requerimiento del sistema con lo cual califica al sistema como apto para entrar en la etapa de paralelo.

3. Falta de documentación de las pruebas de aceptación debidamente firmada por el usuario.

4.2. ANÁLISIS DE RIESGOS

4.2.6. RIESGOS DE AUDITORÍA

1. Que no se revise toda la documentación que soporta la información del sistema.

2. Que no se evalúen los productos resultantes y entregables de la fase de implementación.

3. Pistas de auditorías incompletas.

4.2. ANÁLISIS DE RIESGOS

4.2.7. RIESGOS DE SEGURIDAD

1. Poco control de todos los accesos a la red corporativa

2. Falta de seguridad en la protección física y lógica de servidores

3. Inactivación de registro de seguridad de las aplicaciones críticas.

4. Inexistencia de personal calificado para realizar estos análisis.

5. No se cuenta con una información adecuada y completa sobre la configuración de la seguridad

4.2. ANÁLISIS DE RIESGOS

4.2.8. RIESGOS EN LA POST-IMPLEMENTACIÓN

1. Errores y omisiones que no son consideradas.

2. Falta total o parcial de mensajes de advertencia / error del sistema.

3. Siniestros, desastres e interrupciones no consideradas en un plan de contingencia.

4. Violación de la privacidad, confidencialidad, integridad y disponibilidad del sistema.

5. Robo de los recursos informáticos del Sistema de Información.

6. Dificultades de recuperación.

7. Manejo inadecuado de errores.

8. Validación de datos deficientes.

4.2. ANÁLISIS DE RIESGOS

4.2.8. RIESGOS EN LA POST-IMPLEMENTACIÓN

9. Acceso no autorizado a la base de datos y/o archivos.

10. Debilidades en las políticas de control de la información.

11. Fraude y desfalco.

12. Falta de balanceo de salidas.

13. Falta de control a los programas de interfase.

14. Caídas de sistema operacional.

15. Debilidad de control al usuario.

16. La aplicación consuma muchos recursos.

17. La aplicación no ofrece un rendimiento óptimo.

4.3. CONTROLES DE IMPLEMENTACIÓN

4.3.1. LA ORGANIZACIÓN DE LA IMPLEMENTACIÓN

CONTROLES DE: LA ORGANIZACIÓN DE LA IMPLEMENTACIÓN
OBJETIVOS DE CONTROL: Realizar la organización de la implementación de sistemas una vez que se haya efectuado satisfactoriamente el diseño, construcción, prueba del mismo y existan las evidencias que respalden dicha acción, así como la autorización del líder del proyecto
POLÍTICAS DE CONTROL: 1. Se debe elaborar un plan estratégico para efectuar la implementación del sistema, describiendo el equipo de trabajo, actividades o tareas a realizar y los tiempos de ejecución. 2. El equipo de trabajo del proyecto encargado del desarrollo del plan estratégico sistema debe ser el responsable de la implementación total del mismo o se debe delegar al equipo implementador que corresponda. 3. El equipo del proyecto deberá elaborar un plan de implementación, que involucre todas las actividades necesarias.

CONTROLES DE: LA ORGANIZACIÓN DE LA IMPLEMENTACIÓN
OBJETIVOS DE CONTROL: Realizar la organización de la implementación de sistemas una vez que se haya efectuado satisfactoriamente el diseño, construcción, prueba del mismo y existan las evidencias que respalden dicha acción, así como la autorización del líder del proyecto
POLÍTICAS DE CONTROL: 4. Se deben establecer estrategias de conversión, migración e implementación del sistema, que incluya la sensibilización y capacitación del usuario con el fin de alcanzar un alto grado de confiabilidad y seguridad de la operación del mismo, 5. Se debe elaborar, documentar, probar, aprobar e implementar un plan de continuidad o un plan alterno en caso de que falla la operatividad o se produzcan errores imprevistos en la ejecución del sistema. 6. Se deben documentar todos los procedimientos de continuidad necesarios para la recuperación de la funcionalidad de los sistemas operacionales.

