2

UNIVERSIDAD NACIONAL AUTONOMA DE MEXICO

FACULTAD DE ESTUDIOS SUPERIORES
CUAUTITLAN

"AUDITORIA EN EL AREA DE DESARROLLO Y MANTENIMIENTO DE SISTEMAS"

T E S I S
QUE PARA OBTENER EL TITULO DE
LICENCIADA EN INFORMATICA
P R E S E N T A:

OGILVIA GUADALUPE RICO UREÑA

ASESOR: L.C. CARLOS PINEDA MUÑOZ

CUAUTITLAN IZCALLI, EDO. DE MEX. 2002

FACULTAD DE ESTUDIOS SUPERIORES CUAUTITLAN
UNIDAD DE LA ADMINISTRACION ESCOLAR
DEPARTAMENTO DE EXAMENES PROFESIONALES

ASUNTO: VOTOS APROBATORIOS

U. N. A. M.
FACULTAD DE ESTUDIOS
SUPERIORES-CUAUTITLAN

DEPARTAMENTO DE
EXAMENES PROFESIONALES

DR. JUAN ANTONIO MONTARAZ CRESPO
DIRECTOR DE LA FES CUAUTITLAN
P R E S E N T E

ATN: Q. Ma. del Carmen García Mijares
Jefe del Departamento de Exámenes
Profesionales de la FES Cuautitlán

Con base en el art. 28 del Reglamento General de Exámenes, nos permitimos comunicar a usted que revisamos la TESIS:
"Auditoría en el Area de Desarrollo y Mantenimiento de Sistemas".
que presenta la pasante: Ogilvia Guadalupe Rico Ureña
con número de cuenta: 8901833-2 para obtener el título de :
Licenciada en Informática

Considerando que dicho trabajo reúne los requisitos necesarios para ser discutido en el EXAMEN PROFESIONAL correspondiente, otorgamos nuestro VOTO APROBATORIO.

A T E N T A M E N T E
"POR MI RAZA HABLARA EL ESPIRITU"
Cuautitlán Izcalli, Méx. a 24 de Abril de 2002.

PRESIDENTE	Ing. Sergio P. Acosta Torres
VOCAL	L.C. Carlos Pineda Muñoz
SECRETARIO	Lic. Rogelio Sánchez Arrastio
PRIMER SUPLENTE	Lic. Armando Carmona Bonilla
SEGUNDO SUPLENTE	MAI. Manuel Jauregui Renault

AGRADECIMIENTOS

A MI MAMÁ SRA. MARGARITA UREÑA y

MI PAPÁ SR. MANUEL RICO

A quienes sin escatimar esfuerzo alguno, me han dado gran parte

de su vida para formarme y educarme.

A quienes la ilusión de su vida ha sido convertirme en una persona de provecho.

A quienes siempre han estado cerca de mi, brindándome todo su cariño y apoyo.

A quienes nunca podré pagar todos sus desvelos, ni con las riquezas más grandes del mundo.

Por eso y mucho.....infinitas Gracias.

GRACIAS

A MIS HERMANOS Y HERMANAS

ESTELA, AMI, VICTOR, MARY, IRENE, JUAN,

GUILLERMO Y EDMUNDO

Por escucharme, aconsejarme, enseñarme y permitirme contar con toda su confianza

Pero sobre todo, por creer en mi y alentarme siempre a seguir adelante.

A MIS ABUELITOS

BENITO ✞. MARÍA Y LUPE.

Por su cariño, por enseñarme su fortaleza y que nada en la vida es imposible.

AL AMOR DE MI VIDA

JUAN CARLOS BASILIO OLIVARES

Con especial agradecimiento por su apoyo, ternura, amor y cariño que me has brindado.

Por ser parte importante de mi vida, de la cual día a día hemos aprendido a superarnos, poner todo de nuestra parte a lo que hacemos, siempre intentar ser mejores y así alcanzar poco a poco todos nuestros objetivos.

A LA FAMILIA BASILIO OLIVARES

SRA. SUSANA, SR. JUAN, ARA [illegible]LI

Por abrirme las puertas de su hogar,

por brindarme su apoyo [illegible]

y sobre todo por confiar en mí [illegible]

A LA SRA. "ANDREA", ELO Y D[illegible]LIS

Por todo su [illegible]riño, com[illegible]anza y

por [illegible]rme las puertas [illegible] su corazón.

A LA TÍA DE J.C. "MARY"

Por siempre creer en mi, por su confianza y en especial, por su apoyo y aliento para no detenerme y concluir uno de los objetivos más importantes de mi vida, mi Titulación.

A TODOS MIS AMIGOS Y EN ESPECIAL A

ALINA, SANDRA, NORMA, REINA, HECTOR, RICARDO Y GERMAN

Por su amistad, cariño y confianza, por poder siempre contar con ustedes,

por escucharme y aconsejarme en los momentos que más se necesita,

lo cual los convierte en mis verdaderos amigos.

A SERGIO RUIZ, ALIDA POLANCO, PILAR PLIEGO, CARLOS CHALICO, SARAI, MARGARITA, BERTHA, ROCIO, BETY Y DEMÁS AMIGOS Y COMPAÑEROS DE MANCERA ERNST & YOUNG

Por toda su ayuda y apoyo, por dejarme aprender un poquito de ellos, así como por ser parte muy importante para el logro de una de mis metas más importantes, mi Titulación.

GRACIAS

A LA UNIVERSIDAD NACIONAL AUTÓNOMA DE MÉXICO

Por haberme abierto las puertas para forjarme [illegible] mejor [illegible]

Por poder formar parte del selecto grupo de personas que [illegible]

nos sentimos orgullosamente Universitarios

Por brindarme el apoyo para concluir el bachillerato y la licenciatura.

A LA FACULTAD DE ESTUDIOS SUPERIORES CUAUTITLÁN

Por abrigarme y permitirme recibir en ella, los conocimientos

que me abren el camino a una vida profesional y personal.

A MIS PROFESORES Y PROFESORAS

Por compartir su tiempo, conocimientos y experiencias en favor

de mi desarrollo profesional.

AL L.C. CARLOS PINEDA MUÑOZ

Por su enseñanza, asesoría y colaboración

para la realización de [illegible] Trabajo.

A [illegible] SINODALES

Por representar una parte fundam[illegible]al en mi [illegible]da profesional.

A toda la gente que de alguna u otra manera a [illegible]ado por mi vida y de la cuál he aprendido.

Todos y cada uno han contribuido en [illegible]formación y en el logro de éste objetivo.

ÍNDICE

PLANTEAMIENTO DEL PROBLEMA

Actualmente en la mayoría de las empresas públicas y privadas, no se le da la importancia suficiente a la auditoría en el área de desarrollo y mantenimiento de sistemas, debido a que solo se les considera como un área generadora de sistemas procesadores de información, sin embargo existe gran riesgo en el manejo de la seguridad de la información confidencial dentro de los mismos.

JUSTIFICACIÓN

La presente investigación sirve para resaltar la importancia, beneficios y ventajas que tiene la auditoría en el área de desarrollo y mantenimiento de sistemas, así como de apoyo para el auditor informático en el desempeño del proceso de evaluación de seguridad de acceso y manejo de información dentro de una auditoría en el área de desarrollo y mantenimiento de sistemas.

OBJETIVO GENERAL

Mostrar la importancia y beneficios que tiene la Auditoría en Sistemas en el Área de Desarrollo y Mantenimiento de Sistemas.

OBJETIVOS PARTICULARES

- Explicar la importancia del papel que desempeña el Auditor en Sistemas dentro de una evaluación de seguridad de acceso y manejo de la información, dentro de los sistemas.

- Dar a conocer el marco de conocimientos que rodean a las actividades realizadas por el Auditor en Sistemas en el Área de Desarrollo y Mantenimiento de Sistemas.

- Analizar los factores que se requieren para que un sistema sea lo suficientemente seguro y confiable, disminuyendo el riesgo de plagio y sustracción no autorizada de información, así como un buen procesamiento dentro de los mismos, ya fuese adquirido o desarrollado.

- Establecer una fuente de información e investigación para aquellos estudiantes que tienen interés en profundizar en la Auditoría en Sistemas, dentro del Área de Desarrollo y Mantenimiento de Sistemas, así como a las personas que se inician en el ámbito de la Auditoría en Sistemas.

- Retribuir con el presente trabajo, los conocimientos y experiencias que me brindaron: la Universidad Nacional Autónoma de México, los profesores y mis compañeros.

INTRODUCCIÓN

El acelerado crecimiento de las Instituciones, Empresas o Compañías y su consecuente necesidad de delegar funciones y responsabilidades sin perder los controles básicos, así como la necesidad fundamental de poder mantenerse en el mercado a niveles competitivos, son factores que justifican el uso de sistemas de información a través de computadores, pero además requieren de un buen desarrollo, mantenimiento y uso de los mismos.

Introduciéndonos un poco al inmenso mundo de la informática, cuya palabra se deriva del frances *informatique*, neologismo que proviene de la conjunción de *information* (información) y *automatique* (automática) [1], es el campo que se encarga del estudio y aplicación práctica de la tecnología, métodos, técnicas y herramientas relacionadas con las computadoras y el manejo de la información por medios electrónicos; definiremos el concepto de "Sistema", como un grupo de elementos interrelacionados que forman un todo, por lo que "Sistema de Información" es el conjunto de elementos y procedimientos íntimamente relacionados que tienen como propósito manejar datos y elaborar reportes que permitan tomar decisiones adecuadas para el logro de los objetivos de una organización.

Cabe mencionar que ante el acelerado crecimiento del uso de la computadora personal y ante la carencia de capacitación adecuada, en la mayoría de los casos, el uso y la programación, se han desarrollado de una manera un tanto empírica y autodidacta, sin tener una clara conciencia de riesgos, responsabilidades y controles con el consecuente costo de tiempo y mal uso de los recursos tecnológicos.

[1] Rodríguez Beristain, Luis Manuel, Auditoría al Área de Telecomunicaciones

Aquí es donde el Auditor surge por la necesidad de realizar análisis para investigar el control a detalle en cada operación, recomendando y concluyendo a nivel Gerencial para obtener una mayor eficiencia y economía en los controles establecidos o por establecer.

La Auditoría Informática es la revisión y evaluación de los controles, sistemas, procedimientos de informática; de los equipos de cómputo, su utilización, eficiencia y seguridad, de la organización que participa en el procesamiento de la información, a fin de que por medio del señalamiento de cursos alternativos se logre una utilización más eficiente y segura de la información que servirá para una adecuada toma de decisiones[2]. La Auditoría Informática también es conocida como Auditoría en Sistemas.

El Auditor Informático dentro del área de Desarrollo y Mantenimiento de Sistemas debe evaluar la suficiencia de los procesos usados en el desarrollo y mantenimiento de sistemas y del control interno de los sistemas, tanto manual como automático.

[2] Echenique García, J.A., Auditoría en Informática

1.- FUNDAMENTOS DE AUDITORÍA

1.1.- Origen de la Auditoría

La Auditoría tuvo su origen después de que surgieran las primeras empresas y negocios del mundo. En un principio éstas eran atendidas por sus propietarios, pero al empezar a crecer tuvieron que contratar personal para poder seguir atendiendo al cliente; debido a que los propietarios no se daban abasto, además de la falta de control oportuna, originó los primeros fraudes, situación por la cual el propietario además de realizar las clásicas labores de supervisión, empezó a realizar labores de auditoría, surgiendo así el primer Auditor.

La función de Auditoría se cree fue creada en los Estados Unidos de América, en las empresas de ferrocarriles durante el siglo XIX, debido a la red tan amplia que tenía en sus operaciones. Otras empresas que tenían sus operaciones en más de una localidad, como eran supermercados, empresa eléctricas y de servicios públicos entre otras, empezaron a contar entre sus empleados con Auditores.

Durante gran parte del siglo XX, la Auditoría se ha encontrado conceptualizada como una actividad de "protección", cuya única finalidad era la detección y prevención de fraudes.

Con el paso del tiempo y gracias a los cambios de mentalidad del propietario de la organización y del Auditor, su campo de actuación se ha ido incrementando o ampliando inclusive en otros campos y ciencias.

Su desarrollo ha sido paulatino y a pesar de que sus funciones se ampliaron al examen de nóminas, conciliaciones bancarias, la comprobación de la exactitud de las operaciones en los registros contables, en los estados financieros y en la verificación de los activos fijos, las revisiones del Auditor seguían siendo consideradas como de "autopsia" (después de los hechos).

Sin embargo actualmente la Auditoría constituye un elemento muy importante en la supervisión y el control de las distintas operaciones realizadas por las Instituciones o Empresas.

1.2.- Concepto de Auditoría

La palabra AUDITORIA viene del latín *auditorius*, que significa oír, y fue aplicada a las personas que oían y comprobaban las cifras y operaciones reportadas por los empleados de las empresas, para certificar ante el propietario y ante el público en general la veracidad de las mismas.

Existen diversas definiciones, de las cuales podemos globalizar en la siguiente:
Actividad consistente en la emisión de una opinión profesional a las partes interesadas, sobre si el objeto sometido a análisis (operaciones financieras, administrativas, operativas, fiscales, informáticas y de otros tipo de una entidad pública o de una empresa) presenta adecuadamente la realidad que pretende reflejar y/o cumple las condiciones que le han sido prescritas, a fin de evaluar la eficiencia y eficacia con que se están llevando a cabo,

para que por medio de opciones alternas se tomen decisiones que permitan corregir los errores y así mejorar el marco de actuación.

1.3.- Tipos de Auditoría

La Auditoría se divide en dos grandes rubros tomando en cuenta las características del personal que la realiza, con respecto a la Empresa o Institución y son:

- Auditoría Externa.
- Auditoría Interna.

La ***Auditoría Externa*** es aquella que se realiza por Contadores Públicos independientes o Profesionistas especializados, que no tienen ingerencia alguna en la administración del negocio, ni dependencia económica ni funcional dentro de la Empresa o Institución. El Auditor externo es un tercer intermediario en la relación de responsabilidad entre el emisor de la información auditada y los usuarios de ésta[3].

Su primera responsabilidad es para las personas que lo contrataron, por lo tanto sus objetivos principales y específicos de revisión se sintetizan en:

- Coincidencia de cifras mostradas en estados financieros y auxiliares.
- Adecuado control interno.
- Comprobación de que todas las obligaciones estén debidamente registradas y presentadas en los rubros correspondientes.
- Comprobar que las cuentas de activo correspondan a derechos o propiedades reales.

[3] Corporación Salazar y Asociados S C. Apuntes de Diplomado

El trabajo de Auditoría tiene como finalidad inmediata, proporcionar al propio auditor los elementos de juicio y convicción necesarios, para poder dar su dictamen de una manera objetiva y profesional.

La ***Auditoría Interna*** es la actividad independiente dentro de la Empresa, para la evaluación de la organización y el control, y para la revisión de las operaciones y en especial de aquello que tiene repercusión en la información, como base para proporcionar un servicio a la dirección[4].

El objetivo de la auditoría interna es prestar servicio a todos los miembros de la organización en el efectivo desempeño de sus responsabilidades, a través de proporcionarles análisis, evaluaciones, recomendaciones, asesoría, e información relacionada con las actividades revisadas; es objetivo también de la auditoría interna la promoción de un efectivo control a un costo razonable, así como proporcionar ayuda a la administración para comprobar el correcto control de las operaciones, observando y sugiriendo mejoras a los sistemas de control interno.
Es recomendable que esta área para su buen desempeño y funcionamiento e independencia mental, se encuentre directamente a cargo del ejecutivo de más alto nivel dentro de la Organización, ya que de esta forma se garantiza un involucramiento integral.

Las principales diferencias que existen entre la Auditoría Externa e Interna son:

[4] Corporación Salazar y Asociados S.C. Apuntes de Diplomado

	Grado de Independencia	Intereses servidos	Aplicación de técnicas básicas
Auditoría Externa	Mayor	A ninguno en la Organización.	En función de indicadores.
Auditoría Interna	Menor	A la Alta Dirección.	En función de las áreas de interés para la Alta Dirección.

1.4.- Clases de Auditoría

La auditoría se encuentra dividida en diversas clases, éstas, de acuerdo al objeto sometido a estudio y a la finalidad con que se realiza el mismo. A continuación enuncian algunas de éstas.

Clase	Objeto	Finalidad
Financiera	Cuentas anuales	Presentan realidad
Informática	Sistemas de aplicación, recursos informáticos, planes de contingencia, etc.	Operatividad eficiente y según normas establecidas.
Gestión	Dirección	Eficacia, eficiencia, economicidad.
Cumplimiento	Normas establecidas	Las operaciones se adecuan a estas normas

Para efectos de este trabajo, en capítulos posteriores profundizaremos en la Auditoría Informática.

1.5.- Normas y Técnicas de Auditoría

Las ***Normas de Auditoría*** constituyen la referencia autorizada de la auditoría profesional y son los requisitos mínimos de calidad relativos al auditor, al trabajo que desempeña y a la información que rinde como resultado.

Las Normas de Auditoría se clasifican en:

- Normas personales.
- Normas de ejecución del trabajo, y
- Normas de información.

Las *Normas Personales* se refieren a las cualidades y competencia del auditor, así como de la calidad del trabajo de auditoría, y son las siguientes:

- El examen lo deben llevar a cabo personal que posean la preparación y competencia técnica necesaria.
- Es importante desarrollar un trabajo profesional durante la auditoría y en la elaboración del dictamen.
- Durante el trabajo de auditoría el auditor debe mantener una actitud de independencia mental.

Las *Normas de Ejecución del Trabajo*, estas normas abarcan la planeación, supervisión y administración de la auditoría, la evaluación del control interno y la obtención de evidencia suficiente y competente. Además se hace necesario establecer una relación clara entre el nivel de control interno y el alcance, oportunidad y naturaleza de la prueba de Auditoría.

- La auditoría debe ser planeada adecuadamente y los ayudantes involucrados deben ser supervisados adecuadamente.
- Se debe realizar un estudio y evaluación completos del control interno existente, como base para confiar en éste, asimismo, que le permita determinar el alcance de las pruebas y la naturaleza, extensión y oportunidad de los procedimientos de auditoría.

- El auditor debe obtener evidencia comprobatoria suficiente y competente a fin de tener una base razonable para emitir una opinión.

Las *Normas de Información* son las normas relativas al informe o dictamen de la auditoría, en donde reposa la confianza de los interesados y se valora el trabajo del auditor.

- El dictamen dirá si la información presentada está de acuerdo con los principios generalmente aceptados.
- El informe establecerá si los principios han sido aplicados constantemente durante el período actual y el anterior.
- Las revelaciones informativas que aparezcan en el informe o documentación obtenida se consideraran razonablemente adecuadas.
- El dictamen contendrá la expresión de una opinión o una declaración, cuando no es posible expresar una opinión por diversas razones.

Las ***Técnicas de Auditoría*** son los métodos prácticos de investigación y prueba que se utilizan para analizar y comprobar la información y poder emitir una opinión profesional; y son las siguientes:

- Estudio General
- Análisis
- Inspección
- Confirmación
- Investigación
- Declaración
- Certificación

- Observación
- Cálculo

El *Estudio General*, esta representa la apreciación y juicio sobre la fisonomía y características generales de la unidad auditable a examinar, esta apreciación estará fundamentada por la experiencia profesional que el Auditor debe poseer y aplicada a esa unidad sujeta a revisión. Asimismo, dicho estudio hará posible la determinación de puntos significativos o aspectos importantes que requieran atención especial.

El *Análisis* es la clasificación y agrupación de los distintos elementos individuales que forman un todo o universo, de tal forma que cada uno de los elementos que lo constituyen, por sí mismos forman unidades homogéneas y significativas.

La *Inspección* es el examen físico de los bienes materiales o documentos con el objeto de demostrar su autenticidad.

Confirmación.- Se utiliza para ratificar y asegurar por escrito hechos y operaciones, a través de un tercero que se encuentra en posibilidad de conocer la naturaleza y condiciones de los movimientos.

El procedimiento a seguir será mediante el envío, por parte del Auditor, de una "Carta de confirmación", suscrita y firmada por un funcionario facultado por la propia entidad examinada. Es menester aclarar que el Auditor deberá solicitar al confirmante que la

contestación a su misiva le sea enviada directamente a su domicilio social, diferente al del auditado.

La confirmación puede aplicarse bajo alguna de estas modalidades:

Positiva directa:

Es aquella en donde se le solicita al confirmante que conteste tanto si está o no conforme con los datos consignados en la carta certificación.

Negativa directa:

Su objetivo es solicitar al confirmante su contestación sólo en caso de que no esté de acuerdo con los datos consignados en la carta confirmación.

Ciega o indirecta:

Se distingue de las anteriores ya que en este tipo de confirmación no se consigna cifra alguna, únicamente la fecha en la que se presume se está realizando el examen respectivo, por lo tanto, se solicita al confirmante el envío detallado de las operaciones realizadas con el auditado.

La *Investigación* es la recolección de datos que el auditor obtendrá con funcionarios y empleados de la entidad auditada, con el propósito de ampliar su conocimiento acerca de las características particulares que examina, cuyos datos e informes serán transcritos a papeles de trabajo y que con posterioridad serán utilizados para emitir el informe.

Declaración es la manifestación por escrito de las investigaciones realizadas con los funcionarios y empleados en la cual estampan su firma.

La *Certificación* es la obtención de la información con la cual se comprueba un hecho o circunstancia, en la cual generalmente una autoridad legaliza con su firma.

Observación es definida como la técnica mediante la cual el auditor en forma abierta o directa se asegura de operaciones y hechos específicos de la unidad auditada, relativas tanto a la forma en como se conducen las operaciones, como de quien las realiza.

El *Cálculo* es la verificación matemática de ciertos datos para comprobar las operaciones realizadas.

1.6.- Documentación de la Auditoría

La documentación de la auditoría se divide principalmente en:

- Papeles de Trabajo
- Informe de la Auditoría

Papeles de trabajo

Los papeles de trabajo se entiende que son el conjunto de cédulas y documentación fehaciente que contiene los datos e información obtenidos por el auditor en su revisión, así como el detalle e historia de las pruebas realizadas.

Además éstos son el apoyo principal del dictamen del auditor y lo ayudan a planear, ejecutar y supervisar la auditoría, y también servirán de antecedente para auditorías posteriores.

Los papeles de trabajo más específicamente se utilizan para:

- Registrar el conocimiento del negocio y del sistema de control interno.
- Calificar la calidad de la estrategia de la auditoría y su aplicación.
- Documentar la evaluación a detalle de los sistemas, revisión de operaciones y pruebas de cumplimiento.
- Documentar los procedimientos de prueba.
- Demostrar que los auxiliares de auditoría fueron supervisados.
- Dejar precedente para la planeación de auditorías posteriores.
- Registrar las recomendaciones para mejorar los controles.
- Respaldar y fundamentar la opinión o informe del auditor.

Los principios básicos de los papeles de trabajo son:

- En los papeles de trabajo se reflejara la habilidad, destreza y profesionalismo del auditor.
- Estos deben estar organizados de tal manera que faciliten la pronta localización de la información que se necesite.
- Deben reflejar información completa, clara y concisa.
- Se debe distinguir claramente los hechos de las opiniones.

Debido a la importancia que guardan los papeles de trabajo para el auditor y la propia Institución, son propiedad absoluta de la Institución y responsabilidad del auditor, condicionando su utilización exclusivamente a los propósitos de la revisión; de tal forma que la información contenida en ellos debe salvaguardarse como secreto profesional y responsabilidad ética y moral hacia la Institución que se la confió.

Las condicionantes necesarias en los Papeles de Trabajo son las siguientes:

- Nombre de la Unidad Auditable.
- Auditoría practicada.
- Fecha de la revisión.
- Periodo de la revisión.
- Nombre de la cuenta, área o centro de costos.
- Iniciales del auditor y firma del supervisor.
- Identificación clara de la fuente de información.
- Conclusiones y recomendaciones a las que se llegó.

Informe de la auditoría

Informe de auditoría o dictamen, es el resultado formal de la auditoría desarrollada con el fin de transmitir información, presentando conclusiones, recomendaciones e ideas claras y precisas.