4.3.2. CONTROLES ADMINISTRATIVOS

4.3.2.1 DEFINICIÓN DE PUESTOS

CONTROLES DE: DEFINICIÓN DE PUESTOS
OBJETIVOS DE CONTROL: Ubicación del personal, según sus capacidades y conocimientos en los departamentos idóneos.
POLÍTICAS DE CONTROL: 1. Se debe elegir la persona adecuada para cada puesto, teniendo en cuenta la experiencia y conocimientos técnicos necesarios para cada cargo. 2. Se debe asignar las responsabilidades en el uso del sistema, la cual debe estar claramente definida, identificada y autenticada. 3. Se debe efectuar una verificación de los antecedentes personales de los candidatos a cada puesto. 4. Debe contemplarse la máxima separación de funciones (separación de deberes) posibles en el puesto del colaborador a ser involucrado como usuario del sistema 5. Se debe definir el otorgamiento del mínimo permiso de acceso requerido por cada puesto para la ejecución de las tareas asignadas en el manejo u operación del sistema.

4.3.2.2 CAPACITACIÓN

CONTROLES DE: CAPACITACIÓN
OBJETIVOS DE CONTROL: Educar a los usuarios mediante capacitación continua, para que conozcan el uso de sistemas de información, creando conciencia institucional respecto a seguridad y buen uso de los Sistemas de Información.
POLÍTICAS DE CONTROL: 1. El personal deberá tener capacitación permanente pudiendo así aumentar sus habilidades técnicas. 2. Evaluar el desempeño del personal regularmente para determinar si cumple o no con los estándares requeridos en la organización. 3. Los empleados deberán ser asesorados sobre su desempeño y en el Sistema de Información cuando sea requerido.

4.3.3. CONTROLES DE ACCESO

CONTROLES DE: ACCESO FÍSICO Y LÓGICO

OBJETIVOS DE CONTROL:

Definir la comunidad de usuarios y los roles de los mismos de acuerdo a sus responsabilidades y tareas.

POLÍTICAS DE CONTROL:

1. Se debe elaborar una lista de todos los usuarios que deben tener acceso al sistema con la declaración de los perfiles de seguridad y opciones de menú debidamente autorizadas por su jefe inmediato.
2. El acceso a las transacciones tiene que estar encaminado a dividir las responsabilidades adecuadamente por eso es importante determinar si el usuario tiene la autorización necesaria que le corresponde para ejecutar una transacción.
3. Es preciso controlar el acceso a las transacciones especialmente sensibles, y el acceso a ellas debe ser el mínimo posible.
4. Los accesos de terceros se otorgan siguiendo las directivas de seguridad de la empresa.

CONTROLES DE: ACCESO FÍSICO Y LÓGICO

OBJETIVOS DE CONTROL:

Definir la comunidad de usuarios y los roles de los mismos de acuerdo a sus responsabilidades y tareas.

POLÍTICAS DE CONTROL:

5. Deben emplearse convenciones de nombres apropiados para todos los usuarios y las autorizaciones acorde a los estándares en la creación de políticas de cuentas y contraseñas.
6. Los visitantes de áreas protegidas deben ser supervisados o inspeccionados y la fecha y horario de su ingreso y egreso deben ser registrados. Sólo se debe permitir el acceso a los mismos con propósitos específicos y autorizados, instruyéndose en dicho momento al visitante sobre los requerimientos de seguridad del área y los procedimientos de emergencia.
7. El acceso a la información sensible, y a las instalaciones de procesamiento de información, debe ser controlado y limitado exclusivamente a las personas autorizadas.

CONTROLES DE: ACCESO FÍSICO Y LÓGICO

OBJETIVOS DE CONTROL:

Definir la comunidad de usuarios y los roles de los mismos de acuerdo a sus responsabilidades y tareas.

POLÍTICAS DE CONTROL:

8. Se deben utilizar controles de autenticación, por ej. Tarjeta y número de identificación personal (PIN), para autorizar y validar todos los accesos.
9. Se debe requerir que todo el personal exhiba alguna forma de identificación visible y se lo debe alentar a cuestionar la presencia de desconocidos no escoltados y a cualquier persona que no exhiba una identificación visible.
10. Se deben revisar y actualizar periódicamente los derechos de acceso a las áreas protegidas.