Los propósitos del Informe son:

- Lograr que se lleven a cabo acciones determinadas.
- Presentar métodos y recomendaciones que sirvan al responsable del área para coordinar hechos e ideas en forma coherente y en una secuencia congruente.

Elementos del Informe:

- Asunto del dictamen o informe.
- Antecedentes y alcance.
- Objetivos.
- Resultados obtenidos.
- Observaciones, recomendaciones y conclusiones.
- Anexos (si los hubiera).

Cualidades:

- Producto dirigido al Area Operativa y/o Directiva.
- Ordenado.
- Claro y conciso.
- Sencillo y original.
- Interesante para el lector.

Pasos para su preparación:

- Pensar en el(os) destinatario(s).
- Reunir la información, observaciones y hallazgos.
- Desarrollar las recomendaciones y conclusiones.
- Analizar y sintetizar la información obtenida.
- Emitir borrador y entregar el informe.

Una vez que se ha emitido el informe de la auditoría es necesario realizar una reunión con el área o áreas involucradas y discutir el informe y posteriormente presentar el informe o dictamen a nivel directivo.

A continuación se diferencia lo que implica una discusión contra una presentación de informe:

Discusión	Presentación
No existe seguridad	Seguridad en cada punto
Puede existir negociación	No existe negociación
Se pueden cambiar resultados	No se cambia el resultado
Herramientas de validación y comprobación	No puede ser rebatido
Su objetivo es validar	Su objetivo es enterar

2.- AUDITORÍA EN INFORMÁTICA

2.1.- Auditoría Informática

Informática

Etimológicamente, la palabra informática, deriva del francés *informatique*. Este neologismo proviene de la conjunción de *information* (información), y *automatique* (automática)[5].

Su creación fue tratando de dar una alternativa menos técnica y menos orientada al procesamiento de datos.

Entonces informática fue traducido en 1966 como: "Ciencia del tratamiento sistemático y eficaz realizado especialmente mediante máquinas automáticas, de la información contemplada como vehículo del saber humano y de la comunicación de los ámbitos técnico, económico y social"[6].

Y más recientemente la informática se define como: "Ciencia del tratamiento automático y racional de la información considerada como soporte de los conocimientos y las comunicaciones"[7].

[5] Rodríguez Beristain, Luis Manuel, Auditoría al Área de Telecomunicaciones
[6] Corporación Salazar y Asociados S C. Apuntes de Diplomado
[7] Ramón García / Pelayo y Gross, Pequeño Larousse Ilustrado

Auditoría Informática

"Es la revisión y evaluación de los controles, sistemas, procedimientos de informática; de los equipos de cómputo, su utilización, eficiencia y seguridad, de la organización que participan en el procesamiento de la información, a fin de que por medio del señalamiento de cursos alternativos se logre una utilización más eficiente y segura de la información que servirá para una adecuada toma de decisiones"[8].

La función de Auditoría Informática es examinar y validar los controles, políticas y procedimientos informáticos utilizados por toda la organización, para verificar que aspectos tales como: continuidad del servicio y de la operación, confidencialidad, seguridad e integridad de la información, se estén cumpliendo satisfactoriamente de acuerdo a las normas y políticas vigentes, con el fin de reducir la probabilidad que los riesgos se materialicen.

Tipos de Auditoría Informática

A través del tiempo se han realizado diferentes tipos de Auditoría Informática, siendo las más comunes las siguientes:

- Auditoría alrededor del Computador.
- Auditoría al Computador.
- Auditoría por medio del Computador.
- Auditoría al Area de Informática.
- Auditoría a Centros de Cómputo y Telecomunicaciones.

[8] Echenique García, J.A., Auditoría en Informática

Auditoría Alrededor del Computador

Comienza en los primeros días del uso de la computadora, cuando el auditor tradicional no estaba familiarizado con los conceptos y tecnología de las computadoras. En estos tiempos el acercamiento del auditor fue para inspeccionar el sistema de computación y los programas, como una caja negra, revisando únicamente los documentos de entrada y salida. Los controles y procedimientos usados en el procesamiento de datos fueron considerados sin importancia para el auditor, puesto que las salidas generadas por el computador podían ser rastreadas hacia las entradas, y éstas últimas se consideraban válidas.

Sin embargo, como los sistemas de cómputo evolucionaron, éste método se volvió obsoleto, costoso y poco efectivo.

Auditoría al Computador

La auditoría al computador establece mayor énfasis al verificar y probar el sistema mecanizado que produce la salida, más que examinar los resultados obtenidos, por lo que el auditor verifica la efectividad de los procedimientos de control sobre las funciones del computador y de los sistemas de información, así como la exactitud del procesamiento interno.

Este tipo de auditoría requiere de dos tareas básicas:

- La revisión, análisis y verificación de la información fuente.

- Pruebas de las validaciones y lógica del programa del sistema de información y los controles del mismo.

Con este enfoque de auditoría el auditor asume que el computador es una herramienta exacta y programada adecuadamente para generar resultados confiables. Entonces las pruebas deben planearse y proyectarse para comprobar la lógica de la programación, mediante un plan de pruebas exhaustivas.

Las condiciones que se pueden verificar con este plan, son básicamente las siguientes:

- Trazar la efectividad de los controles y la exactitud de la programación.
- Probar movimientos fuera de secuencia.
- Procesar con archivos falsos.
- Validar condiciones fuera de rango, de unidad, de estructura, de códigos y de tipo de campo.
- Probar números con signo negativo.

Auditoría por medio del Computador

Este tipo de auditoría también es llamada comúnmente "Apoyos computacionales" al área de Auditoría Interna, y en ésta se llevan a cabo desarrollos de programación para explotar las bases de datos, archivos tradicionales u otro tipo de archivos de acuerdo a las

necesidades de las auditorías: operacional, financiera, áreas staff, departamentos especiales, etc.

Los apoyos computacionales varían de acuerdo con la filosofía y técnica de cada Organización. Sin embargo existen ciertas técnicas y/o procedimientos que son compatibles con la mayoría de los ambientes de informática o cómputo.

Al utilizarse estos apoyos en la ejecución de la auditoría, permitirán ampliar la cobertura de ésta, reduciendo el tiempo/costo de las pruebas y procedimientos de muestreo, y dando más tiempo para el análisis y estudio de la información obtenida del computador.

Además al utilizar el auditor el computador le permitirá familiarizarse con la operación del equipo.

La auditoría utilizando el computador puede ser empleada entre otras cosas, para:

- Verificación de cifras de control.
- Calcular y comprobar la exactitud de los reportes de salida producidos por el área de informática.
- Probar los registros de los archivos, verificando la consistencia lógica, las validaciones y la razonabilidad del monto de las operaciones.
- Clasificar datos y analizar la ejecución de los procedimientos.
- Seleccionar, segmentar y comprobar datos utilizando técnicas de muestreo.

- Imprimir confirmaciones preseleccionadas.
- Simular transacciones verificando la programación.

Cuando los programas de auditoría se procesen, los auditores deberán asegurarse de la integridad del procesamiento, con:

- Mantener el control básico sobre los programas que se encuentren catalogados en el sistema y realizar respaldos de información adecuados.
- Observar directamente el procesamiento de las aplicaciones de auditoría.
- Desarrollar programas independientes de control que monitoreen el procesamiento del programa de auditoría.
- Mantener el control sobre las especificaciones de los programas, documentación y comandos de control.
- Controlar la integridad de los archivos que están procesando y las salidas generadas.

Auditoría al Área de Informática

Anteriormente ya hemos definido Auditoría Informática dentro de este mismo capítulo, por lo que al realizar una Auditoría al Area de Informática, debemos de considerar además de la evaluación de los equipos de cómputo, un sistema o procedimiento específico, los sistemas de información en aspectos tales como:

- Entradas.

- Salidas
- Procedimientos.
- Controles.
- Archivos.
- Seguridad Física.
- Seguridad Lógica.
- Obtención de la información.
- Etc.

Ello debe incluir los equipos de cómputo en algunos casos, cómo la herramienta que permita obtener la información adecuada y por otro lado debe ser enfocada al área o áreas involucradas en cada organización (departamento de cómputo, departamento de informática, gerencia de procesos electrónicos, área de sistemas, etc.).

El campo de acción de los auditores al realizar una Auditoría Informática dentro de las organizaciones, será aplicable a las áreas mencionadas en el párrafo anterior en los siguientes aspectos:

Evaluación Administrativa

- Los objetivos de departamentos, dirección o gerencia.
- Metas, planes estratégicos y procedimientos de procesos electrónicos estándar.
- Organización del área y su estructura orgánica.

- Funciones y niveles de autoridad, y responsabilidad del área de procesos electrónicos.
- Integración de los recursos materiales y técnicos.
- Estrategia.
- Costos y controles presupuestales.
- Controles administrativos.

Evaluación de los sistemas y procedimientos

- De los análisis y sus diferentes etapas.
- Del diseño lógico.
- Del desarrollo y mantenimiento.
- Control de proyectos.
- Control de las etapas y programación.
- Documentación y manuales.
- Seguridad física y lógica.
- Confidencialidad de passwords.
- Controles de mantenimiento.
- Formas de respaldo.
- Utilización.

Evaluación del Proceso de Datos y de Equipos de Cómputo

- Control de los datos fuente y cifras de control.
- Control de operación.
- Control de salidas.
- Control de asignación de trabajos.
- Control de medios de almacenamiento masivo.
- Control de recursos de cómputo.
- Seguridad en centros de cómputo.
- Seguridad física y lógica.
- Confidencialidad de la información.
- Respaldos.
- Planes de Contingencia.

Auditoría a Centros de Cómputo y Telecomunicaciones

Es el tipo de auditoría informática que en los últimos tiempos se ha venido realizando, ya que la evolución y capacitación ha sufrido grandes actualizaciones y modificaciones, por lo que este tipo de auditoría está dirigida a identificar áreas de oportunidad dentro de Centros de Cómputo y Telecomunicaciones que las harán más eficientes, controlables y confiables.

Dentro de una Auditoría a Centros de Cómputo y Telecomunicaciones se evalúa principalmente lo siguiente, aunque pueden existir variaciones:

Controles generales administrativos

- Estructura Organizacional.
- Políticas y procedimientos.
- Descripción de puestos.
- Segregación de funciones.
- Vacaciones y Tiempo extra.
- Pólizas de seguro de equipos.
- Informes gerenciales.
- Inventario de equipos y recursos de cómputo y telecomunicaciones.
- Actualización e inventario de manuales de operación y de los sistemas.

Seguridad Física

- Controles de acceso, permanencia y salida de las instalaciones.
- Áreas de acceso restringido.
- Dispositivos de acceso magnético y códigos de acceso.
- Circuito cerrado de T.V.
- Riesgos naturales y provocados.

- Sistema contra incendios.
- Planta de energía e iluminación de emergencia.
- Reguladores y equipos de energía ininterrumpible (No-Break).

Controles generales del Ambiente Operativo de Cómputo

- Planes y calendarios de producción de cómputo.
- Bitácoras o registros de actividades.
- Bitácora automática del equipo (Log).
- Manejo de estadísticas.
- Catálogo de firmas para validar: instrucciones especiales, solicitudes de reprocesos, entrega de reportes, cambios en la producción, etc.
- Control de archivos en cintas, cartuchos y disquetes.
- Procedimientos y controles en microfichas.
- Almacenamiento de papel seguridad.
- Procedimientos y controles en el Area de Captura.

Seguridad y Continuidad de la Operación de Cómputo

- Equipos de respaldo.
- Tableros de control.
- Aire acondicionado.

- Manuales e instructivos de equipos de respaldo.
- Termómetro e hidrógrafo.

Administración de Seguridad de la Información

- Manuales de políticas y procedimientos de Seguridad de la Información.
- Destrucción de listados con información confidencial.
- Perfiles de Usuario y Claves de Usuario.
- Controles de los mantenimientos de los Sistemas de producción.
- Control de Archivos y Bibliotecas de los Sistemas de Aplicación.

Seguridad y Continuidad de Telecomunicaciones

- Políticas y procedimientos de la administración y operación del Área de Telecomunicaciones.
- Seguridad física de instalaciones y equipos fuera del Centro de Cómputo.
- Inventario de equipos y suministros de telecomunicaciones.
- Medios y apoyos alternos para uso y monitoreo de las Telecomunicaciones.
- Administración de Telecomunicaciones.
- Switcheo y equipos de respaldo.
- Atención de fallas, errores y elaboración de estadísticas.

- Relación entre Centro de Cómputo y Area de Telecomunicaciones, física y lógicamente.

Control de Desarrollo y Mantenimiento de Sistemas

- Metodología de Desarrollo de Sistemas.
- Procedimientos para el registro e implantación de cambios en los sistemas de producción.
- Mantenimientos correctivos.
- Pruebas de funcionamiento de los sistemas.
- Control de reprocesos.
- Mantenimientos programados.

Plan de Contingencias

- Procedimiento actualizado de acciones a seguir en caso de interrupción de la operación de cómputo.
- Áreas involucradas en el procedimiento y personal responsable.
- Nivel de conocimiento del plan de contingencias de las áreas involucradas.
- Realización periódica de los respaldos.
- Controles y cumplimiento de traslado de archivos a sitios alternos.
- Suministros de papelería y consumibles utilizados por las aplicaciones.

Controles generales de Centros de Cómputo y Telecomunicaciones

La definición de los siguientes controles y el desarrollo del detalle de éstos deben existir dentro de cualquier organización dentro del ambiente de cómputo y telecomunicaciones.

Controles de Desarrollo y Mantenimiento de Sistemas.- Es importante asegurarse de la integridad de los sistemas de aplicación del negocio y que exista un estándar del Ciclo de Vida del Desarrollo de Sistemas (CVDS), así como de la utilización de una metodología.

Involucrar al usuario, asistencia técnica, pruebas adecuadas de funcionamiento y procedimientos de documentación y transferencia deberán ser establecidos para soportar un ambiente de desarrollo y mantenimiento de sistemas controlado.

Controles de Seguridad de la Información y de Acceso.- La Seguridad de la Información es una de las áreas de más alto riesgo y por lo cual deben establecerse controles bien definidos.

Operaciones de Cómputo.- El control de las operaciones de cómputo asegura el cumplimiento de los procedimientos de operación. Es importante valorar y balancear los controles establecidos contra el funcionamiento del equipo, para que éstos no se contrapongan.

Telecomunicaciones.- Dado que las telecomunicaciones han empezado a ser más integrales, accesibles y complejas, se ha incrementado substancialmente la evaluación de los controles de éstas.

La tecnología en este campo ha evolucionado de manera significativa por lo que su flexibilidad, variantes y expansión imponen introducir nuevos requerimientos de control, que se verán a detalle en el siguiente capítulo.

Planes de Contingencia.- La gran mayoría de las organizaciones hoy en día dependen de los Sistemas de Información (SI) y de las telecomunicaciones, y no sobrevivirían en caso de una pérdida total o significativa de éstas.

El establecer planes de contingencia es una labor muy ardua dentro de la Organización, ya que involucra personal responsable y capacitado, así como una gran cantidad de recursos de todo tipo.

Ponderar las Áreas de Auditoría Informática

El grupo de Auditoría Informática tiene una apreciación diferente de las actividades computarizadas y los sistemas aplicativos en producción. El objetivo de un grupo de Auditoría Informática es revisar lo adecuado y la efectividad de estas actividades y aplicaciones. Las actividades de un área de Sistemas podrán ser divididas dentro de cuatro áreas, que son:

- *Auditoría a los sistemas en producción.*- Comprende la evaluación de los controles internos y la seguridad, completés, y autorización de los datos dentro de los sistemas y aplicaciones computarizadas.

- *Auditoría como soporte.*- La asistencia técnica y el desarrollo de apoyos computacionales proveídos a áreas de auditoría tradicional, dentro de la Organización.

- *Auditoría a la infraestructura.*- Comprende la revisión de las actividades necesarias para soportar el desarrollo y operación de los sistemas y aplicaciones computarizadas, tales como sistemas operativos, sistemas administradores de bases de datos, redes de comunicación, aspectos de seguridad, etc.

- *Auditoría a sistemas en desarrollo.*- Comprende la evaluación de los controles en los sistemas que se encuentran en desarrollo.

Algunos grupos de Auditoría Informática están involucrados en algunas de todas estas áreas. Algunos otros grupos su único objetivo es dar apoyo técnico a las demás áreas de Auditoría. Solamente en las grandes organizaciones, el grupo de Auditoría Informática está involucrado en las cuatro áreas.

El grupo de trabajo deberá de darle un puntaje a cada una de las áreas, para identificar a la más importante para que sea incluida dentro del esquema de actuación de la función del grupo de Auditoría Informática. Los miembros del grupo de trabajo deberán de estar

familiarizados con auditoría para ejecutar adecuadamente su tarea. Primero se le deberá de explicar al grupo de trabajo el concepto de dar puntajes a las áreas. Sólo después de que las áreas fueron entendidas, las hojas de puntajes deberán de ser llenadas por el grupo de trabajo.

Hojas de trabajo para clasificar la importancia de las áreas de auditoría

Cada miembro de la fuerza de trabajo deberá ponderar la importancia de cada categoría de área auditable para el involucramiento de Auditoría Informática. Esta ponderación provee al auditor en informática la guía para distribuir el tiempo de auditoría por categoría, tal como en el desarrollo de sistemas. Estas hojas de trabajo a ser llenadas, serán ilustradas en el Anexo A. Cada hoja de trabajo aplica a cada una de las cuatro áreas de auditoría. Las hojas de trabajo serán usadas para ponderar áreas individuales, tales como pistas de auditoría.

Las hojas de trabajo proveerán la capacidad para la ponderación a dos niveles. Un nivel es la importancia que da a una de las cuatro categorías de involucramiento de auditoría en relación con las otras tres categorías de involucramiento. El segundo nivel es la importancia de un área de auditoría específica.

El factor de calificación le provee a la organización una pérdida de la flexibilidad en la priorización de la importancia de las áreas de auditoría. Por ejemplo, la ponderación primero clasifica la importancia de las cuatro áreas de auditoría (esto es, sistemas aplicativos, auditoría como soporte, auditoría a la infraestructura y auditoría a los

sistemas en desarrollo). Si la estimación cree que Auditoría Informática deberá concentrar sus esfuerzos en el desarrollo de sistemas, deberán de ser excluidas las otras tres áreas de involucramiento de auditoría, esto puede ser indicado usando la categorización de los factores de peso. El segundo nivel de calificación es usando la clasificación de las áreas individuales de auditoría. Esta clasificación indica la importancia de las áreas individuales de auditoría dentro de una categoría de áreas auditables. Por ejemplo, dentro de la auditoría a los sistemas aplicativos la ponderación podrá distinguir entre la importancia del involucramiento de auditoría en tales áreas de auditoría como el control interno, documentación, pistas de auditoría, etc., usando los factores de calificación de las áreas de auditoría.

Factores de calificación de las categorías de las áreas de involucramiento de auditoría

Los factores de la calificación de las categorías son usados para diferenciar la importancia de las cuatro categorías de las áreas de involucramiento de auditoría. La calificación asignada por la ponderación deberá ser una de los siguientes:

Calificación	Significado	Explicación
3	Prioridad muy alta	Tres veces más importante que los de baja prioridad.
2	Prioridad promédio	Dos veces más importante que los de baja prioridad.
1	Baja prioridad	Objetivo o área de más baja prioridad.

Por ejemplo, si a la categoría de participación de auditoría en desarrollo de sistemas le es dado una calificación de 3 y al factor de soporte se le da una calificación de 1, entonces la ponderación indica que el involucramiento de auditoría en el desarrollo de sistemas es tres veces más importante que proveer soporte a los auditores no informáticos.

Después que cada categoría es ponderada, la calificación (1, 2 o 3) deberá ser colocada en la columna de "categoría de calificación" a continuación de cada área de auditoría. Esta clasificación podrá multiplicar los factores de ponderación para calcular el puntaje de cada área de auditoría.

Factores de ponderación de la importancia de cada área de auditoría

El puntaje le permite clasificar la ponderación de la importancia de cada área de auditoría. El puntaje del área de auditoría le permitirá desatenderse del factor de calificación asignado a la categoría en la cuál un área individual cae. Por ejemplo, si una categoría de involucramiento, tal como una auditoría a una instalación, es clasificada como "de muy alta prioridad", todas las demás áreas de auditoría dentro de la categoría deberán ser clasificadas como no muy importantes, de acuerdo a su nivel de importancia comparada contra las otras áreas de auditoría dentro de la categoría.

El puntaje le permita clasificar cada área de auditoría en cada categoría, usando uno de los siguientes puntajes:

Calificación	Significado	Explicación
6	Muy importante	La clasificación más alta de importancia a ser asignada a un área de auditoría.
4	Importante	El área auditable requiere una rápida intervención de Auditoría.
3	Importante, pero no crítico en tiempo	El área no requiere de una atención inmediata, pero deberá ser atendida cuando las auditorías muy importantes y las importantes han sido atendidas.
2	No importante	Un área auditable de relativo bajo riesgo o que está siendo atendida por otro grupo de auditoría.
1	Realmente sin importancia	Un área auditable que no deberá ser considerada por la función de Auditoría Informática.

Objetivos del puntaje y de la clasificación

Después de que las categorías de auditoría han sido explicadas al grupo de trabajo, deberán primero asignar un factor de calificación a cada categoría de área auditable, y entonces asignar un factor de calificación a cada área auditable individual, dentro de las categorías de auditoría. Cuando esto ha sido hecho, a cada área auditable le es dado un puntaje matemáticamente.

El proceso para darle puntajes a las áreas auditables es un proceso matemático. La calificación de la categoría es multiplicada por la clasificación del área auditable, obteniendo un puntaje para cada área auditable. Por ejemplo, una calificación de 2 (prioridad promedio) veces con un puntaje importante, podrá resultar en un puntaje de área auditable por el orden de 8 (esto es, prioridad 2 X clasificación del área auditable 4 = 8).

El puntaje para cada una de las áreas auditables deberá ser calculado y registrado en la hoja de trabajo, dependiendo de la categoría del área auditable (Anexo A). El puntaje obtenido dentro de cada clasificación deberá ser transcrito a la tabla del Anexo B (Hoja de trabajo de la priorización para las áreas auditables para Auditoría Informática). Esta hoja de trabajo tiene columnas para los puntajes hasta para seis promedios individuales. Si más de seis gentes están involucradas en el grupo de trabajo, dos o más de estas hojas de trabajo serán necesarias.

Después de que el puntaje de todos los promedios han sido transcritos a la Hoja de trabajo para la priorización de las áreas auditables para Auditoría Informática, la clasificación de las áreas auditables podrá empezar. El primer paso es sumar todos los puntajes individuales para cada área auditable y el resultado colocarlo en la columna de puntaje total para esa área auditable. A continuación las áreas auditables deberán ser clasificadas del 1 al 28, poniendo el número 1 en la parte alta de la tabla, a continuación el dos, y así sucesivamente hasta el nivel 28, quedando así todas las áreas auditables ya clasificadas.

Una vez que todas las áreas auditables han recibido sus puntajes y han sido clasificadas, el trabajo del grupo de trabajo ha terminado. El ejercicio del grupo de trabajo puede resultar en que se le provee al grupo de Auditoría Informática un panorama de las 28 áreas auditables, así como la importancia de la categoría de las áreas auditables. A continuación el grupo de Auditoría Informática deberá emplear su juicio acerca de la clasificación, para poder obtener el esquema de actuación de Auditoría Informática.
Cuando el grupo de trabajo ha llenado estas cuatro hojas de trabajo (Anexo A), su parte en la definición de la función de Auditoría Informática ha terminado. El grupo de trabajo será desarticulado, cada uno de sus miembros deberá estar plenamente consciente de su ayuda. El grupo de auditores en informática podrán llamar posteriormente a los integrantes del grupo de trabajo para revisar los resultados del proceso de asignación de puntajes y de la clasificación. Ahora, la gerencia de Auditoría Informática estará en condiciones de explicar porqué un área auditable podrán ser o no ser incluida en el esquema de actuación de Auditoría Informática. Este reinvolucramiento del grupo de

trabajo será muy benéfico en la construcción de un soporte continuo para el grupo de Auditoría Informática y para las áreas auditables involucradas y no involucradas.

Aplicar los juicios para realizar la clasificación

La información sugerida por el grupo de trabajo deberá ser usada como una sugerencia y no como un requerimiento obligatorio. Esto es por que el sistema de clasificación es sujeto de los siguientes errores:

- ✓ *Errores de procesión.*- Por forzar porcentajes para categorizar su clasificación, el proceso puede mostrar precisión que no es representativa del promedio exacto. Por ejemplo, la diferencia entre un factor de calificación de 3 y 2 trae consigo una consideración significativa. Sin embargo, en la mente del que realiza la calificación, la diferencia matemática puede ser mayor que lo que realmente se espera.
- ✓ *Errores de la fuerza de trabajo.*- La compensación del grupo de trabajo puede afectar significativamente la calificación total. Por ejemplo, en un grupo de trabajo de 6 personas si tres son usuarios directos de las aplicaciones, su influencia en la clasificación final puede ser muy alta.
- ✓ *Errores mecánicos.*- Al realizar los promedios se pueden realizar errores involuntarios de juicio o de registro cuando estamos llenando las hojas de trabajo. Por lo tanto, el resultado no podrá reflejar el estado actual.

El puntaje matemático le provee al grupo de Auditoría Informática consejos respaldados matemáticamente del nivel de conocimientos del grupo. Estas recomendaciones no deberán de ser tomadas por el grupo de Auditoría Informática, sin embargo, el promedio,

deberá ser usado como la base en la cual la planeación de auditoría y el esquema de actuación serán desarrollados.

Diferencias significativas en los puntajes denotan confianza para tomar decisiones acerca de las pequeñas diferencias. Por ejemplo el puntaje para cualquier área puede andar entre el rango de 1 a 15. Si un objetivo fue clasificado en 3 y otro en 12, esto puede ser claramente evidente que el promedio considera más fuertemente el objetivo marcado con 12, que es mucho más importante que el marcado con 3. Por otra parte si un objetivo es clasificado con un 9 y otro es clasificado con un 10, la diferencia puede no ser significativa, esta clasificación final le permite calificar los factores tales como riesgo potencial, crecimiento a futuro de un área, etc. para ser introducido en la clasificación. El juicio final del auditor es el que será usado en el desarrollo del esquema de actuación del grupo de Auditoría Informática.

Áreas de involucramiento de Auditoría Informática

Un ejemplo de las áreas de involucramiento de Auditoría Informática, son mostradas y explicadas en el cuadro siguiente:

- Procedimientos, estándares y regulaciones.
- Controles internos.
- Datos.
- Documentaciones.
- Pistas de Auditoría.
- Operación del sistema en producción.
- Necesidades de los usuarios.

Auditoría a los sistemas en producción
➢ Consejos técnicos.
➢ Extracción de reportes.
➢ Entrenamiento técnico.
➢ Guías de auditoría.
➢ Apoyo en la dirección de auditorías.
➢ Controles administrativos.
➢ Operaciones computacionales.
➢ Controles en el hardware.
➢ Controles en los sistemas operativos y en el software.
➢ Selección del software y hardware.
➢ Estándares, políticas, procedimientos y convenciones.
➢ Seguimiento de errores.
➢ Seguridad y privacía.
➢ Planes de contingencias / respaldos / recuperaciones.
➢ Procedimientos, estándares y regulaciones.
➢ Controles internos.
➢ Documentaciones.
➢ Pistas de Auditoría.
➢ Aspectos operacionales.
➢ Necesidades de los usuarios.
➢ Conversión de datos.

Auditoría a los sistemas en producción

Un sistema aplicativo es aquel que procesa los datos de la Organización. Ejemplo, nómina, cuentas por pagar, contabilidad, inventarios, depósitos bancarios, etc. El alcance de las aplicaciones varía. En algunos casos un alcance muy amplio es usado, tal como en la aplicación de ingresos que puede incluir facturación, cuentas por cobrar, crédito a

clientes, y recepción de efectivo. En otros casos, una aplicación puede ser definida usando un alcance muy estrecho, tal como en el caso de recepción de efectivo.

Un área auditable es una actividad, procedimiento o control que un auditor puede revisar durante el proceso de auditoría. Las áreas auditables por el grupo de Auditoria Informática, comprenden las siguientes:

- Procedimientos, estándares y regulaciones

  Las organizaciones establecen procedimientos y estándares que rigen el procesamiento de las transacciones y los métodos por los cuales las aplicaciones son construidas y operadas. Los procedimientos y estándares que rigen las transacciones financieras son normalmente desarrollados por la Contraloría de la Organización. Los estándares y procedimientos que rigen la construcción de las aplicaciones son normalmente preparadas por el departamento de procesamiento de datos. Adicionalmente el gobierno emite leyes y las agencias gubernamentales publican las relacionadas con las sistemas aplicativos. Por ejemplo: las regulaciones para manejar las aplicaciones bancarias.

- Controles internos

  Un adecuado sistema de control interno dentro de las aplicaciones computarizadas, rige el registro, procesamiento, almacenamiento y generación de salidas de los datos. La evaluación deberá revisar tanto los controles manuales como los automatizados. La evaluación deberá de tener dos propósitos: el primero, para determinar si existe cualquier debilidad de control dentro del sistema;

segundo, determinar si el auditor puede confiar en lo adecuado de los controles internos, de acuerdo con los límites y alcances de las pruebas realizadas.

- Datos

Las transacciones metidas, procesadas, almacenadas y generadas como salida de los sistemas computacionales deberán ser revisadas. El objetivo de la revisión de las transacciones de datos es para determinar que los datos están seguros, completos y autorizados. El alcance de la prueba de datos dependerá del nivel de confianza que el auditor le de a los controles internos. Entre mayor confianza le de a los controles, el alcance y el tiempo destinado a la realización de las pruebas será menor.

- Documentación

La auditoría a la documentación de los sistemas computarizados tendrá dos propósitos: primero, determinar si la documentación existe para los diferentes sistemas y usuarios; segundo, averiguar si la documentación está completa, es segura y está actualizada. Los usuarios del sistema incluirán a los auditores, programadores, personal de sistemas, operadores de cómputo, usuarios de datos, gente que prepara los datos para su captura y todo el personal de control. Si existen estándares de programación dentro de la organización, la auditoría a la documentación podrá verificar el nivel de cumplimiento de los estándares. Sin embargo, sin un estándar adecuado de documentación, será más difícil para el auditor poder evaluar las documentaciones correctamente.

- **Pistas de Auditoría**

  Las pistas de Auditoría proveen la evidencia que permite que las transacciones sean rastreadas, como por ejemplo de un registro contable hacia el registro fuente y desde el registro fuente hasta un registro contable. Las pistas de auditoría también pueden ser usadas como una ayuda en la recuperación de las transacciones de una aplicación, en caso de que la integridad de los datos de la aplicación esté perdida. Tener pistas de auditoría con el flujo hacia adelante y hacia atrás de las transacciones, podrá ayudar a alcanzar diferentes objetivos de auditoría. Por ejemplo, si el auditor está buscando operaciones que no sean registradas en la contabilidad general de la organización, deberá buscar en el flujo que parte de la transacción y termina en la contabilidad general, por el contrario, si el auditor está buscando el sobreregistro en la contabilidad, deberá buscar desde las cifras control y terminar en las transacciones que soportan dichos movimientos.

- **Operación del sistema en producción**

  Los auditores revisarán la efectividad, la economía y eficiencia operacional de las aplicaciones computarizadas. La efectividad es la mezcla de los esfuerzos entre la gente, el computador, el hardware y el software. La eficiencia es lo fácil en que dicho trabajo puede ser ejecutado. Lo económico se deriva del costo - beneficio recibido del procesamiento. Normalmente se requiere un amplio conocimiento del negocio para poder conducir las auditorías a la parte operacional de las aplicaciones.

- Las necesidades de los usuarios

  A menos que las necesidades de los usuarios sean conocidas, el desempeño operacional y el cumplimiento de las políticas será de poca importancia. Un estudio realizado por la The United States General Accounting Office (Oficina de Contabilidad General de los Estados Unidos) demostró que los sistemas desarrollados generalmente no contemplan los objetivos de los usuarios.

Auditoría como soporte a las demás áreas de auditoría

Los auditores no informáticos frecuentemente requieren soporte técnico cuando auditan aplicaciones computarizadas. Los estándares del campo de trabajo, requieren que los auditores estén adecuadamente calificados para realizar la auditoría que están dirigiendo. En una auditoría a una aplicación computarizada, se requieren conocimientos de computación. La competencia técnica está relacionada con la competencia del equipo de Auditoría. Cuando los auditores no informáticos requieren del apoyo de Auditoría Informática para realizar una revisión a un sistema computarizado, el equipo formado por ambos grupos de auditores deberá tener la competencia necesaria. Un objetivo a largo plazo deberá ser que todo el grupo de auditores deberán ser técnicamente competentes en aspectos de procesamiento electrónico de datos.

El soporte técnico podrá abarcar desde la respuesta a pequeñas preguntas técnicas, el desarrollo de apoyos computacionales, hasta la realización de la parte técnica de la auditoría. Por ejemplo, un auditor no informático le puede preguntar a los auditores informáticos como realizar la revisión de una aplicación computarizada, mientras que en

otro caso, el auditor no informático desea conocer algunos aspectos y características técnicas del hardware de la computadora.

Cuando trabajamos como soporte técnico, normalmente el auditor no informático es quien inicia el requerimiento para dicho soporte. De esta forma el auditor informático operará como uno más de los miembros del equipo de trabajo, proveyendo los juicios técnicos correspondientes.

Los objetivos específicos incluidos en el soporte técnico, son:

- Consejo técnico

  El auditor informático provee los aspectos técnicos tanto en el aspecto de computación como en el aspecto de auditoria para las aplicaciones computarizadas. El auditor en informática puede ayudarle al auditor tradicional en el diseño del programa de auditoría, identificando los riesgos nuevos o los que se han incrementado en el medio ambiente computacional. Por lo tanto, el auditor informático podrá sugerir las herramientas, técnicas y enfoques que considere efectivos para ser usados durante la revisión.

- Extracción de reportes

  El auditor en informática desarrollará los programas computacionales para producir los reportes necesarios para efectos de auditoría. Estos programas pueden ser construidos usando un software generalizado de auditoría, Queries u otros lenguajes de programación, tal como el COBOL. Algunas veces el auditor no informático podrá especificar los métodos de extracción de la información, pero por

lo general el auditor tradicional necesita asistencia para conocer qué es lo que se tiene disponible y cómo recuperarlo. Normalmente el auditor informático le indicará al auditor tradicional como leer y usar la información contenida en los reportes extraídos. Muchos de los paquetes de auditoría de uso generalizado contienen rutinas estadísticas disponibles, por medio de las cuales el auditor tradicional podrá obtener ejemplos válidos.

- Entrenamiento técnico

  El auditor en Informática deberá participar como una ayuda para incrementar el nivel de conocimientos técnicos del personal de auditores tradicionales. Este entrenamiento deberá de ser llevada a cabo a través de uno o de todos los métodos siguientes:

  - Seleccionando y obteniendo publicaciones técnicas y manuales.
  - Seleccionando seminarios, conferencias y clases de informática para los auditores tradicionales.
  - Desarrollar y conducir sesiones de entrenamiento informático, para los auditores tradicionales.
  - Desarrollar y conducir sesiones de entrenamiento técnico en el uso de las computadores y de las ayudas informáticas.
  - Criticar las auditorías terminadas, para proveer una guía de cuáles auditorías a los sistemas en producción podrán mejorarse la próxima vez que se realice.

- Guías de auditoría

El auditor de informática podrá desarrollar guías de auditoría para revisar aplicaciones computacionales. Esto es hecho frecuente cuando hay muchas auditorías similares. Por ejemplo, las auditorías a los distritos de ventas, a los centros de distribución, a las aplicaciones bancarias, a las aplicaciones de agencias de seguros, etc. El auditor en informática provee guías para realizar auditorías paso a paso, junto con las instrucciones de como obtener la información necesaria de las aplicaciones computacionales. La guía normalmente incluye el desarrollo y escritura de programas de software necesarios para proveer la información necesaria para propósitos de auditoría, junto con las instrucciones de como usar dicha información.

- Apoyo en la dirección de auditorías

El auditor en informática podrá conducir una o más partes de una auditoría bajo la dirección de la auditoría tradicional. Esto es normalmente hecho cuando el auditor a cargo de la auditoría no tienen dentro de su grupo de auditores ningún miembro con los conocimientos y habilidades técnicas necesarias para conducir esa parte de la auditoría. Las dos tareas más comunes asignadas a los auditores en informática son las revisión preliminar de todas las aplicaciones importantes desde el punto de vista financiero para la organización, y segundo para evaluar lo adecuado de los controles internos en una instalación informática o en una aplicación computarizada. Por ejemplo el auditor a cargo podrá buscar conocer que aplicaciones son las de más alto riesgo o podrá buscar que el auditor en informática revise los controles del centro de cómputo.

Auditoría a la Infraestructura

Las instalaciones computacionales es donde los sistemas son normalmente desarrollados, implementados, operados y mantenidos. El desarrollo de estas tareas deberá de ser controlado. La revisión de los controles y procedimientos que gobiernan estas tareas normalmente requieren de habilidades en informática y son generalmente realizadas por los auditores en informática.

Los sistemas computarizados pueden ser divididos en dos partes. Estas partes son: (a) los sistemas aplicativos en producción, y (b) los sistemas operativos y todos los sistemas relacionados con el software. Anteriormente se trataron los sistemas aplicativos en producción. El término sistema operativo es usado para denotar los paquetes y software proveído por los proveedores, usado para correr los sistemas aplicativos en producción dentro del computador. En algunos computadores, ningún programa podrá correr sin la interface con el sistema operativo. Ejemplos de software proveído por los proveedores incluyen los sistemas de seguridad, los sistemas de comunicaciones, los sistemas administradores de bases de datos, etc.

Dentro de los paquetes proveídos por los proveedores se encuentran muchos de los controles que aseguran procesos seguros, completos y autorizados. Por ejemplo, estos sistemas ofrecen controles de seguridad que restringe quién puede obtener acceso a los datos.

Los vendedores de estos sistemas pueden construir los controles opcionales necesarios. Adicionalmente, estos proveedores entregan manuales y otros materiales que enseña a los usuarios cómo usar estos controles. Sin embargo, muchos de estos controles son discrecionales y no necesariamente deberán de ser usados si la organización decide no hacer uso de ellos. Por ejemplo, los passwords son un control opcional distribuido dentro de los paquetes del proveedor.

Adicionalmente las opciones de control automatizados proveídas por los proveedores, aún son orientadas al personal. El hardware y el software son generados, operados y supervisados por la gente. Las guías, estándares y procedimientos gobiernan el alcance y la operación de estas actividades realizadas por el personal.

La operación técnica de una computadora deberá de ser revisada por auditores con las habilidades técnicas necesarias. Mientras los auditores no informáticos pueden auditar aplicaciones computarizadas con las ayuda de los auditores en informática, la auditoría a la tecnología computacional será mejor desarrollada por auditores en informática. Esto es necesario para asegurar que las debilidades de control significativas podrán ser adecuadamente interpretadas.

Las áreas auditables para revisar las instalaciones computaciones, incluyen:

- Controles administrativos

  Los controles administrativos gobiernan el medio ambiente en el cual las transacciones son procesadas. Estos incluyen la estructura organizacional, los

procedimientos de desarrollo de sistemas, los procedimientos para calendarización de trabajos, los procedimientos para reportar estátus, procedimientos de selección de hardware y software, los procedimientos para control de cambios y los procedimientos para aprobación de proyectos. Los controles administrativos representan la filosofía de control de la Dirección General.

- Operaciones computacionales

La operación exitosa del computador requiere de gente competente, con habilidades suficientes y procedimientos estandarizados de operación. La función de operación normal del computador incluye el diseño y operación de un cuarto de computadoras; de un almacén de medios magnéticos, tanto dentro del centro de cómputo, como fuera de las instalaciones de la organización; el ordenar, almacenar y distribuir los consumibles de cómputo, tales como papel, cintas de impresora, toner, etc.; desarrollar y probar planes en casos de desastres; proveer las facilidades, procedimientos y entrenamiento para el personal de operación; realización de respaldos / recuperaciones; seguridad física en el cuarto de computadoras; y la contratación, entrenamiento y supervisión del personal de operación. En muchas organizaciones, el área de operación es responsable de la preparación de los datos de entrada a las aplicaciones, del control sobre el procesamiento y distribución de las salidas generadas.

- Controles en el hardware

Los controles de hardware son circuitos especialmente construidos dentro de las computadoras, en sus equipos periféricos, o adicionado a otros equipos fuera de

línea, tales como grabadoras de datos, etc. para asegurar la función adecuadamente. Los controles en el hardware también incluyen los mantenimientos preventivos y de emergencia, el monitoreo de la eficiencia operacional del hardware, el monitoreo que nos asegure que la capacidad existente es suficiente para alcanzar las necesidades de la organización.

- Controles en los sistemas operativos y en el software

  Los controles en el software del sistema incluyen los controles opcionales y mandatorios incluidos en la paquetería proporcionada por el proveedor. Estos controles son necesarios para operar y soportar las aplicaciones del negocio interconectadas con el software de sistemas. Los controles incluyen manuales, entrenamiento y mantenimiento por parte del proveedor a los paquetes de software. Adicionalmente los controles incluyen el monitoreo de la eficiencia del software para determinar si está funcionando apropiadamente. Los procedimientos deberán ser establecidos para determinar qué controles, de toda la gama de controles proporcionada por el proveedor, serán seleccionados. Desafortunadamente, esta selección de los controles es delegada en los System Programmers.

- Selección del software y hardware

  La selección del hardware y del software está en un proceso continuo de emparejamiento entre las facilidades computacionales y las necesidades de capacidad de la organización. Este proceso de selección es un proceso complejo debido a la multiplicidad de opciones disponibles. Las grandes organizaciones

frecuentemente asignan gente de tiempo completo para la evaluación de las opciones.

Las organizaciones pequeñas confían más ampliamente en los servicios de análisis de hardware y de software, o en consultores tales como Auditoría Informática. La responsabilidad de la selección del hardware y del software deberá incluir también la determinación de cuándo un paquete de software deberá cambiar a una nueva versión o cuándo será necesario aumentar la capacidad de almacenamiento o la velocidad de procesamiento del hardware.

- Estándares, políticas, procedimientos y convenciones

Los estándares, políticas, procedimientos y convenciones establecen los métodos por medio de los cuales el personal de sistemas deberá utilizar las facilidades de cómputo. Estos rigen todos los aspectos de la operación del computador. Los ejemplos incluyen los estándares de lenguajes de programación, el ciclo de vida de desarrollo de sistemas, los estándares para definición de datos, los estándares de documentación, los estándares de la operación del computador, los estándares para la retención de los datos, los análisis de riesgos, los estándares para diagramación, los estándares para la realización de pruebas, etc. Si los estándares, procedimientos, políticas, etc. son efectivos, la función de procesamiento de datos necesita un mecanismo que haga cumplir estos estándares, en beneficio de la auditoría. En algunas organizaciones, esta función es delegada a la función de Aseguramiento de la Calidad.

- **Seguimiento de errores**

  El seguimiento de errores es una función que le consume tiempo al personal de informática. El seguimiento de errores normalmente es parte del trabajo del personal de sistemas, de programación o de los system programmers o del personal responsable de las actividades del sistema donde está ocurriendo el error. Tener un grupo separado que realice las funciones de seguimiento de errores, ayudará a la segregación de funciones dentro de las funciones de sistemas. Recientemente algunas organizaciones han comenzado a asignarle la responsabilidad de seguimiento de errores en los sistemas en producción a una función staff. En muchas otras organizaciones esta función es responsabilidad del grupo de Aseguramiento de la Calidad. El objetivo de tener centralizada esta función es evaluar las implicaciones de dicho error en las demás aplicaciones, también como transmitir ese conocimiento a otras áreas interesadas o involucradas.

- Seguridad y privacía

  La seguridad y privacía incluye tanto los aspectos físicos y lógicos de las operaciones computarizadas. La seguridad física es normalmente manejada por las operaciones computacionales y por la función de seguridad de la organización. Esto puede involucrar el uso de equipo sofisticado y así el Auditor en Informática podrá estar disponible para contribuir de manera limitada en la revisión de estos controles. La principal contribución puede ser la habilidad para identificar las áreas de riesgo. La seguridad lógica protege la información durante su procesamiento, comunicación y almacenamiento dentro del computador. La revisión de la

seguridad lógica raramente recibe una atención suficiente. Esto es porque las implicaciones de seguridad del software de sistemas, como el sistema operativo, pueden no ser realmente conocidas. La seguridad lógica incluye la prevención de la destrucción o cambios accidentales también contra la manipulación intencional de los datos. Los sistemas interactivos de bases de datos normalmente poseen una mayor seguridad y privacía contra las amenazas que los sistemas batch, lo que requiere un mayor esfuerzo por parte de auditoría.

- Planes de contingencias / respaldos / recuperaciones

  Los planes de contingencia proveen de medios alternos de recuperación en caso de que la fuente primaria de las operaciones se pierda. Los planes de contingencia deberán ser preparados para eventos tales como fallas de energía eléctrica, malfuncionamientos del hardware y del software, fuego, inundaciones, fallas en general, etc. El plan de contingencias deberá incluir las provisiones para respaldar datos; el almacenamiento de datos, programas y procedimientos fuera del centro de cómputo, también deberá prever la forma en cómo la organización trabajará mientras la aplicación es restablecida.

Auditoría a los sistemas en desarrollo

El proceso de desarrollo de sistemas incluye la construcción y mantenimiento de aplicaciones computarizadas. Los pasos y procedimientos que rigen este proceso normalmente son incluidos dentro de los procedimientos del ciclo de vida de desarrollo de sistemas definido por la organización (aunque no todas las organizaciones tienen dicho ciclo de vida de desarrollo de sistemas). El ciclo de vida de desarrollo de sistemas divide

el proceso de desarrollo en etapas. Las etapas más comunes incluyen el estudio de factibilidad, el diseño de sistemas, la programación, la realización de pruebas, la conversión de datos, la operación de la aplicación y el mantenimiento.

Muchas organizaciones gastan mucho esfuerzo de programación y de sistemas en el mantenimiento de los sistemas existentes, en lugar que en el desarrollo de nuevas aplicaciones. Sin embargo muchos mantenimientos de crecimiento incluyen los mismos pasos que pueden ser incluidos en el desarrollo de nuevos sistemas. Normalmente los mantenimientos de emergencia son los que rompen los procedimientos del ciclo de desarrollo de sistemas.

Las áreas de involucramiento para el desarrollo de sistemas son similares a las aplicadas en los sistemas aplicativos en producción. Hay tres diferencias entre los sistemas aplicativos en producción y entre los sistemas en desarrollo. La primera es que en los sistemas aplicativos en producción se evalúa la forma en la que se está ejecutando la aplicación. Una auditoría a un sistema bajo desarrollo es diseñada para proveer una opinión de cómo el sistema se ejecutará en el futuro. La segunda diferencia es que en una auditoría a las aplicaciones en producción examina los datos procesados como base para realizar los juicios, mientras que en los sistemas en desarrollo no usan las transacciones de datos en vivo para realizar el análisis. La tercera, el sistema bajo desarrollo deberá pasar por un proceso de conversión de datos antes de que sea puesto en producción.

Esto puede requerir un tipo diferente de auditores para evaluar un sistema bajo desarrollo, debido a la orientación a futuro de las conclusiones de auditoría. Es normalmente seguro esbozar una conclusión basado en un evento histórico. Por otro lado, realizar un juicio basado en algo que aún no sucede deberá usar diferentes métodos y técnicas.