4.3.4. CONTROLES DE CONVERSIÓN

CONTROLES DE: CONVERSIÓN

OBJETIVOS DE CONTROL:

Se debe realizar un proceso de limpieza de los datos antes de la conversión, para garantizar que todos los datos a convertir sean precisos, válidos y estén actualizados.

POLÍTICAS DE CONTROL:

1. Se debe elaborar un plan de conversión que involucre las estrategias y los recursos informáticos necesarios, el tiempo, los costos, la organización del personal que efectuará la conversión y la asignación de responsabilidades.
2. La gerencia usuaria y de sistemas deben dar el visto bueno o la aprobación respectiva al plan de conversión.
3. Se debe efectuar un análisis detallado de las interdependencias con otros módulos o subsistemas.
4. Se debe desarrollar procesos y procedimientos dependiendo del tipo, cantidad y calidad de los datos convertidos tales como:
    - Proceso de limpieza de los datos antes de la conversión, para garantizar que todos los datos a convertir son precisos, válidos y están actualizados.

CONTROLES DE: CONVERSIÓN

OBJETIVOS DE CONTROL:

Se debe realizar un proceso de limpieza de los datos antes de la conversión, para garantizar que todos los datos a convertir sean precisos, válidos y estén actualizados.

POLÍTICAS DE CONTROL:

- Procedimientos de reconciliación y validación de todos los datos.
- Procedimientos para llevar a cabo un mantenimiento paralelo de los archivos maestros.
- Posesión de los archivos convertidos para permitir que se establezcan los procedimientos de aceptación y cierre por parte del usuario.
- El personal ajeno a la empresa debe acceder a la menor cantidad de datos posible, y cualquier dato que introduzcan debe estar sometido a una validación extraordinaria

5. Las conversiones automáticas requieren que se tengan en cuenta consideraciones especiales que aseguren un control adecuado:
   - Deben generarse automáticamente informes de control desde los archivos de entrada, intermedios y finales.
   - Los informes de control deben contener en los campos clave tanto los contadores de los registros y los totales de los controles. • Debe generarse un listado automático de los registros no transferidos debido a cualquier error.

CONTROLES DE: CONVERSIÓN

OBJETIVOS DE CONTROL:

Se debe realizar un proceso de limpieza de los datos antes de la conversión, para garantizar que todos los datos a convertir sean precisos, válidos y estén actualizados.

POLÍTICAS DE CONTROL:

6. Se debe mantener una operación en paralelo para la puesta en producción de un sistema nuevo.

7. La finalización de la operación del paralelo sólo debe ser realizada con la aceptación por escrito del Jefe o Gerente del proyecto una vez que se han realizado todas las pruebas de aceptación y comprobación requeridas.

8. Se debe determinar la fecha de corte de los procesos anteriores y la fecha de inicio del nuevo sistema.

9. Los productos tangibles de esta fase constituyen la evidencia de que la misma ha sido completada satisfactoriamente.

4.3.5. CONTROLES DE PRUEBA

4.3.5.1 CONTROLES DE LAS PRUEBAS DE ACEPTACIÓN

CONTROLES DE: PRUEBAS DE ACEPTACIÓN

OBJETIVOS DE CONTROL:

Efectuar pruebas de Aceptación, que consistan en probar con datos reales la información con que el sistema deberá operar.

POLÍTICAS DE CONTROL:

1. La documentación de los programas, el manual del usuario y el manual de operación deben existir antes de ejecutar una prueba de aceptación
2. Se debe concluir las pruebas de aceptación por parte del usuario con la firma del usuario en el requerimiento del sistema con lo cual califica al sistema como apto para entrar en la etapa de paralelo
3. Se debe contar con una documentación de las pruebas de aceptación debidamente finada por el usuario.
4. Se deben efectuar inspecciones de las pruebas de aceptación realizadas.
5. Se debe mantener documentación de la prueba de aceptación.

4.3.6. CONTROLES DE AUDITORÍA

CONTROLES DE: AUDITORÍA
OBJETIVOS DE CONTROL: Realizar auditorías internas y/o independientes en intervalos de tiempos determinados para que la empresa se vea beneficiada con mejores recomendaciones para la implementación de los sistemas de información y de esta manera aumentar los niveles de confianza.
POLÍTICAS DE CONTROL: 1. La alta gerencia deberá establecer normas, políticas y estatutos de control en las que se detallen las responsabilidades de quienes realicen las auditorías independientes 2. Los miembros del comité de auditoría deberán ser independientes tanto de la empresa como a los Sistemas de Información por lo que se recomienda contratar los servicios de auditores externos. 3. Se deben desarrollar, documentar, y probar los procedimientos de respaldo de la auditoría del SI. 4. Activar en la auditoría, alarmas para la recuperación de reglas de acceso incorrectas, inexistentes o redundantes en los elementos que interactúan con el sistema, así como para detectar configuraciones incorrectas.

CONTROLES DE: AUDITORÍA

OBJETIVOS DE CONTROL:

Realizar auditorías internas y/o independientes en intervalos de tiempos determinados para que la empresa se vea beneficiada con mejores recomendaciones para la implementación de los sistemas de información y de esta manera aumentar los niveles de confianza.

POLÍTICAS DE CONTROL:

5. El auditor debe revisar:

- El plan de implementación.
- El desarrollo de la capacitación formal a los usuarios involucrados en el SI.
- El cumplimiento adecuado de la conversión y el funcionamiento del paralelo.
- La suspensión del paralelo y el inicio en la operación del nuevo sistema.
- La adecuada asignación de las funciones, perfiles y accesos otorgados
- La aceptación formal del usuario
- Los procedimientos y la documentación del sistema.

6. Auditoría debe evaluar los productos resultantes y entregables de la fase.

4.3.7. CONTROLES DE SEGURIDAD

CONTROLES DE: CONTROLES DE SEGURIDAD
OBJETIVOS DE CONTROL: Evaluar la seguridad del Sistema de Información y establecer la confiabilidad de las mismas.
POLÍTICAS DE CONTROL: 1. Se debe designar un responsable de la función de seguridad de los sistemas empresariales. 2. Se deben hacer revisiones de las Capas de la Seguridad Empresarial, aunque si bien éstas se concentran en otros aspectos y no hacen foco en las fases del ciclo de vida de software, de una u otra manera incidirán en la implementación del nuevo SI. Por ello a través de una lista de chequeo se debe efectuar revisión de estos elementos que indirectamente podrían generar vulnerabilidades en el SI, los cuales son: ▣ Seguridad en la Arquitectura de la Red. ▣ Sistemas de Protección. ▣ Seguridad en Sistemas Operativos.

CONTROLES DE: CONTROLES DE SEGURIDAD

OBJETIVOS DE CONTROL:

Evaluar la seguridad del Sistema de Información y establecer la confiabilidad de las mismas.

POLÍTICAS DE CONTROL:

3. Se debe evaluar el riesgo (análisis de riesgo) determinado de la criticidad o impacto en el sistema.
4. Se deben efectuar pruebas de seguridad (test de seguridad) y éstas no deben ocasionar intencional o involuntariamente interferencia en la operación de los sistemas de información a no ser que estas estén autorizados para el efecto,
5. Debe contarse con un consentimiento escrito por parte de la gerencia para desarrollar el test de seguridad.
6. Los probadores de seguridad deben tener cuidado de no alterar o dañar cualquier información o sistemas de información durante la prueba a no ser que estas estén autorizados para el efecto.
7. Se deben efectuar pruebas y evaluaciones técnicas del sistema con fa finalidad de ver cuan bien están configurados los requerimientos de seguridad internamente

CONTROLES DE: CONTROLES DE SEGURIDAD

OBJETIVOS DE CONTROL:

Evaluar la seguridad del Sistema de Información y establecer la confiabilidad de las mismas.