Las áreas de involucramiento de auditoría para los sistemas en desarrollo son las mismas que para los sistemas aplicativos en producción, con la sola excepción de que la auditoría a los datos no está incluida y la auditoría a la conversión de datos es adicionada. Las áreas comunes para ambos tipos de auditoría son descritos en la auditoría a los sistemas aplicativos en producción: A continuación se listarán las áreas de involucramiento que ya fueron explicadas anteriormente:

- Procedimientos, estándares y regulaciones.
- Controles internos.
- Documentaciones.
- Pistas de Auditoría.
- Aspectos operacionales (Eficiencia, economía efectividad).
- Necesidades de los usuarios.
- Conversión de datos

Nuevos sistemas necesitan pasar por un proceso de conversión de datos para liberarlos a producción. Este proceso puede incluir algunos o todos los pasos siguientes:

- Cambiar datos a un nuevo formato.
- Adicionar nuevos elementos de datos.
- Borrar viejos elementos de datos.

- Escribir nuevos procedimientos.
- Adicionar programas a las bibliotecas de producción.
- Modificar procedimientos operativos.
- Entrenar al personal.
- Ordenar nuevas formas y consumibles.
- Ordenar nuevo hardware o software de sistemas.
- Avisar y entrenar a los usuarios.

El proceso de conversión no deberá de comenzar hasta que el sistema haya sido probado totalmente y que los objetivos hayan sido alcanzados.

2.2.- Normas y Principios Aplicables a los Auditores de los Sistemas de Información

La ISACA (Information Systems Audit and Control Association / Foundation), Asociación de Auditoría y Control de Sistemas de Información de los Estados Unidos de América ha determinado que la naturaleza especializada de la auditoría de los sistemas de información y las habilidades necesarias para llevar a cabo este tipo de auditorías, requieren el desarrollo y la promulgación de Normas Generales para la Auditoría de los Sistemas de Información.

La auditoría de los sistemas de información se define como cualquier auditoría que abarca la revisión y evaluación de todos los aspectos (o de cualquier porción de ellos) de los sistemas automáticos de procesamiento de la información, incluidos los procedimientos no automáticos relacionados con ellos y las interfaces correspondientes.

Las normas promulgadas por la Asociación de Auditoría y Control de Sistemas de Información son aplicables al trabajo de auditoría realizado por miembros de la Asociación de Auditoría y Control de Sistemas de Información y por las personas que han recibido la designación de Auditor Certificado de Sistemas de Información.

Los objetivos de estas normas son los de informar a los auditores del nivel mínimo de rendimiento aceptable para satisfacer las responsabilidades profesionales establecidas en el Código de Ética Profesional y de informar a la gerencia y a otras partes interesadas de las expectativas de la profesión con respecto al trabajo de aquellos que la ejercen.

Normas generales para los sistemas de auditoría de la información

Título de auditoría

Responsabilidad, autoridad y rendimiento de cuentas. La responsabilidad, la autoridad y el rendimiento de cuentas abarcados por la función de auditoría de los sistemas de información se documentarán de la manera apropiada en un título de auditoría o carta de contratación.

Independencia

Independencia profesional. En todas las cuestiones relacionadas con la auditoría, el auditor de sistemas de información deberá ser independiente de la organización auditada tanto en actitud como en apariencia.

Relación organizativa. La función de auditoría de los sistemas de información deberá ser lo suficientemente independiente del área que se está auditando para permitir completar de manera objetiva la auditoría.

Ética y normas profesionales

Código de Ética Profesional. El auditor de sistemas de información deberá acatar el Código de Ética Profesional de la Asociación de Auditoría y Control de Sistemas de Información.

Atención profesional correspondiente. En todos los aspectos del trabajo del auditor de sistemas de información, se deberá ejercer la atención profesional correspondiente y el cumplimiento de las normas aplicables de auditoría profesional.

Idoneidad

Habilidades y conocimientos. El auditor de sistemas de información debe ser técnicamente idóneo, y tener las habilidades y los conocimientos necesarios para realizar el trabajo como auditor.

Educación profesional continua. El auditor de sistemas de información deberá mantener la idoneidad técnica por medio de la educación profesional continua correspondiente.

Planificación

Planificación de la auditoría. El auditor de sistemas de información deberá planificar el trabajo de auditoría de los sistemas de información para satisfacer los objetivos de la auditoría y para cumplir con las normas aplicables de auditoría profesional.

Ejecución del trabajo de auditoría

Supervisión. El personal de auditoría de los sistemas de información debe recibir la supervisión apropiada para proporcionar la garantía de que se cumpla con los objetivos de la auditoría y que se satisfagan las normas aplicables de auditoría profesional.

Evidencia. Durante el transcurso de una auditoría, el auditor de sistemas de información deberá obtener evidencia suficiente, confiable, relevante y útil para lograr de manera eficaz los objetivos de la auditoría. Los hallazgos y conclusiones de la auditoría se deberán apoyar por medio de un análisis e interpretación apropiados de dicha evidencia.

Informes

Contenido y formato de los informes. En el momento de completar el trabajo de auditoría, el auditor de sistemas de información deberá proporcionar un informe, de formato apropiado, a los destinatarios en cuestión. El informe de auditoría deberá enunciar el alcance, los objetivos, el período de cobertura y la naturaleza y amplitud del trabajo de auditoría realizado. El informe deberá identificar la organización, los destinatarios en cuestión y cualquier restricción con respecto a su circulación. El

informe deberá enunciar los hallazgos, las conclusiones y las recomendaciones, y cualquier reserva o consideración que tuviera el auditor con respecto a la auditoría.

Actividades de seguimiento

Seguimiento. El auditor de sistemas de información deberá solicitar y evaluar la información apropiada con respecto a hallazgos, conclusiones y recomendaciones relevantes anteriores para determinar si se han implementado las acciones apropiadas de manera oportuna.

Principios generales para los sistemas de auditoría de la información

El Código de Conducta de The British Computer Society, que establece los estándares profesionales de competencia, conducta y ética de la práctica informática en el Reino Unido, contiene los principios aplicables a los auditores, de los cuales algunos de ellos son mencionados brevemente a continuación:

Principio de beneficio del auditado

El auditor deberá ver cómo se puede conseguir la máxima eficacia y rentabilidad de los medios informáticos de la empresa auditada, estando obligado a presentar recomendaciones acerca del reforzamiento del sistema y el estudio de las soluciones más idóneas según los problemas detectados en el sistema informático de esta última, siempre y cuando las soluciones que se adopten no violen la ley ni los principios éticos.

Principio de calidad

El auditor deberá prestar sus servicios a tenor de las posibilidades de la ciencia y medios a su alcance con absoluta libertad con respecto a la utilización de dichos medios y en unas condiciones técnicas adecuadas para el idóneo cumplimiento de su labor. En caso en que la precariedad de medios puestos a su disposición impidan o dificulten seriamente la realización de la auditoría, deberá negarse a realizarla hasta que se le garantice un mínimo de condiciones técnicas que no comprometan la calidad de sus servicios o dictámenes.

Principio de capacidad

El auditor debe estar plenamente capacitado para la realización de la auditoría encomendada, sobretodo teniendo en cuenta que, en la mayoría de los casos, dada su especialización, a los auditados en algunos casos les puede ser extremadamente difícil verificar sus recomendaciones y evaluar correctamente la precisión de las mismas.

Principio de cautela

El auditor debe en todo momento ser consciente de que sus recomendaciones deben estar basadas en la experiencia contrastada que se le supone tiene adquirida, evitando que, por un exceso de vanidad, el auditado se embarque en proyectos de futuro fundamentados en simples intuiciones sobre la posible evolución de las nuevas tecnologías de la información.

Principio de comportamiento profesional

El auditor tanto en sus relaciones con el auditado como con terceras personas deberá, en todo momento, actuar conforme a las normas, implícitas o explícitas, de dignidad de la profesión y de corrección en el trato personal. Asimismo debe guardar un escrupuloso respeto por la política empresarial del auditado, aunque ésta difiera de las del resto del sector en las que desarrolla sus actividades, evitar comentarios extemporáneos sobre la misma en tanto no estén relacionados o afecten al objeto de la auditoría y analizar pormenorizadamente las innovaciones concretas puestas en marcha por el auditado a fin de determinar sus específicas ventajas y riesgos, eludiendo evaluarlas únicamente a tenor de los estándares medios del resto de empresas de su sector.

Principio de concentración en el trabajo

El auditor deberá evitar que un exceso de trabajo supere sus posibilidades de concentración y precisión en cada una de las tareas a él encomendadas, ya que la saturación y dispersión de trabajo suele a menudo, si no está debidamente controlada, provocar la conclusión de los mismos sin las debidas garantías de seguridad.

Principio de confianza

El auditor deberá facilitar e incrementar la confianza del auditado en base a una actuación de transparencia en su actividad profesional sin alardes científico-técnicos que, por su incomprensión, puedan restar credibilidad a los resultados obtenidos y a las directrices aconsejadas de actuación.

Principio de criterio propio

El auditor durante la ejecución de la auditoría deberá actuar con criterio propio y no permitir que éste esté subordinado al de otros profesionales, aún de reconocido prestigio, que no coincidan con el mismo.

Principio de discreción

El auditor deberá en todo momento mantener una cierta discreción en la divulgación de datos, aparentemente inocuos, que se le hayan puesto de manifiesto durante la ejecución de la auditoría.

Principio de economía

El auditor deberá proteger, en la medida de sus conocimientos, los derechos económicos del auditado evitando generar gastos innecesarios en el ejercicio de sus actividades. En las recomendaciones y conclusiones realizadas en base a su trabajo deberá asimismo eludir, incitar o proponer actuaciones que puedan generar gastos innecesarios o desproporcionados.

Principio de formación continua

Éste principio, íntimamente ligado al principio de capacidad y vinculado a la continua evolución de las tecnologías de la información y las metodologías relacionadas con las mismas, impone a los auditores el deber y la responsabilidad de mantener una permanente actualización de sus conocimientos y métodos a fin de adecuarlos a las necesidades de la demanda y a las exigencias de la competencia de la oferta.

Principio de fortalecimiento y respeto de la profesión

La defensa de los auditados pasa por el fortalecimiento de la profesión de los auditores informáticos, lo que exige un respeto por el ejercicio, globalmente considerado, de la actividad desarrollada por los mismos y un comportamiento acorde con lo requisistos exigibles para el idóneo cumplimiento de la finalidad de las auditorías.

Principio de independencia

Éste principio, muy relacionado con el principio de criterio propio, obliga al auditor, tanto si actúa como profesional externo o con dependencia laboral respecto a la empresa en la que deba realizar la auditoría informática, a exigir una total autonomía e independencia en su trabajo, condición ésta imprescindible para permitirle actuar libremente según su leal saber y entender.

Principio de información suficiente

Obliga al auditor a ser plenamente consciente de su obligación de aportar, en forma pormenorizadamente clara, precisa e inteligible para el auditado, información tanto sobre todos y cada uno de los puntos relacionados con la auditoría que puedan tener algún interés para él, como sobre las conclusiones a las que ha llegado, e igualmente informarle sobre la actividad desarrollada durante la misma que ha servido de base para llegar a dichas conclusiones.

Principio de integridad moral

Obliga al auditor a ser honesto, leal y diligente en el desempeño de su misión, a ajustarse a las normas morales, de justicia y probidad, y a evitar participar, voluntaria o inconscientemente, en cualesquiera actos de corrupción personal o de terceras personas.

Principio de legalidad

En todo momento el auditor deberá evitar utilizar sus cocimientos para facilitar, a los auditores o a terceras personas, la contravención de la legalidad vigente.

Principio de no discriminación

El auditor en su actuación previa, durante y posteriormente , deberá evitar inducir, participar o aceptar situaciones discriminatorias de ningún tipo, debiendo ejercer su actividad profesional sin prejuicios de ninguna clase y con independencia de las características personales, sociales o económicas de sus clientes.

Principio de no injerencia

El auditor deberá evitar aprovechar los datos obtenidos de la auditoría para entrar en competencia desleal con profesionales relacionados con ella de otras áreas del conocimiento. Esa injerencia es mayormente reprobable en los casos en los que se incida en aquellos campos de actividad para los que el auditor no se encuentre plenamente capacitado.

Principio de precisión

Exige del auditor la no conclusión de su trabajo hasta estar convencido, en la medida de lo posible, de la viabilidad de sus propuestas, debiendo ampliar el estudio del sistema informático cuanto considere necesario, sin agobios de plazos (con la excepción de lo ya indicado anteriormente respecto al principio de economía) siempre que se cuente con la aquiescencia del auditado, hasta obtener dicho convencimiento.

Principio de publicidad adecuada

La oferta y promoción de los servicios de auditoría deberán en todo momento ajustarse a las características, condiciones y finalidad perseguidas, siendo contraria a la ética profesional la difusión de publicidad falsa o engañosa que tenga como objetivo confundir a los potenciales usuarios de dichos servicios.

Principio de responsabilidad

El auditor deberá, como elemento intrínseco de todo comportamiento profesional, responsabilizarse de lo que haga, diga o aconseje, sirviendo esta forma de actuar como cortapisa de injerencias extraprofesionales.

Principio de secreto profesional

La confidencia y la confianza son características esenciales de las relaciones entre el auditor y el auditado e imponen al primero la obligación de guardar en secreto los hechos e informaciones que conozca en el ejercicio de su actividad profesional. Solamente por imperativo legal podrá decaer esa obligación.

Principio de servicio público

La aplicación de éste principio debe incitar al auditor a hacer lo que éste en su mano y sin perjuicio de los intereses de su cliente, para evitar daños sociales como los que pueden producirse en los casos en que, durante la ejecución de la auditoría, descubra elementos de software dañinos (virus informático) que puedan propagarse a otros sistemas informáticos diferentes del auditado. En estos supuestos el auditor deberá advertir, necesariamente en forma genérica, sobre la existencia de dichos virus a fin de que se adopten las medidas sociales informativas pertinentes para su prevención, pero deberá asimismo cuidar escrupulosamente no dar indicios que permitan descubrir la procedencia de su información.

Principio de veracidad

El auditor en sus comunicaciones con el auditado deberá tener siempre presente la obligación de asegurar la veracidad de sus manifestaciones con los límites impuestos por los deberes de respeto, corrección y secreto profesional.

2.3.- Planeación de la Revisión

Objetivo: Definir el alcance de la revisión y elaborar el plan de trabajo.

En esta actividad se deberá analizar el entorno del proyecto, para conocer como está organizado, dimensionarlo e identificar a las áreas involucradas en la revisión de la unidad auditable, con el propósito de definir el alcance y elaborar el plan de trabajo correspondiente.

Cabe mencionar que el nivel de información existente hasta este momento es de tipo general; sin embargo, es importante considerar los siguientes aspectos:

- Políticas organizacionales, relacionadas con la unidad auditable.
- Información preliminar existente (organigramas, descripciones de puestos, etc.).
- Enfoque y conocimiento general que tiene el auditor del área auditable.

Definición de objetivos y alcances

Con base en el análisis y estudio previo de la unidad auditable, se establecen en forma clara y concreta los objetivos de la revisión, así como la cobertura y el nivel de profundidad de la misma.

Como parte de esta actividad debe elaborarse la carta inicial de revisión, a fin de presentar a las áreas involucradas, el grupo de Auditoría que estará a cargo de la revisión.

Productos finales:

- Lista de objetivos y alcances.
- Carta de inicio de la revisión.

Recabación de información básica

Consiste en acudir directamente con los responsables de las áreas involucradas para solicitar la información tanto administrativa como técnica indispensable para llevar a cabo la revisión, considerando que independientemente del volumen de información recabada solo se analice lo necesario para cubrir los objetivos de esta fase y realizar un análisis profundo en las fases posteriores.

Revisar la información obtenida previamente, para tener una perspectiva general que nos permita conocer las principales características de la unidad auditable.

Durante el desarrollo de esta actividad es necesario hacer un programa de entrevistas definiendo para ello, el perfil de cada una de las mismas, con base en la naturaleza de las funciones que realicen las personas entrevistadas y a efecto de prever el nivel de información que se solicitará.

Como resultado de las entrevistas es importante documentar y resumir la información obtenida en cada una de las mismas.

La inclusión de nuevas entrevistas debe ser considerada, en virtud de que existe la posibilidad de identificar áreas que originalmente no habían sido contempladas en la revisión.

Productos finales:

- Lista de requerimientos de información básica.
- Programa de entrevistas iniciales.
- Resumen de entrevistas.

Análisis de información

Debe efectuarse un examen minucioso de la información obtenida, con el propósito de identificar y seleccionar los aspectos primarios, secundarios y no relevantes, así como la determinación de la información adicional o complementaria que debe ser requerida.

Productos finales:

- Descripción narrativa de las características principales.
- Resumen del análisis de la información inicial.

Diagnóstico de viabilidad.

Considerar en esta actividad, los elementos de información identificados en el análisis, con el objeto de hacer un examen previo de la unidad auditada y decidir si se realiza la revisión o no, estableciendo las causas que justifiquen ambas situaciones, considerando los siguientes aspectos:

a) Importancia e impacto de la unidad auditable para la Organización (Nivel de Riesgo).

- Cobertura de servicio.
- Tecnología existente.
- Interacción con otros sistemas.
- Costo financiero de la función.
- Dimensión del sistema en términos de programas o procesos.
- Número de personas involucradas.
- Áreas participantes.
- Nivel de automatización.

b) Situación de control.

Determinar cuál es la situación que presenta la unidad auditable en cuanto a la suficiencia y debilidades de control y probabilidad de riesgo.

c) Beneficios esperados de la revisión.

- Identificar los factores de riesgo, determinando los aspectos relevantes que pudieran afectar a la Institución en términos financieros, de operación o administrativos.
- Con base en el diagnóstico de los aspectos citados elaborar la propuesta para efectuar la revisión o indicar cuales son las causas que justifican la suspensión de la misma.

Producto final:

- Resumen de viabilidad.

Planeación del desarrollo

Elaborar el programa de trabajo, asignando tiempos y responsables a las actividades de las siguientes fases de la metodología.

Producto final:

- Plan de desarrollo de la revisión.

2.4.- Desarrollo de la Auditoría

Objetivo: Identificar y ponderar los factores de riesgo, para determinar el grado de eficiencia del sistema o unidad auditable.

Obtención de información detallada

Con base en el resultado del análisis de la información y el conocimiento adquirido hasta ahora de la unidad que estamos revisando, podemos determinar qué información adicional requerimos para satisfacer nuestras necesidades.

Producto final:

- Documentación de auditoría (legajo de auditoría, conteniendo los productos finales de las fases anteriores).

Detallar plan original

Siguiendo el plan de desarrollo en donde se identificaron para las macroactividades, se procederá a desglosar aquellas que requieran mayor detalle para obtener programas de revisión de acuerdo con las características de la función auditada.

Producto final:

- Programa de trabajo detallado.

Evaluación de controles

En esta actividad se evaluarán los puntos de control determinados en el programa de revisión, con el propósito de conocer la eficiencia en el manejo de información y en la generación de resultados, vigilando el cumplimiento de los objetivos determinados en el programa de revisión.

Productos finales:

- Lista de controles.
- Matrices de evaluación (cuestionarios de control interno).
- Resumen de situación de control Interno.

Diseño de pruebas de auditoría

En esta actividad se deberá de diseñar y realizar el programa de pruebas de aquellas funciones y procedimientos que por su nivel de riesgo sea necesario validar.

Producto final:

- Programa de pruebas de auditoría.

Aplicación de pruebas de auditoría

En esta actividad se deberá aplicar el programa de pruebas de la unidad auditada, para validar aquellos controles que de acuerdo a sus características es necesario revisar a través de pruebas de auditoría.

Productos finales:

- Papeles de trabajo de las pruebas.
- Lista de observaciones.
- Resumen de hallazgos.

2.5.- Comunicación

Objetivo: Elaborar el Informe Final con su Carpeta de Apoyo que lo sustente y comentarlo con las áreas involucradas a fin de obtener su confirmación, así como la aprobación por parte de los ejecutivos de Auditoría para emitirlo. Establecer compromisos y acuerdos para la atención de las observaciones.

Evaluación y documentación de resultados

Con base en el resultado de las pruebas y apoyándose en el resumen de situación de control interno, el auditor determinará los riesgos debido a controles deficientes, inexistentes o duplicados. Lo anterior servirá para facilitar el análisis de las observaciones, el establecimiento de recomendaciones, el cumplimiento con los objetivos de la revisión.

Posteriormente, el auditor deberá analizar y evaluar las observaciones a fin de comenzar a estructurar el "Borrador de observaciones", determinando el impacto de cada una de ellas en cuanto al riesgo que representan para la Institución.

Como resultado de esta etapa, el auditor deberá generar el "borrador de observaciones" para la elaboración del informe, en donde cada una de las observaciones deberá ser sustentada con evidencias suficientes y competentes (papeles de trabajo), con las cuales formará la carpeta de apoyo y la económica que será de gran utilidad cuando se comente el informe con los auditados.

Productos finales:

- Borrador de observaciones y sus recomendaciones.
- Carpeta de apoyo actualizada.

Elaboración del Informe

El auditor redactara el Informe ponderando y seleccionando aquellas observaciones que impliquen alto nivel de riesgo para la Institución, tomando en cuenta para su estructura, el siguiente formato:

- *Fecha del informe.*- Deberá fecharse preferiblemente en el momento de su entrega.
- *Destinatario.*- El informe será dirigido al titular de la Dirección del área auditada.
- *Discusión del Informe.*- Incluir el nombre de las personas con quienes se discutió el Informe, incluyendo su puesto y área.
- *Objetivo y Alcance.*- Indicar el propósito de la revisión y sus alcances considerando lo establecido en la planeación de auditoría.
- *Antecedentes.*- Describir claramente los hechos relevantes que ocurrieron antes, que guarden relación con la situación actual y con las observaciones detectadas, las cuales deberán sustentarse con papeles de trabajo.
- *Situación actual.*- Mencionar el estado actual del proyecto o unidad auditada, sustentado con papeles de trabajo. Esta situación deberá reflejar los efectos de los antecedentes y su posible relación con las observaciones, en términos de riesgo y problemática general.

- ***Observaciones y Recomendaciones.***- Con base en el "borrador de observaciones" generado en la etapa anterior, afinar la descripción de las observaciones, resaltando en cada una de ellas el efecto en cuanto a riesgo. Para cada una de estas observaciones se deberá poner un especial cuidado en la forma de exponerlas, procurando su correcta interpretación y fácil entendimiento.
- Conviene dar una serie de *sugerencias y recomendaciones* con el fin de facilitar la solución a las observaciones referidas o para dimensionar el alcance de los controles requeridos, que permitan minimizar los riesgos expuestos.
- *Comentarios de los auditados.*- Cuando no exista acuerdo en alguna observación, incluir textualmente los comentarios de los auditados.
- *Conclusiones.*- Exponer las opiniones de auditoría, derivado del análisis integral de los resultados obtenidos.
- *Párrafo final y firma.*- Debe haber un párrafo de cierre, que incluya el plazo máximo de respuesta (entre 15 y 20 días naturales), así también la frase de "Atentamente" con la firma del Subdirector de Auditoría.
- *Distribución.*- Marcar copia del informe a los titulares y usuarios directos de todas las áreas involucradas en la revisión.

Recomendaciones adicionales

Para la elaboración del informe se sugiere considerar lo siguiente:

- Es importante cuidar la redacción y la ortografía.

- Preparar anticipadamente los lineamientos de argumentación para facilitar el análisis del informe con los involucrados en la auditoría.
- Revisar que el informe incluya comentarios que eviten posibles malas interpretaciones en cuanto a críticas que pudieran parecer tendenciosas.
- Redactar el informe teniendo en mente que es definitivo, es decir, no considerar que los superiores lo revisaran.

A efecto de procurar la objetividad en la opinión de los involucrados al momento de comentar el Informe, se preparará un borrador de Informe para comentar, el cual contendrá únicamente situación actual, observaciones y recomendaciones.

Productos finales:

- Borrador de Informe.
- Borrador de Informe para comentar (situación actual, observaciones y recomendaciones).
- Documentación de sustento a las observaciones (carpeta económica).

Autorización de la Subdirección de Auditoría

El auditor conjuntamente con el supervisor o Gerente deberá presentar el informe al Subdirector de Auditoría para su revisión y autorización, llevando consigo la carpeta de apoyo que lo sustente.

Producto final:

- Informe autorizado.

Comentar con responsable directo y áreas involucradas

El auditor conjuntamente con el supervisor o Gerente y en caso necesario también el Subdirector, deberán comentar el "borrador de Informe" (es decir solo situación actual, observaciones y recomendaciones) con los responsables directos y con las áreas involucradas en el proyecto o unidad auditada.

Al comentarse con las áreas involucradas, es conveniente tomar como referencia lo acordado con los responsables directos y con las áreas con las que ya se haya comentado anteriormente.

En caso de surgir diferencias con los responsables o involucrados, solicitar la documentación que soporte sus apreciaciones para comparar con nuestros papeles de trabajo y en caso de justificarse las diferencias, el auditor procederá a realizar los cambios respectivos al Informe.

El auditor recolectara las modificaciones y ajustes con los elementos que la propiciaron.

De ser posible durante las entrevistas se deberán establecer los compromisos con el responsable de atender las observaciones expuestas en el informe. Es conveniente formalizar estos compromisos a través de una minuta con firmas de los involucrados.

En caso de que no se puedan establecer los compromisos de inmediato, se establecerá con los responsables la inclusión de los mismos, en la respuesta al Informe, aclarando que esta respuesta debe ser única y debe venir en términos de responsable, acción a realizar y fechas planeadas de terminación.

Es recomendable:

- Concertar la cita con anticipación y sugerirle al responsable, que se presente con su documentación.
- Llevar papeles de trabajo y carpeta de apoyo.
- Durante la reunión utilizar los lineamientos de argumentación previamente definidos.
- Comunicar al Subdirector los resultados de la revisión del informe.

Productos finales:

- En caso de diferencias, la documentación que sustente los cambios al Informe.
- Informe confirmado por las áreas involucradas (levantando minuta formal).

Documentación de acuerdos y ajustes

El auditor documentará los cambios, así como los acuerdos surgidos durante las reuniones y realizar los ajustes al Informe final, a fin de tener actualizada la carpeta de apoyo que lo sustenta.

Productos finales:

- Carpeta de apoyo actualizada.
- Informe final.

Autorización de la Dirección de Auditoría

El Subdirector de Auditoría deberá presentar al Director de Auditoría el Informe de la revisión, a fin de tener su aprobación para emitirlo.

Producto final:

- Informe final autorizado

Emisión del Informe

Enviar el informe final aprobado por el Director de Auditoría y firmado por el Subdirector de Auditoría, acompañado de un memorándum que indique con quienes fue comentado y los resultados de las entrevistas.

Enviar simultáneamente copias del informe a quienes se indiquen en la distribución, con su respectivo memorándum.

Si se considera conveniente, enviar copias ciegas de dicho informe a otras áreas a las cuales pueda ser de interés. Ej. otras áreas de Auditoría, áreas del interior, etc. Se notificará a los superiores para obtener su autorización. A esta copia, deberá anexarse un memorándum donde se indique la razón del envió.

Productos finales:

- Memorándum para envío del Informe y copias correspondientes.
- Copias ciegas (del Informe final).

2.6.- Seguimiento

Objetivo: Certificar que las deficiencias y problemas detectados durante la revisión han sido corregidos y evaluar el estátus de control. Para esto se elaborará el programa de seguimiento y con base en él se verificará que las actividades contempladas dentro del plan de acción, se efectúen de acuerdo a lo establecido. generando un Informe que permita conocer los resultados de las medidas correctivas.

Al determinar el grado de avance de las soluciones, se desarrollarán actividades de la fase de desarrollo, con lo cual se dará continuidad al proceso de Auditoría.

Son objeto de seguimiento todas las revisiones que se encontraron en un estado de control deficiente, regular, bueno o con posibilidades de optimizarse.

Obtención de respuesta al Informe

Establecer en el informe un período razonable (entre 15 o 20 días naturales) para la respuesta al informe. En caso necesario, solicitar la respuesta mediante un memorándum.

Una vez recibida la respuesta, analizar el contenido para determinar los compromisos o acciones, verificando que se apeguen a lo observado y acordado anteriormente.

Productos finales:

- Solicitud de respuesta al Informe (en caso necesario).
- Respuesta del Informe.

Revisión de la respuesta

Verificar la suficiencia de los planes de acción generados por el área responsable de contestar el Informe.

Producto final:

- Comunicación de desacuerdos (en caso de existir).

Programación del Seguimiento

Con base en el plan de acción (en caso de no existir el plan de acción recurrir a la estructura del Informe), áreas afectadas y compromisos anticipados obtenidos en las confirmaciones del Informe, generar un programa de revisión al seguimiento, con actividades y fechas tentativas de realización. Considerando para ello alguna otra observación que se deba incluir.

Producto final:

- Programa de Seguimiento.

Desarrollo del Seguimiento

Proceso de seguimiento:

Los auditores deberán hacer el seguimiento correspondiente para cerciorarse de la suficiencia de las medidas adoptadas para corregir las debilidades de control reportadas. La auditoría deberá determinar si las medidas correctivas tomadas logran los resultados deseados, o si el área auditada asumió la responsabilidad de no tomar ninguna medida correctiva sobre los hallazgos reportados.

Durante el desarrollo del seguimiento, se aprovechará para que a juicio del auditor o superiores se revisen aspectos adicionales cuando por su importancia lo amerite o por su relación con los resultados de la auditoría, con el fin de tener una continuidad en la permanencia de la función de auditoría en el proyecto o unidad auditada.

Informe de resultados:

Dependiendo de la importancia de los avances en la solución a las observaciones, la aplicación de las medidas correctivas, la desatención de los compromisos contraídos o cualquier otro factor que se juzgue relevante, se emitirá el Informe del seguimiento con las características definidas en la etapa de Elaboración de Informe.

Para la realización del Informe del seguimiento, se desarrollarán las actividades necesarias, dando lugar a la continuidad de la función de auditoría.

Productos finales:

- Resumen de observaciones.
- Informe del seguimiento.
- Carpeta de apoyo del informe del seguimiento.

3.- RIESGOS Y CONTROLES PARA LA AUDITORÍA DE SISTEMAS DE INFORMACIÓN

3.1.- La Necesidad de Tener Seguros los Sistemas de Información

La seguridad de los sistemas de información puede ser definida como la estructura de control establecida para administrar la integridad, confidencialidad y disponibilidad de los datos y recursos de los sistemas de información. Debido a que el nivel de confianza en los sistemas de información ha crecido, actualmente la seguridad se ha vuelto una parte fundamental en la viabilidad de muchas organizaciones.

Una estructura de control es necesaria para asegurar los datos y recursos de los sistemas de información usados o producidos por el sistema. En las grandes organizaciones con millones de transacciones y clientes, las operaciones no pueden continuar sin que los sistemas de información funcionen adecuadamente. En organizaciones pequeñas, se podrían tener reducciones significativas o pérdidas de la productividad.

Tanto los datos como los recursos son valiosos para la Organización y deberán ser mantenidos en forma segura. El equipo es valioso por las obvias razones monetarias; los datos almacenados o procesados por los computadores pueden ser más valiosos por las siguientes razones:

- Importancia estratégica de los datos.
- La confianza en los datos para la toma de decisiones.
- Confidencialidad de los datos.

- Las expectativas de una tercera parte.
- Requerimientos externos.

Importancia estratégica de los datos

La información estratégica puede ser definida como información única para la Organización que le provee una ventaja sobre la competencia. Los datos almacenados en la computadora puede contener información estratégica para la Organización, como ejemplo de esta información es la siguiente:

- Listas de precios de los clientes.
- Secretos de marca (tales como fórmulas de los productos).
- Anuncio de nuevos productos.
- Códigos de programas para aplicaciones propias.
- Costos de los datos para los productos o servicios.

La confianza en los datos para la toma de decisiones

Los datos almacenados en las computadoras son usados por la Organización para la toma de decisiones, las cuales pueden variar desde financieras hasta operacionales. Como un ejemplo de estos sistemas computacionales usados para la toma de decisiones, se mencionan los siguientes:

- Sistemas usados para administrar y tomar decisiones financieras.
- Sistemas usados para controlar las salidas y llegadas de los vuelos de una línea aérea.

- Sistemas usados para diagnosticar a pacientes.
- Sistemas usados para calendarizar las rutas de los autobuses.
- Sistemas usados para procesar órdenes y calendarios de procesos.

Confidencialidad de los datos

Una Organización puede desear tener sus datos almacenados en una forma segura por varias razones. Si los datos son relacionados con el personal o con los recursos humanos, deberá haber un requerimiento legal para su confiabilidad. La Organización puede ser requerida para almacenar los datos de una forma segura y estar de acuerdo con el requerimiento de una tercera parte. Como ejemplo de datos confidenciales tenemos los siguientes:

- Datos militares o de seguridad nacional.
- Datos relacionados con la propuesta adquisición de otra organización.
- Datos almacenados por un Buró de servicio para ser usados al proveer un servicio de cómputo.
- Datos relacionados con los contratos del gobierno con la Organización.

Las expectativas de una tercera parte

Las partes que se encuentran fuera de una organización (incluyendo a los clientes, empleados y público en general) pueden tener expectativas de proteger sus datos. Las terceras partes pueden esperar que la Organización mantenga en forma segura los datos relacionados con:

- El precio pagado o los proveedores por ciertos productos o servicios.
- Información de los clientes.
- Información de los empleados.
- Código fuente de los programas amparados por una licencia de uso de software.
- Números de cuenta y estado de las tarjetas de crédito.

Requerimientos externos

Un requerimiento derivado de una legislación, obligatorio o un conjunto de medidas pueden requerir que los datos sean almacenados en un lugar seguro. Los requerimientos legales y obligatorios son especificados por las jurisdicciones nacionales o locales que tienen autoridad sobre la Organización. Actualmente existen una cuantas leyes relacionadas directamente con la seguridad de los datos y recursos de los sistemas de información. Las leyes relacionadas con los sistemas de información se pueden clasificar de la siguiente manera:

- Criminales.
- Contabilidad corporativa.
- Privacia.

Algunos grupos industriales tienen estándares para sus miembros para asegurar los datos y recursos relacionados con los sistemas de información. Las organizaciones que hacen

negocios con agencias del gobierno o que usan el Intercambio Electrónico de Información (EDI) o la Transferencia Electrónica de Fondos (EFT) pueden estar sujetas a tales estándares. Los auditores internos deberán de estar familiarizados con los requerimientos internos y externos que afectan a la Organización.

3.2.- Riesgos en los Datos y Recursos de los Sistemas de Información

La integridad, confidencialidad y disponibilidad de los datos y recursos de los sistemas de información podrán tener riesgos, debido a:

- Errores humanos, accidentes y omisiones.
- Empleados deshonestos.
- Empleados molestos con la Organización.
- Individuos ajenos a la Organización.
- Daños ambientales.
- Fluctuaciones eléctricas.
- Desastres naturales y otras amenazas físicas.
- Disturbios civiles.
- Introducción de código erróneo.

Errores humanos, accidentes y omisiones

Los errores humanos, accidentes y omisiones causan directamente las pérdidas más costosas y con mayores repercusiones en la Organización cada año. Estos errores van desde la captura de datos hasta los errores en la programación del software.

Empleados deshonestos

Casi todos los reportes de crímenes computacionales revelan que la persona que los realizó fue un empleado de la compañía quien tuvo "autorización" para accesar

información con la cual el crimen fue cometido. Los empleados deshonestos pueden causar cuantiosas pérdidas, por lo que la seguridad deberá enfocar su atención a los empleados.

Empleados molestos con la Organización

Los empleados enojados con la Organización usualmente no están motivados por la codicia, pero si por factores emocionales. Los actos de los empleados molestos pueden resultar en pérdidas significativas para la Organización.

Individuos ajenos a la Organización

Los individuos que se encuentran fuera de la Organización tienen el mismo nivel de riesgo que los empleados deshonestos o molestos. Los riesgos de los individuos que se encuentran fuera de la Organización generalmente tienen una baja prioridad de ocurrencia, pero puede resultar en pérdidas cuantiosas a la Organización. Mientras que las grandes pérdidas provienen de las aciones de los empleados, las acciones de los individuos ajenos a la empresa no deberán de ser minimizados. Una publicidad adversa puede resultar de tales acciones y puede afectar la habilidad de la Organización para atraer y retener a los clientes.

Daños ambientales

Los daños por fuego son las más significativos y previsibles de todas las amenazas físicas que le pueden ocurrir a los sistemas de información. Mientras que el fuego puede ocurrir dentro del cuarto del computador, lo más común es que se inicie en las áreas adyacentes

a dicho cuarto. El que se extienda el fuego, el humo o el agua podrían dejar al edificio o al centro de cómputo inoperable.

El daño por agua al equipo o a las instalaciones donde se encuentra el computador es una amenaza seria, considerando los desagües construidos en los modernos edificios. El equipo es particularmente susceptible de almacenar pequeñas cantidades de humedad, debido a las necesidades de refrigeración y a las altas corrientes eléctricas.

Otros tipos de daños pueden ocurrir, incluyendo las basuras en el aire dejadas por los químicos usados cerca de donde se localiza el centro de cómputo. Este tipo de riesgos y los daños por agua o fuego son particulares a todas organizaciones.

Fluctuaciones eléctricas

Los equipos de cómputo requieren de un suministro de energía "limpio". Esto se refiere a la calidad del suministro eléctrico para los equipos. Los apagones, descargas eléctricas y fallas en el suministro de energía pueden causar la pérdida de datos y de las capacidades de operación.

Desastres naturales y otras amenazas físicas

Terremotos, tornados, inundaciones, tifones, mareas, y otros desastres naturales son de baja ocurrencia pero de grandes repercusiones financieras, por lo que es necesario tomarlos en cuenta en la planeación en casos de desastre. Los procedimientos de

seguridad diseñados para reducir la exposición al fuego, y al agua deberán ser considerados como desastres naturales también.

Disturbios civiles

Los recursos y los datos de los sistemas de información pueden estar en riesgo debido al comportamiento de la población del lugar donde se encuentra el centro de cómputo. Los alborotos, guerras civiles, o actos de terrorismo son ejemplos de este tipo de riesgos. Estos riesgos varían dependiendo del país y/o del estado en donde opera la organización.

Introducción de código erróneo

La introducción de código erróneo o dañino (esto es, virus o worms 'write only, read many times') en un ambiente de cómputo puede resultar en pérdidas o destrucciones de datos y pueden dejar al ambiente de cómputo inoperable hasta que el código es identificado, aislado y removido. Tal código puede ser introducido inadvertidamente dentro de un programa legítimo o dentro de datos que han sido contaminados.

3.3.- Clasificación de controles

Los controles internos relacionados con los Sistemas de Información (SI) tienen diferentes clasificaciones, a continuación se describirán las siguientes cinco clasificaciones:

- Controles preventivos, detectivos, y correctivos.
- Controles discrecionales y no discrecionales.
- Controles voluntarios y obligatorios.

- Controles manuales y automatizados.
- Controles generales a los sistemas de información y a las aplicaciones.

El propósito de esta clasificación es proveer un método por el cuál el significado, propósito y costo del procedimiento de control pueda ser evaluado en el contexto de alternativas de procedimientos de control. Cada uno de los esquemas de clasificación nos ayudan a enfocar diferentes aspectos de las técnicas de control. Por ejemplo, las descripciones "control preventivo, voluntario, manual y general" nos dice lo siguiente:

- Los controles previenen los errores desde que se están iniciando.
- El uso de los controles es voluntario y pueden ser fácilmente cambiados.
- Los controles son ejecutados por humanos, por consiguiente, están sujetos a las fallas humanas.
- Los controles son generales y están enfocados al ambiente dentro del cual otros controles operan. Esto es, una ruptura del control puede tener otras implicaciones.

Los controles son necesarios para alcanzar objetivos específicos y se necesitan para corregir las cosas que van mal y que pueden afectar negativamente a la Organización. Tales impactos negativos pueden incluir almacenamientos de registros erróneos, la toma de decisiones erróneas, costos excesivos, pérdida o destrucción de activos, suspensión de las actividades del negocio, sanciones regulatorias y pérdida de ventaja competitiva. Los controles necesitan disminuir o eliminar las causas de estas situaciones.

Tal como un problema puede resultar en múltiples consecuencias negativas, un control puede reducir múltiples riesgos, por lo que la relación entre los riesgos y los controles no es uno a uno y un control puede caer dentro de diferentes clasificaciones en forma simultánea. Algunos controles funcionan en forma independiente de otros controles, mientras que otros controles funcionan en combinación con controles complementarios.

Los controles no son soluciones perfectas a los problemas, pero reducen los riesgos a niveles aceptables. En algunos casos, una combinación de técnicas de control provee una mejor protección a un menor costo global que si se aplicara solamente un solo control.

Por la clasificación de los controles y su relación entre ellos, el auditor puede sistemáticamente determinar los controles que son clave para una apropiada operación del sistema o de la función. La clasificación de los controles es importante para su adecuada localización y prueba en la realización de una auditoría. Derivado de la clasificación y evaluación de los controles, como su propósito y efectividad, el auditor podrá asegurar que los controles fueron apropiadamente probados y evaluados, y que el tiempo de auditoría no fue desperdiciado en probar controles con pocas o nulas consecuencias.

Controles preventivos, detectivos y correctivos:

Los controles preventivos, detectivos y correctivos tienden a operar en combinación con o sin dependencias de otros controles. El costo-beneficio es un elemento clave en el uso de

los controles preventivos, detectivos y correctivos. Algunos errores pueden resultar en graves consecuencias y deberán de ser prevenidos, en la medida de lo posible. Otros errores pueden ser costosos para prevenir, pero puede ser más barato y más sencillo detectarlos y corregirlos. Otros errores o problemas pueden ser imposibles de detectar y corregir, pero es recomendable poner medidas de control correctivas para una adecuada recuperación.

Algunas técnicas de control pueden ser clasificadas como preventivas, detectivas y correctivas, dependiendo donde y cómo son usados en un proceso o en un sistema. Algunas consideraciones en la clasificación y combinación de estos tipos de control son los siguientes:

Controles preventivos

Los controles preventivos evitan que los eventos indeseables ocurran. En un ambiente de SI, los controles preventivos son complementados con la implementación de procedimientos automatizados para prohibir accesos no autorizados a los sistemas y para que se tomen las acciones necesarias por los usuarios. Ejemplos de estos controles preventivos incluyen los siguientes:

- Restricciones en las sustituciones de los usuarios.
- Incapacidad para cerrar archivos si la transacción se perdió.
- Entradas duales o verificación de las transacciones administrativas sensitivas.
- Requerimientos del password antes de meter datos.

Debido a que los controles preventivos no son 100% efectivos, estos suelen operar en combinación con los controles detectivos, los cuales identifican los errores o eventos pero no los previenen. No se puede obtener siempre una buena relación de costo-beneficio para prevenir todos los errores desde la fuente del mismo, y en forma complementaria con los controles detectivos pueden ser usados como una medida para prevenir el error que está siendo llevado a través del sistema.

Controles detectivos

Los controles detectivos identifican a los eventos indeseados antes de que hayan ocurrido. Los controles detectivos tienen los siguientes dos elementos:

- El sistema podrá identificar y registrar las actividades de un usuario, las transacciones clave y las condiciones poco usuales y excepciones y generar reportes sumarios para asegurar una adecuada pista de auditoría.
- La Dirección deberá ser responsable de revisar el reporte sumario y de excepciones, para identificar cualquier anormalidad y para que tome las acciones apropiadas.

Los controles detectivos deberán identificar los tipos de errores esperados tanto como los que no se esperan que ocurran. Debido a que los controles preventivos pueden fallar o pueden ser saltados, los controles detectivos pueden proveer una revisión redundante de todos los tipos de error que debieron ser prevenidos. Esta cobertura puede alertar a los usuarios o a la Dirección de las irregularidades en el sistema o proceso tan pronto

ocurran. Los controles redundantes pueden no tener una relación de costo-beneficio positivo en todos los casos y pueden ser empleados de una forma base.

Para cada control detectivo deberá de haber uno o más controles correctivos, dependiendo del tipo y alcance del error. Algunos errores puede ser solamente reportados; algunos pueden ser removidos del procesamiento y reportados para tomar acciones posteriores; y otros más pueden requerir de acciones correctivas inmediatas antes de continuar con el proceso.

Por ejemplo, un programa identifica la entrada de transacciones que exceden el límite de dólares establecido por la Dirección, generando un reporte. La Dirección recibe y revisa este reporte diariamente para identificar y corregir las transacciones erróneas. Otro ejemplo se enfoca a la detección de errores en un proceso automatizado de manufactura. Los errores y los defectos son detectados por un sistema computacional y la parte defectuosa es reciclada en el proceso para que el error sea corregido.

Los controles detectivos son enfocados en mayor medida en las evaluaciones de auditoría. La detección de errores en las pruebas de auditoría pueden apuntar a errores no considerados en los controles preventivos, detectivos y correctivos.

Controles correctivos o de recuperación

Los controles correctivos o de recuperación fomentan que se realice un evento deseable o una acción correctiva sea realizada después de que un evento indeseable ha sido

detectado. Este tipo de control se lleva a cabo después de que un evento indeseable ha ocurrido y se intenta darle reversa al error o se intenta corregirlo. Si una transacción fue impropiamente aplicada, una acción de corrección del error es un control de recuperación. Tratando con los errores de omisión, un sistema es vulnerable cuando ninguna acción es tomada para corregir una excepción detectada. El sistema deberá de tener controles preventivos en lugar de prevenir o prohibir acciones en respuesta a la excepción.

Tratando con los errores de omisión, un sistema es vulnerable cuando una excepción es detectada y una respuesta incorrecta es tomada. En esta situación, los sistemas deberán tener controles de recuperación en lugar de tratar de darle reversa al error y recuperar la pérdida. Cuando una acción inapropiada ocurre, especialmente en ambientes on-line o en tiempo real, las acciones se llevan a cabo antes de que sea prevenido. En este caso, una pista de auditoria es esencial para proveer la información necesaria para corregir el error y recuperar la pérdida.

En el diseño o evaluación de controles correctivos, es importante relacionar el control al evento que permite o que es la causa del error. Un control correctivo deberá funcionar tan cerca de la fuente del error y deberá de proveer retroalimentación para ser aplicada en la prevención de errores. Los errores que no pueden ser relacionados con su fuente pueden resultar en costos excesivos, debido a que no se encuentran incentivados para reducir los porcentajes de errores. El proceso de controles correctivos también deberá estar sujeto al mismo escrutinio (de los controles preventivos y detectivos) como los demás procesos, para prevenir y/o detectar los errores introducidos durante la corrección de un error.

Controles discrecionales y no discrecionales

Los controles discrecionales están sujetos a la decisión de las personas, y los controles no discrecionales son proveídos automáticamente por el sistema y no pueden ser saltados, ignorados o aplicados según el juicio de las personas. Por ejemplo, la revisión de la supervisión de firmas autorizadas es un control discrecional. El requerimiento de digitar el Número de Identificación Personal (NIP) en un cajero automático para que pueda aceptar transacciones, es un control no discrecional.

La clasificación de los controles discrecionales y no discrecionales es importante, debido a que el diseño apropiado de los controles no discrecionales tienden a ser más confiables que los controles discrecionales y son probados de manera diferente. Algunos controles automatizados no pueden ser clasificados como no discrecionales, porque pueden ser ignorados o saltados. Un ejemplo de un control automatizado discrecional es un archivo de transacciones suspendidas del procesamiento, las que esperan la intervención de una persona. El proceso de corrección no puede realizar la corrección de cada una de las transacciones, debido a que no se tenga el proceso de corrección o que no se cuente con la validación o edición de todas las entradas inválidas. En este caso el control que por arriba parece ser no discrecional, es altamente discrecional y puede darle debilidad a todo el sistema de control interno.