POLÍTICAS DE CONTROL:

8. Se deben preservar los principios básicos de seguridad, confidencialidad, integridad y disponibilidad en el sistema, por ello se deberán efectuar pruebas que permiten velar el cumplimiento de dichos principios.
9. Incluir políticas de control de Obtención de Aseguramiento independiente.

4.3.7.1. SEGURIDAD EN LA ARQUITECTURA DE LA RED

CONTROLES DE: SEGURIDAD EN LA ARQUITECTURA DE LA RED
OBJETIVOS DE CONTROL: Proteger físicamente el Sistema de Información, controlando los accesos a la red de información.
POLÍTICAS DE CONTROL: 1. Se deben cuantificar y prevenir de situaciones de error y deben ser mitigadas. 2. Se deben disponer de mecanismos de recuperación ante problemas graves, y desastres o siniestros. 3. Se debe proteger físicamente a los servidores. 4. Controlar todos los accesos a la red corporativa 5. Revisión de las conexiones de red físicas y lógicas a fin de evitar vulnerabilidades.

4.3.7.2. SISTEMAS DE PROTECCIÓN

CONTROLES DE: SISTEMAS DE PROTECCIÓN
OBJETIVOS DE CONTROL: Determinar las herramientas necesarias que se utilizarán para proteger el sistema de información.
POLÍTICAS DE CONTROL: 1. Es necesario activar las opciones de registro de las aplicaciones críticas. 2. Deben realizarse revisiones periódicas de los registros. 3. Debe existir personal calificado para realizar estos análisis. 4. Se debe contar con herramientas para facilitar el análisis de estos logs off-line, así como para la detección de comportamientos anómalos de forma automática y que activen alarmas.

4.3.7.3 SEGURIDAD EN SISTEMAS OPERATIVOS

CONTROLES DE: SEGURIDAD EN SISTEMAS OPERATIVOS
OBJETIVOS DE CONTROL: Cerrar la mayor cantidad de puertos posibles para salvaguardar la información.
POLÍTICAS DE CONTROL: 1. Se deben cerrar la mayor cantidad de puertos posibles, ya que cualquier puerto abierto es una puerta de entrada 2. Se deben cerrar los puertos no usados. 3. Se debe emplear protección para los puertos usados. 4. Conceder los permisos adecuados en detalles a cada recurso 5. Activar contraseñas del sistema (logs) y revisarlos periódicamente.

4.3.8. CONTROLES EN LA POST-IMPLEMENTACIÓN

CONTROLES DE: POST-IMPLEMENTACIÓN

OBJETIVOS DE CONTROL:

Verificar que el sistema implantado funcione correctamente, mediante el seguimiento de las operaciones que realiza.

POLÍTICAS DE CONTROL:

1. Se debe ejecutar un seguimiento de los procesos y funciones implementados con el objeto de detectar desviaciones y determinar posibles soluciones para ser consideradas en el momento o en las implementaciones posteriores.
2. En caso de encontrarse falencias significativas, se debe enviar al área de desarrollo las desviaciones o fallas encontradas para que elaboren las modificaciones pertinentes en forma oportuna.
3. Se debe proporcionar de área de mantenimiento o soporte de usuarios todos los elementos necesarios para que puedan hacerse cargo del sistema.
4. A todo proyecto que se ponga en operación se le deberá practicar una evaluación operativa post-implementación, para determinar si éste realmente ha cubierto los requerimientos del usuario en términos de objetivos, efectividad y análisis costo beneficio.

CONTROLES DE: POST-IMPLEMENTACIÓN

OBJETIVOS DE CONTROL:

Verificar que el sistema implantado funcione correctamente, mediante el seguimiento de las operaciones que realiza.

POLÍTICAS DE CONTROL:

5. Se debe evaluar la efectividad del Sistema y el cumplimiento de los requerimientos de los usuarios teniendo en cuenta los siguientes aspectos:

- Satisfacción del usuario
- Tiempos de respuesta
- Grado de uso
- Confiabilidad
- Oportunidad de la inf. brindada
- Integridad
- Documentación

6. Deberá tomarse como fuente de información durante el desarrollo de la evaluación operativa la documentación del sistema.
7. La evaluación operativa se realizará utilizando las técnicas de recopilación de información más adecuadas y será aplicada a los usuarios directos de los productos del sistema
8. Intervendrán en la evaluación operativa el personal informático que

CONTROLES DE: POST-IMPLEMENTACIÓN

OBJETIVOS DE CONTROL:

Verificar que el sistema implantado funcione correctamente, mediante el seguimiento de las operaciones que realiza.