Controles voluntarios y obligatorios

Los controles voluntarios son elegidos por una Organización para soportar la administración de las actividades del negocio. Procedimientos específicos para iniciar, procesar, registrar y reportar transacciones son ejemplos de controles voluntarios.

Los controles obligatorios, requeridos por las leyes y regulaciones gubernamentales, son impuestas a la Organización por las autoridades externas. Las regulaciones federales, estatales y locales, también como los requerimientos internacionales deberán de ser considerados cuando se dirigen las actividades del negocio. Deberán existir procedimientos acordes para satisfacer los requerimientos externos.

Controles manuales y automatizados

En todos los ambientes de SI, los controles manuales y automatizados soportan el procesamiento de datos a través de los sistemas y la habilidad de los usuarios para verificar lo completo, la seguridad y lo apropiado de los procesos.

Controles manuales

En un ambiente manual, es usual tener una relación uno a uno entre las funciones de proceso y los controles, siendo las personas las directamente responsables de realizar o ejecutar las funciones de control. Por ejemplo, los cálculos manuales básicos son usualmente verificados por un segundo individuo (por lo menos a nivel de pruebas). En un ambiente automatizado, sin embargo, no existe esa relación uno a uno. Esto es similar a,

por ejemplo, que los cálculos son ejecutados por una computadora y no son verificados manualmente.

Los controles manuales seguido trabajan en forma conjunta con los controles automatizados. Por ejemplo, Los sistemas de pago de nómina identifican generalmente los incrementos en los pagos, basados en los parámetros programados. Un reporte de excepciones es generado y revisado por el usuario.

Controles automatizados

Los controles automatizados son procedimientos programados diseñados para prevenir, detectar y corregir errores o irregularidades que pudieran tener un impacto adverso en las operaciones de la Organización. Estos controles enfocan los aspectos esenciales del procesamiento de transacciones y datos, desde la actividad de inicio hasta la actividad de generación de reportes. Los controles automatizados y sus funciones computarizadas de procesamiento relacionadas soportan directamente los sistemas de negocio más importantes y ayudan a asegurar la consistencia y confiabilidad de los procesos automatizados. Por ejemplo, la edición automatizada de los datos de entrada asegura que estos son correctamente digitados y se encuentran completos, previniendo así la introducción de datos erróneos al sistema.

Controles generales a los sistemas de información y a las aplicaciones

Los controles generales a los sistemas de información y a las aplicaciones son usados para mitigar los riesgos asociados con los sistemas de aplicaciones y con el ambiente de los Sistemas de Información.

Controles en las aplicaciones

Los controles de las aplicaciones se enfocan tanto a las entradas, procesamiento y salidas, y pueden ser usados para prevenir, detectar y corregir errores en el flujo de las transacciones dentro del sistema.

- Los controles en las entradas aseguran que se graben en forma completa y confiable las transacciones autorizadas. También tiene la función de identificar las transacciones a ser rechazadas, las duplicadas y las suspendidas; y deberán asegurar que estas transacciones sean reincorporadas al proceso.
- Los controles en el procesamiento, aseguran que todas las transacciones autorizadas sean procesadas completamente.
- Los controles en las salidas, aseguran que las salidas estén completas y que sean confiables, produciendo adecuadas pistas de auditoría de los resultados procesados, que serán enviados a los individuos correspondientes para su revisión.

Controles generales de los Sistemas de Información

Los controles generales de los sistemas de información se encuentran localizados dentro del ambiente de sistemas de información de la Organización, y tienen una influencia significativa en la efectividad de los controles de las aplicaciones. Estos son diseñados para asegurar que la información procesada sea razonablemente controlada y que sea consistente con el medio ambiente. Estos controles incluyen los relacionados con las operaciones de cómputo, con el desarrollo de sistemas, con la seguridad de los datos y con las telecomunicaciones, además tienen un impacto en la efectividad de todos los controles y funciones de proceso relacionadas con los sistemas de información. Las características principales de los controles generales se describen a continuación:

- *Controles en el desarrollo y mantenimiento de sistemas.* "La administración de la información y el desarrollo de sistemas". Es crítico tener estándares de desarrollo de sistemas y procedimientos de control de cambios para asegurar la integridad de los sistemas de aplicaciones del negocio dentro del ciclo de vida del sistema. Un ciclo de vida de desarrollo de sistemas deberá ser definido y una metodología de desarrollo deberá de ser empleada. El involucramiento de los usuarios, el soporte técnico, pruebas adecuadas del sistema y procedimientos de documentación deberán de tomarse en cuenta para soportar un ambiente de desarrollo y mantenimiento de sistemas controlado.
- *Controles de acceso y seguridad de datos.* "Seguridad". La seguridad de datos es una de las áreas relacionadas con los sistemas de información con más alto riesgo. Estos controles deberán de proveer integridad, confidencialidad y disponibilidad de los datos de la Organización y de los recursos de información.

- *Operaciones de cómputo.* "Administración de los recursos de cómputo". Los controles en las operaciones de cómputo aseguran el acatamiento a los procedimientos de operación. Un manual de estándares deberá existir para proveer criterios específicos para las operaciones de cómputo contra los cuales se realizará la evaluación del desempeño.
- *Bases de datos.* "La administración de la información y el desarrollo de sistemas". Las bases de datos son administradas independientemente de los sistemas aplicativos que usan los datos. Aseguran la integridad y el control de las bases de datos involucradas, estableciendo los chequeos organizacionales, protegiendo los datos contra accesos no autorizados y salvaguardando los datos usados por los sistemas aplicativos. Un enfoque sistemático deberá ser diseñado para verificar que la integridad de las bases de datos es mantenida en los centros de cómputo locales y remotos.
- *Telecomunicaciones.* "Telecomunicaciones". Las redes de telecomunicaciones han tenido más integración, más accesibilidad y se han vuelto más complejas, por lo que la necesidad de controles para evaluar las redes se ha incrementado. La tecnología de telecomunicaciones ha permitido una flexibilidad y una expansión en las redes de los sistemas y ha introducido nuevas áreas que requieren de controles (esto es, la seguridad en la transmisión de los datos, seguridad de acceso a la red, controles de respaldo y controles de hardware).
- *Computación de usuario final.* "Computación de usuario final y departamental". Debido a que el poder de cómputo le permite a las microcomputadoras trabajar "stand-alone", conectadas a una red de microcomputadoras o de

minicomputadoras o a un equipo mainframe, nuevos controles deberán ser desarrollados para que incluyan todas estas opciones.

- *Planeación de contingencias.* "Plan de contingencias". Muchas organizaciones dependen grandemente de los sistemas de información y no pueden sobrevivir a una pérdida completa de las capacidades de procesamiento de datos. La planeación de contingencias requiere de muchos recursos humanos y técnicos para prevenir tales pérdidas. El departamento de sistemas de información tiene la responsabilidad principal para realizar el plan de contingencias para cada centro de cómputo de la Organización. Los procedimientos y responsabilidades deberán ser claramente definidos y especificados.

Controles generales de los Sistemas de Información, su interrelación

Los controles de las aplicaciones son dependientes de los controles generales que soportan el procesamiento de datos en un ambiente de sistemas de información. Cuando un control de aplicación es identificado como crítico, el control general deberá ser efectivo para asegurar todo el tiempo la consistencia y operación de los controles de las aplicaciones. Por ejemplo, un control de aplicaciones incluye, por parte de un usuario, la revisión de un reporte de datos relacionados con la seguridad del programa de cómputo que produce el reporte (un control general) y los controles sobre las funciones de operaciones de cómputo que ejecuta el programa (un control general).

Esto es una sociedad entre los controles generales y las aplicaciones. Cuando diseñamos e implementamos controles de las aplicaciones, el efecto y contribución de los controles generales deberá de ser considerado para asegurar una estructura de control efectiva.

Cuando los controles de aplicaciones deberán de aplicarse en un periodo de tiempo, debemos asegurarnos que los controles generales son efectivos en ese mismo periodo de tiempo. Cualquier debilidad en los controles generales, tales como el control de acceso a los archivos de producción o el control de cambios, podrían anular los controles de las aplicaciones. Los controles de las aplicaciones que comparan las condiciones esperadas de un archivo contra las condiciones actuales y reporta las diferencias, también podría identificar debilidades potenciales en los controles generales (esto es, administración de datos, administración de archivos de producción, y operaciones de respaldo y recuperación).

La redundancia en los controles es apropiada en muchos ambientes para asegurar que las fallas de control que se pasaron en un punto son detectados por los controles en otra parte del proceso. Por ejemplo, cuando los controles de edición no permiten la captura de letras en un campo numérico, los controles del programa deberán validar esta condición antes de intentar realizar operaciones matemáticas. Los controles redundantes también son aplicados en la información recibida de fuentes externas.

Una redundancia de controles no es aceptada cuando una aplicación duplica el proceso que ya fue realizado por un control general. Por ejemplo, los procedimientos para

respaldo de aplicaciones pueden resultar en un gasto innecesario (esto es, la creación y mantenimiento de archivos innecesarios) si el respaldo no es coordinado con el área responsable de realizar los respaldos.

Nuevas tecnologías han alterado tanto las relaciones de los negocios y las estructuras de los sistemas de información, como la forma en la que son relacionadas y conducidas sus actividades. Un cambio en la tecnología podría requerir de diferentes enfoques para asociar los mismos objetivos de negocio. La integración de la tecnología con las aplicaciones y las operaciones de los sistemas de información nos debe dar un enfoque y perspectiva de auditoría diferente, para evaluar el ambiente de control.

Existe una tendencia de migrar los controles de las aplicaciones hacia los controles generales. Por ejemplo, el sistema de administración de bases de datos puede ser usado para restringir el acceso a las funciones críticas de una aplicación. Un control general de los sistemas de información puede impactar múltiples aplicaciones y es más confiable que un control de aplicaciones.

Más y más frecuentemente el auditor realiza revisiones a los controles generales de los sistemas de información y de las aplicaciones al mismo tiempo, para asegurar que todos los aspectos clave del sistema de control interno están siendo considerados durante la auditoría. Es difícil revisar una unidad de negocio y los procedimientos manuales de los usuarios sin la consideración de sistemas automatizados y de los controles generales de los sistemas de información, relacionados con la seguridad, con los programas, y con las

operaciones de cómputo. La coordinación e integración de las actividades de auditoría deberá de proveer información al proceso de administración de la auditoría que puede afectar significativamente el alcance y duración de la auditoría. Por ejemplo, una auditoría a las funciones de control general de los sistemas de información, deberá de proveer información de la confiabilidad de controles tales como control de accesos, control de cambios de programas, administración de datos, y respaldos y recuperaciones, los cuales pueden impactar significativamente el nivel de las pruebas requeridas durante la aplicación de la auditoría.

Factores críticos para la clasificación de los controles

Existen diferentes factores críticos que deberán ser considerados cuando se clasifican los controles:

- ¿Qué es lo que el control intenta evitar?.
- ¿Cuál es el objetivo de clasificar los controles?.
- ¿Porqué son necesarios varios tipos de control?.
- ¿Cuál es la interdependencia de los controles y su clasificación?.

La clasificación de los controles soporta al sistema de Control Interno de la Organización y le permite a la administración diseñar procedimientos que tienen una buena relación de costo-beneficio para las actividades del negocio y son monitoreadas en el nivel apropiado de la administración. La identificación de los tipos de control le permite a la Organización el enfocar su atención en los componentes de la función del negocio a ser gobernadas

por controles específicos. A continuación de describe las clasificaciones de los controles y presenta un ejemplo de ellos.

Clasificación del control	Enfoque de la clasificación	Ejemplos de los controles
Preventivos, detectivos y correctivos	Cuándo es aplicado el control (estos es, antes, durante o después de que un error ocurra.	• Se requiere de un password para accesar las funciones del negocio (preventivo). • La preparación de reportes de excepciones para su posterior revisión (detectivos). • Procedimientos automáticos de recuperación de archivos para rehacer un archivo dañado (correctivo).
Discrecionales contra no discrecionales.	Quién ejecuta el control (las personas contra las máquinas) y el grado en el cuál el control puede ser saltado.	• La revisión del supervisor de firmas autorizadas (discrecional). • Digitar forzosamente la digitación del NIP para poder usar un cajero automático (no discrecional).
Voluntario contra obligatorio	Quién impuso la necesidad del control (externo o interno).	• Razonabilidad de los controles para realizar pagos (voluntario). • Controles en la exportación de divisas, en países donde hay restricciones en el control de las divisa (obligatorio).
Manual contra automatizado	Cómo es implementado el control (esto es, con o sin automatización)	• La preparación por una persona de un documento o papel para amarrar las cifras control de las salidas contra las entradas (manual). • Chequeo computarizado de números de cuenta contra un catálogo de cuentas autorizadas mantenido por el computador (automatizado).
General contra aplicaciones.	Donde se localiza el control (está enfocado a las transacciones individuales o está enfocado al ambiente donde son procesadas las transacciones).	• Mantener una fuerte función de seguridad de los sistemas de información (generales). • Amarrar cifras de control computarizadas entre subfunciones de un sistema automatizado (aplicaciones).

Existe una interdependencia de los controles y sus clasificaciones. Las consideraciones de costo-beneficio de los controles implementados nos darán el nivel de integración de los controles.

Una mezcla de costos-beneficios de diferentes controles es usada para obtener un ambiente de control más fuerte.

	Tipo de control	Ejemplos de procedimientos de control.				
		A	B	C	D	E
Clasificación número 1.	Preventivo	X		X	X	
	Detectivo		X			X
	Correctivo				X	
Clasificación número 2.	Discrecional		X	X		
	No discrecional	X			X	X
Clasificación número 3.	Voluntario	X	X	X	X	
	Obligatorio					X
Clasificación número 4.	Automatizado	X	X		X	X
	Manual			X		
Clasificación número 5.	Aplicaciones	X	X	X		X
	Generales	X			X	

Ejemplos de los procedimientos de control.

A.- Medidas de seguridad (esto es, firmarse en la terminal o microcomputadora con la clave de usuario y password), restringe en forma general el acceso a los recursos de cómputo y a datos específicos.

B.- Revisión automática en la captura de importes, validando un rango en los porcentajes de los incrementos de sueldos. La transacción es aceptada y el sistema genera un reporte con todas las excepciones.

C.- El usuario checa las aprobaciones de la administración en los gastos de los empleados, antes de que sean capturados.

D.- Procedimientos de recuperación automática de archivos, que permiten la reconstrucción de archivos dañados.

E.- Reportar las transacciones con grandes importes, éstas deberán ser conocidas por las instituciones financieras.

3.4.- Controles del software de microcomputadoras

Los controles deberán ser establecidos sobre la adquisición y desarrollo del software de aplicaciones también como para las licencias de programas de aplicación. En adición la documentación del software de aplicaciones deberá ser mantenida.

Desarrollo y adquisición de software de aplicaciones

Objetivo de control.

La Dirección General de la Organización (DGO) deberá establecer políticas para establecer las guías para el desarrollo o adquisición de software aplicativo para microcomputadoras.

Consideraciones de auditoría.

Las políticas establecidas por la DGO acerca del desarrollo y adquisición de software aplicativo, deberán ser revisadas.

- ⇨ Determinar si los procedimientos para desarrollo y adquisición de software aplicativo para microcomputadoras está conforme a la Metodología de DGO

- Determinar si la DGO ha emitido políticas que provean una guía en la alternativa de desarrollo o compra de software aplicativo para microcomputadoras, y en estas políticas se consideren por lo menos:
  - Que los estándares para documentar el análisis, estén de acuerdo a las políticas.
  - Que los requerimientos legales deban ser dados a conocer por el dueño del código fuente.
  - El mantenimiento del hardware y del software.
  - La documentación de la aplicación.
- Determinar si la DGO ha emitido políticas relacionadas a la compra de software de aplicación a través del departamento de compras, para tener las ventajas de los descuentos por las compras por volumen, el manejo de licencias y otros beneficios.
- Establecer si los procedimientos organizacionales para comprar software aplicativo requieren de el nombre de un producto específico en la requisición, las siguientes preguntas deberán ser contestadas antes de ser llenada la requisición de compras:
  - ¿Es el paquete de software compatible con el hardware y software de las microcomputadoras que están siendo usadas por la Organización?.
  - ¿El paquete de software contiene cláusulas de integridad de datos, en las cuales el proveedor del software toma la responsabilidad de los errores del software, o daños al software o provocados a otros softwares?

- ¿Los procedimientos disponibles nos pueden asegurar que el paquete del software comprado es una copia legítima y que está libre de virus?

- Determinar si la DGO ha designado a miembros del personal específicos para desarrollar en microcomputadoras software de aplicaciones y para evaluar el software de programas aplicativos ofrecidos por los proveedores para las microcomputadoras.
- Valorar el grado de involucramiento de la Gerencia del Departamento en la determinación de si el software para microcomputadoras deberá ser desarrollado o comprado.
- Determinar si un análisis de costo-beneficio es desarrollado antes de que la Organización decida si el software deberá ser desarrollado o comprado.
- Determinar si las guías organizacionales para desarrollar aplicaciones en microcomputadora bajo contrato provee de:
  - Revisión y aprobación, de la Dirección, de los requerimientos para tales servicios.
  - Asegurarse de que el proveedor de los servicios cumplirá con los estándares usados por la Organización para el manejo de archivos, nombres convencionales, documentación de los programas y procedimientos de prueba.
  - La determinación de los servicios a ser ejecutados y los productos a ser obtenidos, por el proveedor de la Organización deberán ser claramente definidos y completamente realizables.

- Asegurarse de que las cantidades pagadas al proveedor están conforme a lo previsto y de acuerdo con la Organización y reflejan el trabajo realmente hecho.

- Determinar si los procedimientos que han sido establecidos le permiten al departamento usuario aprobar y aceptar el software aplicativo desarrollado para las microcomputadoras.
- Determinar si los departamentos usuarios requieren que la documentación provelda sea aprobada por el área de Sistemas antes de que el software aplicativo haya sido desarrollado para el Departamento usuario.
- Determinar si las aprobaciones y aceptaciones necesarias por la Gerencia del departamento usuario han sido aseguradas cuando el área de Sistemas ha modificado algún paquete de software aplicativo.
- Determinar si las aprobaciones por la Gerencia del área de Sistemas han sido aseguradas antes de que el usuario modifique algún programa del paquete del software aplicativo.

Biblioteca de programas aplicativos con licencia

Objetivo de control.

Si los programas aplicativos de microcomputadoras son compartidos por un número de diferentes usuarios bajo una misma licencia del producto desarrollador, los procedimientos deberán ser establecidos por la Dirección para registrar las actividades de los usuarios.

Consideraciones de auditoría.

Los procedimientos establecidos por la Dirección para registrar las licencias de uso compartidas por un programa aplicativo de microcomputadora, deberán ser revisados.

- Determinar si la Dirección ha designado miembros específicos del personal del área de Sistemas para actuar como responsables de las bibliotecas de programas aplicativos para microcomputadoras y para registrar los movimientos y regresos de programas específicos.
- Determinar si los procedimientos que han sido establecidos por la Dirección nos aseguran que los programas aplicativos para microcomputadoras están protegidos contra copiado o modificación.
- Determinar si la Dirección ha establecido procedimientos para asegurar un manejo y almacenamiento apropiado de los medios magnéticos que contienen las licencias de los programas aplicativos para microcomputadoras.
- Determinar, considerando que los programas aplicativos para microcomputadoras son usados para accesar datos mantenidos en el mainframe y estos programas aplicativos no están protegidos contra el copiado y modificación, si:
  - Procedimientos adecuados han sido establecidos para identificar cualquier cambio que pudo haber sido hecho en el programa durante el periodo que fue prestado a un usuario determinado.
  - El programa aplicativo de microcomputadora tiene rutinas que aseguran que al programa no le han hecho modificaciones y tampoco puede ser copiado mientras se encuentre en uso.

- Establecer que cualquier cambio realizado a programas aplicativos para microcomputadoras, ha sido aprobado por todos los usuarios de los departamentos afectados por el cambio, antes de que los cambios sean hechos.
- Determinar si los procedimientos han sido establecidos dentro de la Organización para asegurar que las copias no autorizadas de los programas bajo licencia no son mantenidos en las microcomputadoras equipadas con disco duro.

Documentación de los programas de procesamiento

Objetivo de control.

La DGO deberá establecer procedimientos para catalogar los programas aplicativos dentro de las microcomputadoras y asegurar que una lista de estos programas es creada y es mantenida actualizada.

Consideraciones de auditoría.

Los procedimientos de la Organización para catalogar y listar los programas aplicativos para microcomputadoras, deberán ser revisados.

- Determinar si la Organización ha designado a miembros específicos del personal del área de Sistemas para catalogar todos los programas aplicativos para microcomputadoras y para desarrollar una lista de estos programas.

- Valorar, considerando que los programas aplicativos para microcomputadoras son usados en aplicaciones para el procesamiento de datos para accesar datos mantenidos en el mainframe, si:
  - La documentación está al corriente.
  - Esta documentación es mantenida de una forma segura en áreas que no son accesibles a todos los departamentos usuarios.
  - El software de aplicación para microcomputadoras de uso común está protegido contra borrado.
  - Programas más importantes de aplicación para microcomputadoras está sujeto a controles de desarrollo formales.
- Determinar si la documentación de los programas de aplicación para microcomputadoras incluyen lo siguiente:
  - Nombre de la operación y fecha de creación.
  - Autor del programa y uso.
  - Nombre del programa.
  - Localización del programa.
  - Nombre del archivo de datos.
  - Localización del archivo de datos.
  - Estructura del archivo de datos.
  - Descripción de la operación.

- Fecha de la documentación.
- Impresión del programa.
- Diagrama de flujo.
- Ejemplos de los reportes generados.

3.5.- Controles de archivos de microcomputadoras

La Dirección deberá asegurar que los controles que han sido establecidos e implementados controlaran tanto a los datos como a los archivos.

Archivos de datos

Objetivo de control.

Considerando que las microcomputadoras han sido autorizadas para accesar datos en las operaciones de procesamiento de datos del mainframe o son usadas en aplicaciones "stand-alone", los procedimientos deberán ser establecidos por DGO para tratar con la creación y mantenimiento de los archivos de datos en estas microcomputadoras.

Consideraciones de auditoría.

Los procedimientos organizacionales para la creación y mantenimiento de archivos de datos en las microcomputadoras deberán de ser autorizadas para accesar datos en las operaciones de procesamiento de datos del mainframe o para ser usadas en aplicaciones "stand-alone", deberán ser revisadas.

- Determinar si formatos de registro estándar han sido aprobados para la creación y uso de archivos de datos para las microcomputadoras de la Organización.
- Valorar si los procedimientos de conversión de datos usados por las microcomputadoras de la Organización han sido documentados y son adecuados.
- Determinar si las cifras control u otros chequeos programados han sido construidos rutinariamente dentro de los archivos de datos creados y usados por las microcomputadoras de la Organización.
- Valorar si los procedimientos organizacionales para la catalogación, almacenamiento y respaldo de los archivos de datos de las microcomputadoras por los usuarios, son adecuados.
- Determinar si los controles tales como empacado son usados para regular la velocidad de transmisión de las transferencias de archivos de datos desde las microcomputadoras del Departamento al área de Sistemas y evitan la sobrecarga de los buffers usados, causando el alentamiento de la red de comunicaciones.
- Examinar la frecuencia de la bajada de archivos (copiar archivos de las operaciones de procesamiento del mainframe a una microcomputadora seleccionada) y determinar el alcance de la redundancia de archivos de datos y el "overhead" de procesamiento creado por esta práctica. Considerar la factibilidad y el costo efectivo del uso por la Organización de los métodos alternativos de distribución de copias de archivos de datos en diferentes

microcomputadoras, como a través de una minicomputadora intermedia, una red de microcomputadoras, o una transferencia de medios de almacenamientos magnéticos de datos.

- Determinar si los archivos de datos sensitivos o confidenciales creados y usados por las microcomputadoras son rutinariamente encriptados.