POLÍTICAS DE CONTROL:

opera y/o administra el sistema.

9. La evaluación operativa post-implementación deberá cumplir con los objetivos propuestos.
10. Debe llevarse a cabo una revisión de los resultados de procesamiento por personal del grupo de control de calidad en forma programada

12. Realizar rutinariamente evaluaciones del grado de satisfacción del usuario, para determinar si sus requerimientos y necesidades han sido cumplidas en base a la solicitud original.

13. La revisión post-implementación debe incluir un análisis de los beneficios y de los costos originalmente estimados, en comparación con los costos y beneficios reales.

    Se debe evaluar factores como cambios en los volúmenes y tiempos de proceso.

CONTROLES DE: POST-IMPLEMENTACIÓN

OBJETIVOS DE CONTROL:

Verificar que el sistema implantado funcione correctamente, mediante el seguimiento de las operaciones que realiza.

POLÍTICAS DE CONTROL:

14. Se debe controlar los recursos materiales y tecnológicos que intervienen en el sistema.

15. La integridad del sistema en cuanto al cumplimiento de lo que hace o debe hacer, debe estar garantizada en la fase de la prueba de aceptación de la implementación, sin embargo se deben efectuar pruebas de efectividad y cumplimiento del sistema en la fase de post-implementación, luego de la instalación del mismo

Figura 4.0 PORCENTAJES DE SISTEMAS DE INFORMACIÓN QUE SE IMPLANTAN DENTRO Y FUERA DEL PRESUPUESTO ASIGNADO AL PROYECTO

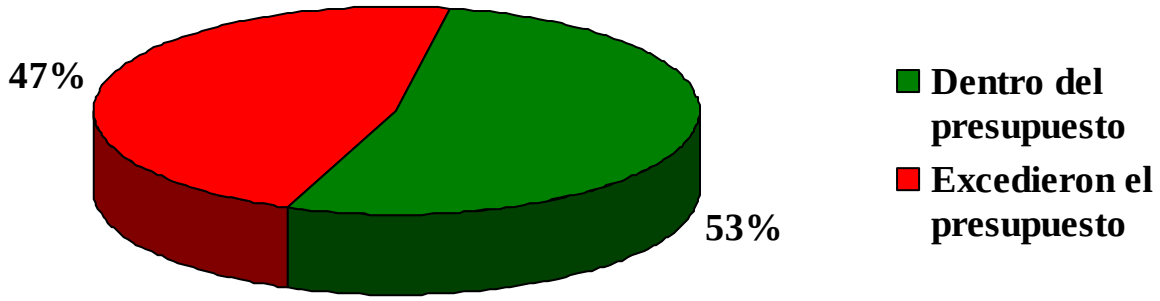


Figura 4.1 PORCENTAJES DE SISTEMAS DE INFORMACIÓN CUYA IMPLEMENTACIÓN FUE FINALIZADA O CANCELADA

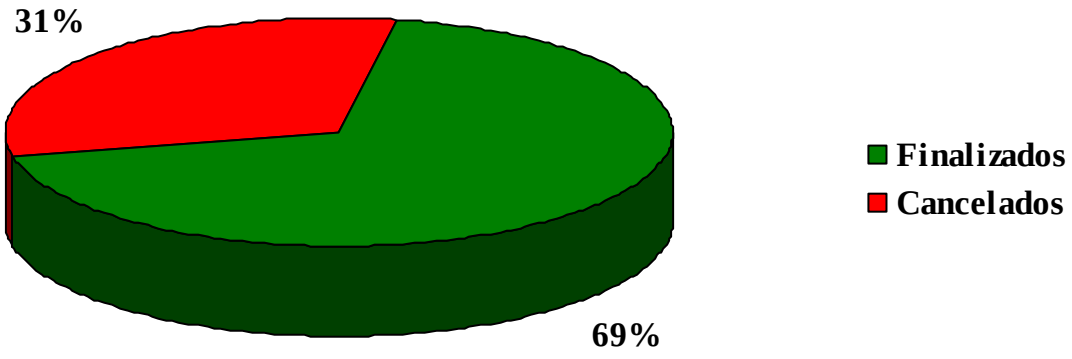
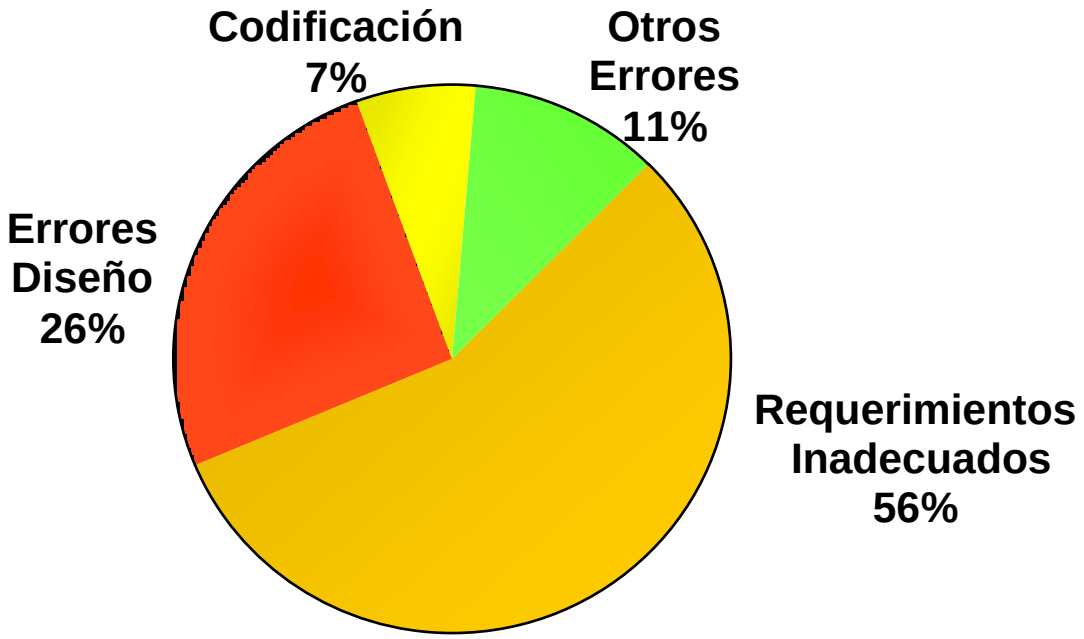


Figura 4.2 ERRORES FRECUENTES EN LA IMPLEMENTACIÓN DE SISTEMAS DE INFORMACIÓN



CONCLUSIONES

1. Los sistemas de información tienen como objetivo principal ayudar a tomar decisiones oportunas para la empresa, proporcionando la información requerida de manera eficiente.

2. Los controles que deben aplicarse en la implementación de sistemas de información se deben redactar en un manual, el cual será de gran ayuda para los usuarios de la información guardada en estos sistemas. Lo cual facilita las operaciones de la empresa porque la información se obtiene en tiempos reales es decir inmediatamente luego de ser ingresados los datos al sistema.

3. Durante los próximos años, los Sistemas de Información cumplirán tres objetivos básicos dentro de las organizaciones:
   - Automatización de procesos operativos.
   - Proporcionar información que sirva de apoyo al proceso de toma de decisiones.
   - Lograr ventajas competitivas a través de su implantación y uso.

4. Los Sistemas de Información deben enfrentar varias clases de retos tales como: el reto estratégico de los negocios, en el cual se destacen las siguientes características:

   - Los cambios tecnológicos se mueven más rápido que los cambios de los seres humanos o las instituciones.
   - Necesitarán del uso de la tecnología para simplificar la comunicación y la coordinación.
   - En la actualidad las instituciones solo automatizan lo que hacen actualmente, dejan pasar en gran medida el potencial de la tecnología de la información.