Archivos de transacciones

Objetivo de control.

Considerando que las microcomputadoras son aprobadas para accesar datos mantenidos por las operaciones de procesamiento de datos del mainframe o para ser usadas en modo "stand-alone", los procedimientos para inicio, aprobación y verificación de transacciones de datos desde la microcomputadora deberán ser establecidas por la DGO.

Consideraciones de auditoría.

Los procedimientos organizacionales para el inicio, aprobación y verificación de transacciones de datos para microcomputadoras deberán aprobar el acceso a los datos mantenidos por las operaciones de procesamiento de datos del mainframe o para ser usadas en modo "stand-alone", deberán ser revisados.

- Determinar, considerando que las transacciones son metidas usando una microcomputadora como una terminal, que las características del control mantenido por las operaciones de procesamiento de datos del mainframe tales como validación del user y password, no están siendo sesgadas.

- Determinar si los individuos dentro de los departamentos usuarios, quienes inician las transacciones a través de las microcomputadoras, no tienen la responsabilidad del desarrollo de programas aplicativos.
- Evaluar si las transacciones iniciadas a través de una microcomputadora están propiamente aprobadas y documentadas.
- Determinar si todas las transacciones creadas por las microcomputadoras de la Organización son registradas e incluyen cifras de control, totales parciales, conteo de documentos u otros controles programados similares y evaluar los procedimientos para establecer y comparar estos totales para chequeo.
- Determinar si los registros del control de totales creados por las microcomputadoras de la Organización son retenidos para un seguimiento posterior.

3.6.- Controles de seguridad en las microcomputadoras

La Dirección deberá asegurar que los controles sean implementados sobre el acceso a los recursos físicos incluyendo el hardware. Estas guías deberán estar enfocadas a los programas, datos, respaldos lógicos y seguridades.

Acceso a los recursos de las microcomputadoras

Objetivo de control.

Los procedimientos para usar microcomputadoras para garantizar el acceso a los mantenimientos de datos por el área de operación de procesamientos de datos del mainframe deberán ser establecidas por la DGO.

Consideraciones de auditoría.

Los procedimientos establecidos por la DGO para permitir el acceso por medio de las microcomputadoras a los datos del mainframe, deberán ser revisados.

- Determinar si la DGO debería aprobar usuarios específicos o microcomputadoras para requerir el acceso a los datos del mainframe.
- Determinar si los códigos, passwords u otros dispositivos o mecanismos son usados para identificar a los usuarios de las microcomputadoras autorizados y verificar si el acceso a estos passwords o códigos está restringido.

- Determinar si el uso de programas de discado ("dial-up") para digitar el password del usuario de las microcomputadoras están prohibidos.
- Determinar si los códigos, matrices u otros esquemas son usados para identificar el nivel del recurso al cuál cada usuario de microcomputadora está autorizado.

Respaldos de programas y datos y seguridad

Objetivo de control.

La DGO deberá establecer guías para respaldar de las microcomputadoras los programas de aplicación, los archivos de datos y la documentación asociada a ellos.

Consideraciones de auditoría.

Las guías para realizar los respaldos de las microcomputadoras los programas de aplicación, los archivos de datos y la documentación asociada a ellos, deberán ser revisadas.

- Verificar si un inventario actualizado es mantenido, el cuál contiene todos los medios magnéticos usados en las microcomputadoras de la Organización.
- Determinar si la DGO ha emitido guías adecuadas para respaldar los programas de aplicación de las microcomputadoras, archivos de datos y la documentación asociada a ellos.
- Valorar si las facilidades de almacenamiento de los programas de aplicación de las microcomputadoras, de los archivos de datos y de la documentación asociada a ellos, están de acuerdo a los requerimientos de protección contra fuego.
- Determinar si los programas aplicativos originales, las copias de los programas aplicativos, datos sensitivos o críticos, y la documentación asociada a ellos, son guardados en un almacén fuera del centro de cómputo.
- Determinar si los individuos quienes usan los microcomputadoras de la Organización para realizar procesos críticos, patentados, o información sensitiva, tienen custodiados los disquetes en una forma segura cuando se alejan del área de trabajo en la cuál la microcomputadora está localizada.
- Determinar si el plan de recuperación en casos de desastres incluye el uso de las microcomputadoras.

- Verificar que los programas o archivos de datos sensitivos, patentados o confiables usados en las microcomputadoras de la Organización, son encriptados si se encuentran en el disco duro o en disquetes.
- Determinar que los archivos fuente de los programas de aplicación de las microcomputadoras están protegidos contra modificaciones no autorizadas, manejando versiones de archivos solo de lectura.
- Evaluar si el uso de las utilierías de sistema operativo de las microcomputadoras se encuentra controlado apropiadamente.

Seguridad física del hardware

Objetivo de control.

Procedimientos adecuados deberán ser establecidos para asegurar que el hardware de las microcomputadoras no será robado o vandalizado.

Consideraciones de auditoría.

La existencia de controles adecuados para prevenir el robo o daño al hardware de las microcomputadoras, deberá ser revisado.

- Determinar si los cuartos en donde se encuentra localizadas las microcomputadoras se encuentran cerrados bajo llave después de la terminación normal de labores y si las microcomputadoras se encuentran fijas o ancladas a las mesas de trabajo dentro de estos cuartos.
- Determinar si los componentes de las microcomputadoras de la Organización han sido marcados con un número de identificación indeleble o irremovible.

- Determinar si todos los números de identificación, números de serie, y descripciones de equipo asociados con las microcomputadoras de la Organización son registrados y almacenados en un lugar seguro.
- Determinar si las microcomputadoras de la Organización se encuentran protegidas con cubiertas contra polvo cuando no están en uso.
- Determinar si cada una de las microcomputadoras de la Organización están protegidas contra descargas eléctricas o contra fallas de energía, averiguar si las microcomputadoras que contienen información crítica o confidencial se encuentra conectadas a un equipo de energía continua (no-break).
- Verificar si un extinguidor de fuegos está localizado cerca del lugar donde se encuentran las microcomputadoras.
- Verificar si en cada una de las microcomputadoras de la Organización se encuentra colocado un software que dé sign-off a la microcomputadora cuando no se encuentre en uso.

3.7.- Controles de procesamiento en las microcomputadoras

Los controles implementados por la administración sobre el procesamiento de datos en las microcomputadoras deberá incluir el mantenimiento al equipo, entrenamiento del personal, comunicación de datos y pistas de auditoría de los recursos usados.

Controles principales

Objetivo de control.

La DGO deberá valorar los riesgos asociados con el uso de las microcomputadoras y analizar las consideraciones de costo-beneficio de los controles que serán implementados en su uso.

Consideraciones de auditoría.

Los riesgos asociados con el uso de las microcomputadoras de la Organización y los controles principales que serán empleados, deberán ser valorados.

- Determinar si los riesgos asociados con el uso de las microcomputadoras han sido evaluados en cuanto a:
  - La clasificación de los tipos de aplicaciones dentro de las microcomputadoras, como contables, administrativos, analíticos, procesadores de texto, automatización de oficinas, etc.
  - Medir la sensibilidad y vulnerabilidad de los datos usados en cada una de estas aplicaciones.
- Determinar si un análisis de costo-beneficio de los controles principales usados en las microcomputadoras ha sido realizado por la Organización.
- Valorar la razonabilidad de las conclusiones obtenidas por la Dirección, de la valuación de los riesgos y del análisis costo-beneficio de las microcomputadoras usadas en la Organización.

Operación de microcomputadoras

Objetivo de control.

Los procedimientos adecuados para regular la operación de las microcomputadoras deberán ser establecidos por la Dirección.

Consideraciones de auditoría.

Los procedimientos organizacionales deberán ser revisados para asegurar que las microcomputadoras están siendo usadas de una forma consistente y los recursos asociados con éstas están de acuerdo a los estándares definidos por la Dirección.

- Determinar si el personal que opera las microcomputadoras de la Organización ha recibido un entrenamiento adecuado a su función.
- Verificar si más de una persona está familiarizada con la operación de cada una de las aplicaciones críticas o sensitivas que corren en las microcomputadoras.
- Determinar si los procedimientos de mantenimiento básico han sido realizados en forma regular a las microcomputadoras de la Organización.
- Verificar que: solo los programas y archivos de datos autorizados son mantenidos en el disco duro de las microcomputadoras de la Organización y que éstos no pueden ser copiados o modificados sin autorización. Verificar además que los programas y archivos de datos que no son del uso común, son borrados del disco duro.
- Determinar si una convención de nombres estándar ha sido establecida para ser usada en las aplicaciones y archivos de datos usados en las microcomputadoras.
- Determinar si una calendarización de operaciones es mantenida para todas las microcomputadoras de la Organización como el proceso de nómina y otras aplicaciones que corren en forma cíclica.

Comunicación de datos en las microcomputadoras

Objetivo de control.

La Dirección deberá establecer procedimientos para controlar y registrar el movimiento de las transacciones, registros y archivos de datos a través de sus microcomputadoras y con otras organizaciones.

Consideraciones de auditoría.

Los procedimientos para controlar las transacciones, registros y archivos de datos a través de redes internas y externas de microcomputadoras, deberán ser revisados.

- Examinar los comandos usados en la comunicación entre microcomputadoras y determinar si están conforme a los procedimientos relevantes de la Organización.
- Determinar si las microcomputadoras conectadas a una red pública de telecomunicaciones son puestas en modo de recepción, para recibir archivos de datos y varias fuentes de información, y si esta actividad está controlada adecuadamente a través del uso de passwords. Verificar que los archivos de datos y los programas de aplicación almacenados en estas microcomputadoras no pueden ser borrados o modificados remotamente, sin la autorización adecuada y a través de los controles para cambios de datos.

Documentación de los procesos que corren en las microcomputadoras

Objetivo de control.

Considerando que las microcomputadoras están aprobadas para accesar los datos mantenidos en el mainframe o serán usadas en aplicaciones "stand-alone", la Dirección deberá establecer los procedimientos para registrar el uso de las microcomputadoras.

Consideraciones de auditoría.

El registro del uso de las microcomputadoras que accesan datos del mainframe o son usadas "stand-alone", deberá ser revisado.

- Determinar el alcance, naturaleza y suficiencia de los registros de uso de las microcomputadoras usadas en la Organización.
- Determinar que todas las transacciones procesadas por las microcomputadoras de la Organización son registradas.

3.8.- Calidad del Software

El término calidad es ambiguamente definido y pocas veces comprendido, esto se debe porque: *La calidad no es una sola idea, es un concepto multidimensional;* la dimensión de calidad incluye el interés de la entidad, el punto de vista de la entidad, y los atributos de la entidad; por cada concepto existen diferentes niveles de abstracción, varía para cada persona en particular.

Podemos clasificar a la calidad bajo dos puntos de vista, *popular y profesional.*

Punto de vista popular

La calidad contiene características intangibles, términos como alta, baja, y buena calidad son utilizados sin intentar definirlos.

Punto de vista profesional

Juran(1970)[8] definió la calidad como "adaptabilidad de uso", esto implica dos parámetros: calidad de diseño y calidad de conformidad. Es decir, adaptable a la necesidad de los usuarios.

Crosby(1979)[8] definió la calidad como la "conformidad con los requerimientos."

Los factores de calidad deben ser:

Ausencia de defectos;
Satisfacción del usuario;
Conformidad con los requerimientos.

Sin lugar a dudas el factor inherente sobre calidad de software es la ausencia de defectos, este factor usualmente se expresa de dos maneras: *tasa de defecto* (número de defectos) y *confiabilidad* (número de fallas por *n* horas de operación, tiempo medio entre fallas, otra probabilidad de libre de fallas por unidad de tiempo).

La satisfacción del usuario usualmente es medida por porcentaje de *satisfacción* o *insatisfacción*. Para evitar prejuicios se utiliza las técnicas de estudio o encuesta ciega (el

entrevistador no sabe quién es el cliente, y el cliente no sabe a qué empresa representa el entrevistador).

Características de la calidad del software

Según la norma **ISO 9126,** las características presentes para la calidad del software son *portabilidad, eficiencia, confiabilidad, usabilidad, funcionalidad y mantenibilidad.*

Algunas empresas definen sus propios factores/atributos de calidad de software, por ejemplo en el caso de IBM se enfoca hacia:

Capacidad(funcionalidad), usabilidad, performance, confiabilidad, instalación, mantenabilidad, documentación/información, servicio, y "totalidad".

En el caso de Hewlett-Packard se enfoca hacia:

Funcionalidad, usabilidad, confiabilidad, performance, servicio.

La gestión de la calidad se puede entender como el conjunto de actividades y medios necesarios para definir e implantar un sistema de la calidad, por una parte, y responsabilizarse de su control, aseguramiento y mejora continua, por otra. En este sentido, la gestión de la calidad en cualquier organización (y, por supuesto, en las dedicadas al desarrollo y mantenimiento de software) cuenta con dos niveles de trabajo:

- El nivel de entidad u organización, donde se trata de crear y gestionar una infraestructura que fomente la calidad de los productos software mediante la

adecuación y mejora de las actividades y procesos involucrados en su producción e, incluso, en su comercialización y en la interacción con los clientes.

- El nivel de proyecto, donde las guías que la infraestructura organizativa prevé para las distintas actividades de desarrollo y mantenimiento de software deben ser adaptadas a las características concretas del proyecto y de su entorno para ser aplicadas en la práctica.

Calidad al nivel de organización

Dentro del primer nivel de acción, la gestión de la calidad en organizaciones de software ha seguido dos líneas que pueden ser complementarias entre sí:

- Por una parte, se ha seguido la línea marcada por las entidades internacionales de estandarización para todas las organizaciones de producción o servicios. Principalmente, se ha impuesto en la práctica las directrices marcadas por **ISO** (*Organization for International Standarization*) a través de su serie de normas ISO 9000 para la gestión de calidad. En el caso del software es principalmente aplicable la norma ISO 9001 [ISO, 1994a], aunque en los últimos años se está incrementando el número de organizaciones de este sector adheridas a la norma ISO 9002 [ISO, 1994b], en buena parte debido a que es más fácil conseguir certificación por esta norma, dejando a un lado cumplir los apartados sobre diseño (aunque se realice diseño). Debido a que el sector del software

difiere por la naturaleza del producto tanto del resto de sectores productivos, ha sido necesario crear una guía específica para su aplicación a este sector: el anexo ISO 9000-3 [ISO, 1997]. En esta línea de trabajo, se trabaja bajo el supuesto principal no tanto de asegurar a los clientes directamente la calidad de los productos sino de trabajar en la calidad del proceso empleado en su producción como medio indirecto de asegurar un buen nivel de calidad en los productos.

- Por otra parte, el mundo del software ha creado su propio línea de trabajo en la gestión de la calidad del software tomando las ideas básicas de la anterior, es decir, trabajar sobre los procesos de producción de software como medio de asegurar la calidad del producto software. Así, se comenzó en el SEI (Software Engineering Institute) de EE.UU. proponiendo un modelo de clasificación y mejora de los procesos empleados por las organizaciones de software denominado CMM [Paulk *et al.*, 1993]. Su trabajo se centra en el estudio y clasificación de los distintos procesos involucrados en la producción de software bajo el enfoque de una serie de niveles de madurez. Sobre este modelo pionero, se han creado nuevos modelos que suponen tanto actualizaciones y variantes por parte del propio SEI o de su entorno como de otros ámbitos (por ejemplo, europeos) [Calvo y Fernández, 1996]. La última aportación en esta línea de trabajo es el modelo SPICE [UNE 15504, 1994], estandarizado por ISO y que pretende ser el modelo de software que recoja las ideas tanto de los modelos de software (tipo CMM y similares) como de la línea marcada por ISO 9001.

Dentro de este nivel de actuación, el análisis de las necesidades de medición tiene una doble vertiente:

- Los modelos específicos de evaluación de procesos de software (como CMM o SPICE) suponen la clasificación de los mismos mediante análisis subjetivos cuyo resultado suele ser un valor en una escala ordinal. Bajo esta perspectiva, convendría analizar la adecuación, desde el punto de vista teórico y práctico, de las mediciones efectuadas sobre los procesos de software.

- Tanto ISO 9001 como los modelos específicos de evaluación de procesos de software suelen dictar una serie de requisitos de medición que deben cumplir las organizaciones que quieran acceder a un nivel de calidad de procesos determinado. Así, en el caso de ISO 9001 (mediante ISO 9000-3) se indica en uno de sus apartados la necesidad de realizar mediciones tanto de productos como de procesos en cada proyecto. En el caso de CMM, no se abordan directamente las necesidades de medición aunque hay publicaciones [Fenton y Pfleeger, 1997, pp. 88-94 y 470] que han preparado directrices de medición para cada uno de los niveles de madurez de proceso del modelo en función de sus características generales de aseguramiento de calidad. Bajo esta perspectiva, habría que estudiar los requisitos de medición que supone la adopción de cualquiera de los modelos citados (tanto en el esquema propuesto por ISO como en el de los modelos de procesos de software).

Calidad al nivel de proyecto

En cada proyecto de desarrollo, el aseguramiento de la calidad del software supone la aplicación de las guías de proceso marcadas por las disposiciones que, al nivel de organización, se han establecido, bien sea como un sistema de calidad bien definido o bien mediante una serie de procedimientos y estándares preceptivos. En cualquier caso, la medición supone, junto a las actividades de verificación y validación (básicamente, pruebas de software y actividades de revisión y auditoría), una de las técnicas principales previstas en los estándares para el control y el aseguramiento de la calidad [IEEE 1074, 1991]. Desde este punto de vista, la medición puede contribuir tanto en el control de los procesos y actividades como en el de los productos, para comprender la situación de los mismos o para controlar si cumplen los requisitos pedidos o un cierto nivel de calidad. Desde este punto de vista, cabe destacar dos importantes líneas de trabajo sobre medición:

- Por una parte, el concepto de calidad es demasiado complejo como para poder ser evaluado o medido mediante una única medida. La norma UNE-EN ISO 8402 [AENOR, 1995] define el Aseguramiento de la Calidad (AC) como "el conjunto de acciones planificadas y sistemáticas implantadas dentro del sistema de calidad, y demostrables si es necesario, para proporcionar la confianza adecuada de que una entidad cumplirá los requisitos para la calidad". Estos requisitos deben reflejar totalmente las necesidades y expectativas del usuario. En definitiva, el AC debe recoger el conjunto de acciones necesarias para asegurar que el cliente recibe el producto software acordado y, por tanto, queda satisfecho. Cada vez más se está asociando el concepto de calidad a la

satisfacción del usuario y este hecho supone una mayor complejidad y ambigüedad en la obtención de mediciones reales y fiables de la calidad del software. En cualquier caso, se reconoce comúnmente que la idea de calidad varía de un cliente a otro, de un proyecto a otro. De hecho, uno de los campos en los que más se ha trabajado es en la utilización de modelos de evaluación de calidad de software que tratan de aportar un medio para definir y descomponer el concepto de calidad de software en características más sencillas de evaluar y medir. Así, podemos encontrar modelos de evaluación generales como el FCM (Factores/Criterios/Métricas) [McCall et al., 1977], métodos para crear modelos propios en cada proyecto como COQUAMO [Kitchenham y Walker, 1989] o el de Gilb [Gilb, 1987] e, incluso, estándares que abordan esta cuestión como ISO 9126 [ISO 9126, 1991] o IEEE 1061 [IEEE 1061, 1992]. En este campo, sería necesario trabajar en el análisis de la adecuación, tanto teórica como práctica, de este tipo de modelos y métodos para evaluar la calidad y en su aplicación en la práctica de proyectos.

- Por otra parte, se han propuesto multitud de mediciones, principalmente de productos, que proclaman su utilidad para evaluar la calidad del software, o alguna de sus facetas. En este caso, el trabajo debería centrarse en analizar cada una de las propuestas (tanto teóricamente como en la práctica), cómo contribuyen o se pueden usar para el aseguramiento de la calidad en un proyecto y qué característica miden realmente y si pueden encajar dentro de los anteriormente mencionados modelos de evaluación de calidad de software y dentro de las actividades de aseguramiento de calidad.

4.- AUDITORÍA DE DESARROLLO Y MANTENIMIENTO DE SISTEMAS

El presente capítulo es el más importante de todos, sin restarles importancia alguna a los capítulos anteriores, sin embargo aún y cuando los tres primeros dan un marco histórico y conceptual de lo que es la Auditoría, en éste se desarrolla lo que es la Auditoría de Desarrollo y Mantenimiento de Sistemas, así como sus riesgos y controles a considerar por los Auditores de Sistemas de Información durante su evaluación de controles al Área de Desarrollo y Mantenimiento de Sistemas.

4.1.- Desarrollo de los Sistemas de Información

El objetivo del auditor de sistemas de información es: evaluar la metodología y los procesos por medio de los cuales se aborda el desarrollo, la adquisición, la implementación y el mantenimiento de los sistemas de aplicaciones de negocios para asegurar que los mismos satisfagan los objetivos del negocio de la organización.

Las compañías comprometen con frecuencia, recursos significativos al desarrollo, la adquisición y el mantenimiento de los sistemas de información. Estos sistemas controlan a menudo los activos de una organización y pueden en si mismos considerarse un activo que necesita ser protegido y controlado.

Una aplicación o proyecto comienza cuando se presenta una de las siguientes situaciones:

- Una nueva oportunidad que se relaciona con un proceso de negocio nuevo o ya existente.
- Un problema que se relaciona con un proceso actual del negocio.
- Una nueva oportunidad que permitirá que la organización obtenga ventajas de la tecnología.
- Un problema con la tecnología existente.

Los proyectos deben iniciarse usando procedimientos bien definidos para comunicar las necesidades del negocio a la gerencia, estos procedimientos requieren a menudo, documentación detallada que identifique la necesidad del problema, que especifique la solución que desea y que relaciona los beneficios potenciales para la organización: se deberán identificar todos los factores internos y externos afectados por el problema y cómo afectan estos a la corporación.

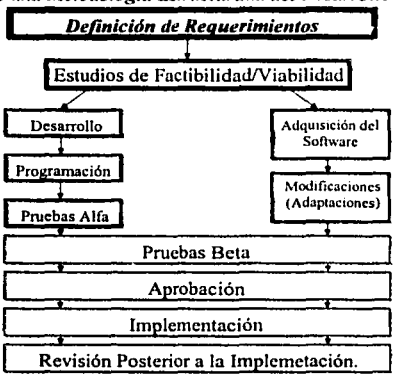
Una metodología estructurada de desarrollo, con fases definidas y con puntos específicos de revisión y evaluación puede brindar las siguientes ventajas para los Auditores de Sistemas de Información (ASI).

- Se incrementa de manera significativa su influencia, cuando existen procedimientos formales y lineamientos (directrices) que identifican cada fase del ciclo de vida del sistema.
- Se incrementa el alcance de su participación.

- Pueden revisar todas las áreas y fases relevantes del proyecto de sistemas y reportar de forma independiente a la Dirección / Gerencia sobre la adhesión a los objetivos planificados y a los procedimientos de la compañía.
- Pueden identificar partes seleccionas del sistema y llegar a involucrarse en los aspectos técnicos sobre la base de sus conocimientos y habilidades.
- Pueden llevar a cabo una evaluación de los métodos y de las técnicas aplicadas en el proyecto del desarrollo del sistema.

Una metodología estructurada de desarrollo de sistema se constituye como lo presenta el siguiente diagrama.

Diagrama de una Metodología Estructurada del Desarrollo de Sistema.



Es esencial que el ASI entienda la metodología de desarrollo, adquisición y mantenimiento de sistemas en uso para identificar las vulnerabilidades potenciales y los

puntos que requiere encontrar. Si faltan controles o si el proceso es desordenado, la función del ASI es notificar las deficiencias al equipo del proyecto y a la Alta Dirección, también puede ser necesario notificar a los que están involucrados en las actividades de desarrollo y de adquisición sobre los controles apropiados que se deben implementar y seguir.