5. El reto de la globalización.

   - Que los sistemas puedan dar soporte a las ventas y compras de productos en muchos países.

6. El reto de la arquitectura de la información.

   - Nuevas formas de hacer negocios
   - Se da más importancia al hardware, software y redes; que a la propia información.

7. El reto de la responsabilidad y control.

- Los Sistemas de Información juegan un papel crítico en los negocios, en el gobierno y en la vida diaria, entonces debemos asegurarnos que sean precisos, confiables y seguros.
- Los sistemas automáticos o semiautomáticos que funcionen mal pueden traer daños desastrosos.

8. La elaboración del presente manual me ayudó a conocer todas las etapas que intervienen en la implementación de Sistemas de Información.

9. Detallé los controles mínimos que deben ejecutarse en el Sistema para poder aminorar los riesgos a los que está expuesto.

10. Con este trabajo he tratado de minimizar los riesgos que pueden aparecer en el momento de implantar un Sistema de Información en un empresa.

RECOMENDACIONES

1. Se recomienda aplicar los controles que se requieran en cada etapa del proceso de los sistemas de información según lo establecen los estándares internacionales.

2. Los usuarios de los sistemas de información deberán tomar la capacitación necesaria para que conozcan cómo se aplicarán los controles preventivos, detectivos y correctivos en la implementación de sistemas.

3. La alta gerencia deberá trabajar en conjunto con el personal de sistemas y de auditoría para conocer cuales serán los controles que deberán aplicarse en la implementación de un nuevo sistema de información con el debido uso y conocimiento del manual realizado.

4. El sistema de información que ha sido implantado deberá actualizarse constantemente en controles según la tecnología y los estándares internacionales para que sea eficiente y eficaz.

5. Siendo el contador público un gran partícipe en la administración de las compañías como asesor o consultor; es este profesional quien debe adquirir el compromiso de propender el desarrollo empresarial con la implementación de nuevos conceptos, como el de control interno moderno que sería de gran utilidad en la consecución de objetivos y metas institucionales sobretodo de las pequeñas y medianas empresas que son las más urgidas de una adecuada asesoría operativa, financiera, de sistemas y normativa. Categorías que reúne en su estructura conceptual y aplicativa el control interno.

BIBLIOGRAFÍA

1. Enciclopedia Autodidáctica Océano, Volumen II (ISBN 84-7764-011-4, Grupo Editorial Océano, 1988)

2. Muñoz Razo Carlos, Auditoría en Sistemas Computacionales (ISBN: 970-17-0405-3, Pearson Education, México, 2002)

3. Senn James, Sistemas de Información para la Administración (Editorial Ibero América, México, 1992)

4. Senn James, Análisis y Diseño de Sistemas de Información (Editorial Mc. Graw Hill, México, 1992)

5. Cuervo José; Delitos informáticos: Protección Penal de la Intimidad http://www.informatica-juridica.com/trabajos/delitos.asp

6. Comité Directivo de COBIT y El IT Governance Institute, 2002. COBIT – Objetivos de Control, Tercera Edición (ISBN: 1-893209-17-2)

7. Diccionario Enciclopédico, Tomo IV (ISBN 84-7153-005-8, Bibliograf S.A., 1973.

8. El mundo de la Informática Forense http://www.xombra.com

9. Internacional Organization for Standarization. Recuperado en abril de 2007. http://www.iso.org/iso/home.htm

10. Miguel Ángel Caffaro; Informática Profesional, publicación del Consejo Profesional en Ciencias Informáticas Año 17, Nº 87, Mayo de 2001. http://www.cpci.org.ar/newsletters/87/Pericia.ht- 22k

11. MONOGRAFIAS. (2006), ”Auditoría de Sistemas”, http://www.monografias.com/trabajos14/auditoriasistemas/auditoriasistemas

12. Microsoft Corporation, Biblioteca Premium Microsoft Encarta 2006.

13. Saffirio Mario, Tecnologías de Información y Arquitectura de Sistemas http://msaffirio.wordpress.com