Riesgos Asociados con una Metodología Inadecuada del Ciclo de Vida del Desarrollo de Sistemas (CVDS)

Existen muchos riegos potenciales que pueden presentarse cuando se utilizan metodologías deficientes o inadecuadas de CVDS, el primero y el más importante es que el resultado final del proceso o el nuevo sistema no satisface las necesidades del negocio, los requerimientos y las expectativas del usuario. Los requerimientos del negocio que debían ser resueltos por el nuevo sistema aún no se han satisfecho y el proceso ha sido un derroche de recursos; e incluso, aún cuando el sistema se implemente muy probablemente será subutilizado y no se le dará mantenimiento, lo que lo hará obsoleto en un período corto de tiempo.

Los sistemas diseñados mediante la utilización de una metodología deficiente de CVDS a menudo excederán los límites de los recursos financieros destinados para el proyecto y podrán ser completados con retraso, si alguna vez finalizan, una metodología inadecuado puede promover una administración deficiente o una administración (gestión) equivocada del proyecto.

Otros riesgos asociados con una metodología deficiente podrían colocar a la organización en una desventaja competitiva o traer como consecuencia que sea incompatible en los sistemas existentes, la perdida de oportunidades de negocios, una disminución de la credibilidad de los Sistemas de Información (SI) y perdida de motivación en los empleados.

El ASI debe estar conciente de que hacer seguimiento únicamente a una metodología de CVDS diseñada de manera adecuada no asegura que un proyecto de desarrollo culmine con éxito. El ASI debe revisar otros aspectos de desarrollo de sistemas, como por ejemplo la participación de los usuarios y el respaldo de la Alta Gerencia, además de cumplir con el CVDS de la organización.

4.2.- Metodología Estructurada (tradicional) del Ciclo de Vida del Desarrollo de Sistemas (CVDS)

Los esfuerzos en gran escala del CVDS se logran mejor por medio de una serie de pasos o de fases que tienen metas y objetivos definidos de fechas de terminación. Las fases reales para cada proyecto pueden variar dependiendo si se escoge una solución desarrollada o una adquirida. Los esfuerzos de mantenimiento de sistemas pueden no requerir el mismo nivel de detalle o las mismas fases que las nuevas aplicaciones, las fases y los productos se deben decidir durante las primeras etapas de la planificación del proyecto. Es importante mencionar que puede que no sean necesarias todas las etapas o pueden estar combinadas dependiendo del tamaño del proyecto y del tipo de herramientas que el equipo del proyecto esté utilizando.

La metodología debe contemplar que los requerimientos del negocio estén definidos con claridad antes de que se apruebe cualquier proyecto de desarrollo, implementación o modificación. COBIT (Control Objetives for Information and Related Technologies) afirma que "La metodología del Ciclo de Vida de Desarrollo de Sistemas debe requerir que los requerimientos funcionales y operativos de la solución sean especificados incluyendo rendimiento, seguridad, fiabilidad, compatibilidad y legislación".

También son críticos el financiamiento adecuado, los recursos y cronogramas (planes) de trabajo así como también el nivel de maestría (experiencia) con la que cuenta el personal de SI y los representantes del departamento de usuarios sobre la metodología escogida de CVDS. Finalmente, la metodología escogida debe encajar en las prácticas y tamaño, particulares de la Organización.

Estudio de Factibilidad / Viabilidad

Un estudio de factibilidad es el análisis para definir claramente la necesidad e identificar alternativas para resolverla, este es realizado una vez que se determina poner en marcha el proyecto de SI, determinando los beneficios estratégicos de implementar el sistema, con base en la productividad o bien evitando costos futuros; identifica y cuantifica los ahorros de costos de un nuevo sistema y estima un plan de reembolso de los costos incurridos al implementar el sistema.

Dentro de un estudio de factibilidad se deben tomar en cuenta los siguientes aspectos:

- Definir un periodo de tiempo que requiere la solución.

- Determinar si se requiere o desea una solución computarizada.
- Determinar si un sistema existente puede corregir la situación con muy poca o ninguna modificación.
- Determinar si un producto de algún proveedor ofrece una solución al problema.
- Determinar el costo aproximado para desarrollar el sistema para corregir la situación.
- Determinar si la solución encaja en la estrategia del negocio.
- Sobre la base de las respuestas y definiciones anteriores, determinar si la solución consistente en un sistema es apropiado y si es necesario desarrollar o adquirir el sistema.

Los factores que afectan a la decisión del desarrollo frente a la de adquirir son:

- Fecha en que se requiere que el sistema esté funcionando.
- El costo para desarrollar el sistema en comparación con el costo de comprarlo.
- Los recursos tanto en personal como en hardware que se requiere para desarrollar el sistema o para implementar una solución provista por un proveedor.
- Otros sistemas necesarios para proporcionar información o utilizar información del sistema adquirido el cual deberá estar en capacidad de interconectarse con el sistema.

Definición de Requerimientos

Es especialmente importante que todos los gerentes y grupos de usuarios se involucren activamente en este proceso para prevenir que se gasten recursos en un sistema que no vaya a satisfacer los requerimientos del negocio. La participación del usuario es necesaria para obtener un compromiso y dedicación y todos los beneficios del sistema. Sin el patrocinio de la Gerencia y sin tener requerimientos claramente definidos, probablemente nunca se logren beneficios.

Dentro de la fase de definición de requerimientos, se tiene en cuenta la siguiente:

- Definir el problema o la necesidad que requiere solución.
- Definir los requerimientos generales o importantes del sistema para la solución.

Los usuarios especifican sus necesidades (incluyen las no automatizadas así como también las automatizadas) y cómo desean que el sistema las resuelva, por ejemplo:

- Controles de acceso
- Requisitos legales
- Necesidades de información de la Gerencia
- Consideraciones operativas
  - Se desarrolla y se presenta a la Gerencia de usuarios un diseño general del sistema para que haga las modificaciones, lo apruebe y lo firme.
  - Se desarrolla un plan del proyecto para desarrollar, probar e implementar el sistema.

- Se obtienen compromisos de los desarrolladores de sistemas y de los departamentos de usuarios afectados para que aporten los recursos necesarios para completar el proyecto.

El no definir o administrar de manera adecuada los requerimientos de un sistema puede tener como consecuencia la aparición de riegos. El primero y el más importante de estos riegos es el "scope creep", el proceso a través del cual cambian los requerimientos durante el desarrollo. Se requiere un proceso bien definido y ejecutado de control de cambios para asegurar que los cambios sean incluidos sólo después de considerar los costos asociados en tiempo, recursos o licencias.

Nota: Si el resultado de la decisión de desarrollar (adquirir) es comprar un paquete de software suministrado por el vendedor, entonces el usuario debe participar activamente en la evaluación del paquete y en el proceso de selección.

Adquisición del Software

La Adquisición del Software no es considerada como una fase estándar en el CVDS. Sin embargo, si se decide adquirir software, en vez de desarrollarlo, la adquisición de software es el proceso que debe tener lugar después de la fase de definición de requerimientos.

El Estudio de Factibilidad y Viabilidad debe contener documentación que respalde la decisión de adquirir el software. Se debe constituir un equipo del proyecto con participación del personal de soporte técnico y de los usuarios claves para redactar una

Solicitud de Propuesta (SP) ésta debe ser enviada a diversos vendedores para determinar cual de sus productos ofrece la mejor solución al mejor precio. La SP debe incluir las áreas que están reflejadas en el siguiente cuadro.

Rubro	*Descripción.*
Producto frente a los requerimientos del sistema.	El producto del vendedor escogido debe estar tan cerca como sea posible de satisfacer requerimientos definidos del sistema. Si el producto ofrecido por el vendedor no satisface todos los requerimientos definidos, el equipo del proyecto, en especial los usuarios tendrán que decidir si aceptan las deficiencias. Una alternativa a vivir con las deficiencias de un producto es que, el vendedor o el comprador, hagan cambios de aceptación al producto.
Referencias del Cliente.	La Gerencia de proyectos debe verificar las referencias suministradas por el vendedor para validarlas y tener un concepto sobre el posible desempeño y realización del trabajo por el vendedor así como el desempeño del producto ofrecido.
Viabilidad (Estabilidad) Financiera del Vendedor.	El vendedor que suministre o que dé soporte al producto debe tener buena reputación y por lo tanto, debe proveer evidencia de su estabilidad financiera. Los vendedores nuevos tal vez no puedan demostrar su estabilidad financiera. Los vendedores nuevos, en especial si el producto es nuevo y/o usted es el primer cliente, presentan un riesgo substancialmente más alto para la organización.
Disponibilidad de Documentación Completa y Confiable.	El vendedor debe estar dispuesto y debe poder suministrar un juego completo de la documentación del sistema para su revisión antes de la adquisición , el nivel de detalle y de precisión que se encuentre en la documentación puede ser un indicador del detalle y de la precisión utilizada dentro del diseño y de la programación del sistema mismo.
Soporte del Vendedor.	El vendedor debe tener a disposición una línea completa de productos de apoyo para el paquete del software. Esto puede incluir una línea de ayuda 24 horas, siete días de la semana, entrenamiento (formación) local durante su implementación, actualizaciones del producto, notificación automática de nuevas versiones y mantenimiento local cuando se solicite.
Disponibilidad del Código Fuente.	El código fuente debe o bien ser recibido del vendedor al inicio o deben hacerse arreglos para adquirir el código fuente en caso de que el vendedor deje el negocio. Usualmente estas cláusulas forman parte de un contrato de fideicomiso del software (depósito de fuentes) en el cual un tercero tiene el software en fideicomiso (depósito de fuentes) si ocurriera algo así. La compañía que adquiere el software debe asegurarse de que las actualizaciones del producto y el mantenimiento del programa estén incluidas en el contrato de fideicomiso.
Número de años de experiencia en ofrecimiento del Producto.	Más años indica estabilidad y familiaridad con el negocio que el producto respalda.
Lista de actualizaciones recientes o planificadas del producto con sus fechas.	Una lista pequeña (corta) sugiere que el producto no se mantiene actualizado.
Número de clientes usando el producto en una lista de usuarios actuales.	Un número mayor sugiere una amplia aceptación del producto en el mercado.
Se debe permitir la realización de pruebas de aceptación del Producto antes de asumir el compromiso de Compra.	Esto es crucial para determinar si el producto satisface realmente los requerimientos de su sistema.

El equipo del proyecto necesita examinar detenidamente y comparar las respuestas de los vendedores a la SP. Después de haber examinado las respuestas a la SP, el equipo del proyecto podrá identificar un solo vendedor. Siempre que sea posible se debe realizar una visita a la compañía escogida con el fin de observar la funcionalidad de los productos en una forma parecida a la manera en que la compañía interesada en comprar el producto, usará estos.

El ASI debe animar al equipo del proyecto para que se comunique con los usuarios actuales. La información obtenida de estas discusiones o visitas puede determinar cual vendedor será escogido.

Las conversaciones con los usuarios actuales deben concentrarse en las características siguientes de cada vendedor:

- *Confianza* - ¿Se puede depender de los productos del vendedor(mejoras, actualizaciones o mantenimiento?
- *Nivel de Servicio* - ¿Puede el vendedor responder a los problemas que tienen sus productos? ¿El vendedor hace las entregas a tiempo?
- *Compromiso de brindar entrenamiento (formación) y documentación para su producto* - ¿Cuál es el nivel de satisfacción del cliente?

Sobre la base las respuestas a la SP y de las visitas a los usuarios actuales, el equipo del proyecto puede hacer una selección del producto. Las razones para hacer una elección en particular deben ser documentadas.

El último paso o fase en el proceso de adquisición es negociar y firmar un contrato para el producto escogido, el cual deberá contener los puntos siguientes:

- Descripción específica de los productos que se van a entregar y sus costos.
- Fechas de compromiso para la entrega de los productos.
- Compromisos de entrega de documentación, mantenimiento, actualizaciones, notificaciones de nuevas versiones y entrenamiento (formación).
- Conformidad para un contrato de fideicomiso del software (deposito de fuentes) si los productos no incluyen el código fuente.
- Descripción del soporte que se brindará durante la instalación.
- Disposición para permitir un periodo razonable de pruebas de aceptación, antes de comprometerse con la compra.
- Autorización para los cambios que deba hacer la compañía compradora
- Acuerdo de mantenimiento.
- Autorización para mantener una copia del software que pueda utilizarse en el proceso de continuidad del negocio.
- Programa de pagos vinculados con las fechas efectivas de entrega.

El riesgo de implementar un paquete de software de aplicación puede ser motivo de gran preocupación para los ASI, si lo controles de seguridad no están instalados en el software, puede llegar a ser difícil asegurar la integridad de los datos para la información que será procesada a través del sistema. Los riesgos involucrados con el paquete del software podrían ser pistas inadecuadas de auditoria, deficientes controles de

contraseñas y la seguridad general de la aplicación. Debido a estos riesgos es que el ASI debe establecer si estos controles están integrados en el software de aplicación.

Sistemas Integrados de Administración / Gestión de Recursos

Un número creciente de organizaciones tanto públicas como privadas, está desplazándose desde un conjunto de grupos separados de aplicaciones interrelacionadas a una solución corporativa totalmente integrada. Frecuentemente estas soluciones son comercializadas como soluciones de planificación de recursos de las empresas.

Este aspecto es tratado frecuentemente como un proyecto habitual de adquisición de software. En realidad eso tiene un impacto importante sobre la forma en que la corporación hace sus negocios, el entorno total de control, la dirección tecnológica y los recursos internos. En términos generales, se exige que una corporación convierta sus filosofías, políticas y practicas de administración en la solución integrada de software del proveedor, a pesar de las numerosas opciones de adaptación o personalización. En este sentido, dicha solución puede o bien dificultar o aumentar la capacidad de tecnología de información para respaldar la misión y las metas de la organización.

Cuando se considera un cambio de esta magnitud, es imperativo que se lleve a cabo un estudio minucioso de impacto y riesgo.

Antes de apoyar este proyecto global, la Alta Dirección debe estudiar y aprobar todos los cambios en la arquitectura de sistemas, la orientación tecnológica , las estrategias de migración y los presupuestos de SI.

Diseño Detallado (DD)

Si durante el estudio de factibilidad, se tomara la decisión de desarrollar el software que se requiere, será necesario desarrollar un diseño detallado. O si se tomara la decisión de adquirir el software de un vendedor, puede o puede que no se desarrolle un diseño detallado dependiendo de cómo satisface el producto del vendedor las especificaciones del usuario.

Un DD se desarrolla sobre la base del diseño general y las especificaciones de usuario desarrolladas en la fase de definición de requerimientos. Se asigna el equipo especifico de programación y los analistas y las especificaciones del sistema comienza a tomar forma. Es en esta fase que se presentan los diseños preliminares de pantalla y se obtienen especificaciones depuradas de los usuarios. Si se fuera a usar una herramienta de prototipos, es en este proceso de diseño de pantallas y de presentación donde dichos prototipos se usan con más frecuencia. A pesar de que la contribución del usuario puede ser mínima durante esta etapa, es imperativo que se incluya a los usuarios en las decisiones de diseño.

La etapa de diseño es donde se prueban tanto el diseño como la confiabilidad general del sistema de aplicación. Las pruebas se deben utilizar usando datos predeterminados bajo

condiciones controladas. Estoa segura que los datos sean procesados correctamente y que se va a obtener un producto confiable y en el formato deseado.

Los diagramas de flujo del sistema son desarrollados para ilustrar como fluirá la información a través del sistema. El DD debe también incluir los planes para convertir los datos y los procedimientos manuales desde el antiguo sistema al sistema nuevo. Los planes detallados de conversión disminuirán los problemas de implementación, debidos a incompatibilidad de los datos, a recursos insuficientes o a que el personal no esta familiarizado con las operaciones del nuevo sistema. Después de que se haya concluido el DD, incluyendo las aprobaciones de los usuarios, el diseño es distribuido a los desarrolladores del sistema para su codificación.

Programación

Esta fase utiliza el DD para iniciar la codificación del sistema. Las modificaciones hechas al software adquirido deben ser documentadas para asegurar que se puedan aplicar con precisión y totalmente las actualizaciones a las versiones futuras del código del vendedor.

Los desarrolladores de cada módulo deben crear la documentación del sistema. El grupo de desarrollo crea y prueba los programas para convertir los datos desde el viejo sistema. Todo el trabajo, en este punto, es realizado en un ambiente de pruebas. Los desarrolladores del sistema y/o los usuarios crean procedimientos de usuarios para manejar la transición al sistema nuevo. El entrenamiento inicial de los usuarios

seleccionados para el nuevo sistema, debe comenzar, ya que su participación va a ser necesaria en la siguiente etapa.

Los estándares de codificación de programa son un control esencial ya que sirven como un método de comunicación entre los miembros del equipo de desarrollo y entre el equipo y los usuarios durante el desarrollo del sistema. Ellas minimizan los contratiempos ocasionales en el desarrollo del sistema por la rotación del personal. También proveen el material que se necesita para usar con eficiencia el sistema y son requeridas para el mantenimiento y para llevar a cabo modificaciones a los programas.

Programación Estructurada (PE)

El Diseño Estructurado es un procedimiento para definir aplicaciones a través de una serie de datos o de diagramas de flujo de procesos, mostrando diversas relaciones, desde el nivel más alto, hasta el detalle. Los diagramas están hechos con esta misma estructura de arriba abajo. Los programas estructurados son más fáciles de desarrollar, entender y mantener ya que se dividen en módulos y secciones. Cada módulo realiza un número limitado de funciones y los módulos no son dependientes entre sí para realizar funciones.

Facilidades de Programación en Línea (On Line)

La Facilidad de Programación en Línea permite que los programadores codifiquen y compilen programas de manera interactiva con la computadora desde una terminal. A través de esta utilidad, los programadores pueden entrar, modificar y eliminar códigos de programación, compilar y almacenar programas (fuente y objeto) en la computadora y

listar programas. Las utilerías en línea (on line) pueden también ser usadas por personas que no pertenecen a SI para actualizar y recuperar datos directamente de los archivos de la computadora.

En general, la facilidad de programación en línea (on line) permite un desarrollo más rápido de programas y mejora las capacidades del programador para resolver problemas. Sin embargo, los sistemas en línea (on line) también crean oportunidades para errores resultantes de accesos no autorizados. Se debe usar software de control de accesos para ayudar a reducir el riesgo.

Una tendencia reciente es proveer utilerías de programación en línea (on line) usando estaciones de trabajo. La biblioteca (librerías) de programas esta en un servidor, como por ejemplo un sistema de administración de bibliotecas en un mainframe, pero la modificación (desarrollo) y prueba se realizan en la estación de trabajo. Este método puede bajar los costos de desarrollo, mantener un tiempo de respuesta rápida y expandir las ayudas disponibles de programación. Desde la perspectiva del control, este método introduce las debilidades potenciales de:

1) Proliferación de múltiples versiones de programas,
2) Reduce la integridad de los programas y de procesamientos a través del incremento potenciadle accesos y actualizaciones no autorizadas y
3) La posibilidad de que los cambios validos podrían ser sobrescritos por otros cambios.

Leguajes de Programación

Los programas de aplicaciones deben primero ser codificados en declaraciones / sentencias (statement), instrucciones o en lenguajes de programación que sea fácil de escribir para un programador y que pueda ser leído por la computadora. Estas sentencias serán luego convertidas por traductor / compilador del leguaje en bits de código maquina o en el lenguaje maquina que la computadora pueda ejecutar.

Los lenguajes de programación usados comúnmente para desarrollar los programas de aplicación son:

- Lenguajes de Alto Nivel, como por ejemplo COBOL, PL/1 y FORTRAN.
- Los lenguajes orientados a objetos para fines de negocio, como por ejemplo C++, 00-BASIC, Eifell, JAVA.
- Los Lenguajes de Ensamblador de bajo nivel diseñados para una computadora especifica.
- Los Lenguajes de Programación de Cuarta Generación (4GLs) que están constituidos por un DBSM, un administrador integro de base de datos y una utilidad no procedimental de informes de generaciones de pantallas. 4GLs provee una iteración rápida a través de diseños sucesivos. Ejemplos de 4GLs incluyen FOCUS, Natural y dBase.
- Lenguajes de Soporte para toma de decisiones y sistemas expertos (express, LISP y PROLOG).

Depuración de Programas (Debugging)

Muchos errores de programación son detectados durante el proceso de desarrollo del sistema, después que un programador ejecuta un programa entorno de pruebas. El propósito de utilizar programas de depuración (debugging) durante el desarrollo del sistema es asegurar que todas las terminaciones anormales del sistema y todos los errores de codificación del programa son detectados y corregidos antes de que el programa final pase a producción.

Una herramienta de depuración (debugging) es un programa que asistirá al programador para afinar, reparar o depurar el programa de desarrollo. Los compiladotes tienen algún potencial para proveer retroalimentación e información a un programador pero no se consideran herramientas de depuración (debugging). Estas herramientas se clasifican en tres categorías principales.

- Monitoreo de la ruta lógica que reporta sobre la secuencia de eventos realizados por el programa, brindando así al programador las pistas de errores lógicos.
- Volcado / vaciado de memoria que proveen una fotografía del contenido de la memoria interna, en un momento determinado. Esto a menudo se produce cuando el programa aborta, lo que da al programador una pista de inconsistencias en los datos o en lo valores de parámetros. Una variante denominada "trace", hará lo mismo en diferentes etapas de la ejecución del programa mostrándola evaluación de cosas tales contadores y los registros.

- Los analizadores de productos resultantes ayudan a verificar si los resultados de la ejecución del programa son correctos. Esto se logra comparando los resultados esperados con los resultados reales.

Pruebas

Las pruebas son el proceso que provee evidencia de un programa, un subsistema o una aplicación realiza las funciones para las cuales ha sido diseñada. Las pruebas también determinan que las unidades que están siendo comprobadas operan sin problemas de funcionamiento ni efectos adversos sobre otros componentes del sistema.

La variedad de metodologías de desarrollo y requerimientos organizacionales provee una amplia gama de esquemas prueba. Cada conjunto de pruebas se realiza con un juego de diferentes datos y bajo la responsabilidad de distintas personas o funciones. El ASI puede desempeñar una función preventiva o detectiva en el proceso de pruebas.

Generadores de datos de prueba se pueden usar para generar de manera sistemática datos al azar que pueden ser usados para probar programas. Los generadores funcionan usando las características del campo, diseño (layout) y de valores de datos. Además de los generadores de datos de prueba existen ayudas interactivas de depuración (debugging) y analizadores lógicos de código disponibles para asistir en las actividades de prueba.

Para orientar el proceso de pruebas y para ayudar a asegurar que todas las facetas del sistema funcionen como se espera, es útil desarrollar y documentar un plan formal de pruebas. Dicho plan identifica las porciones especificas del sistema que va a ser aprobadoy documenta los resultados reales de las pruebas comparándolos con los resultados que se esperaban. El plan de pruebas y los resultados deben ser retenidos como parte de la documentación permanente del sistema.

Hay dos métodos recíprocos para probar el software:

- *De Abajo hacia Arriba (Botton up).-* Comienza a probar las unidades elementales, como por ejemplo los programas o los módulos y trabaja hacia arriba hasta completar las prueba de todo el sistema. Las ventajas son:
  - No se necesitan componentes sustitutos o conductores.
  - Los errores en los módulos críticos se encuentran pronto.
- *De Arriba hacia Abajo (Top down).* Sigue el camino opuesto, considerando primero la profundidad o la amplitud de la prueba. Las ventajas son:
  - Las pruebas de las funciones principales y del procesamiento se realiza antes.
  - Los errores de interfaz se pueden detectar antes.
  - Eleva la confianza en el sistema, ya que los programadores y los usuarios efectivamente ven un sistema de funcionamiento.

Se pueden realizar las pruebas siguientes, basadas sobre el tamaño y la complejidad del sistema modificado:

- *Pruebas Piloto.*- Es la prueba preliminar que se concentra en los aspectos específicos predeterminados de un sistema. No pretende sustituir otros métodos de prueba, sino más bien proveer una evaluación limitada del sistema.
- *Pruebas de Unidad.*- La prueba de un programa o módulo individual. Usa un conjunto de casos de prueba que se concentran en la estructura de control de diseño procedimental (procedural design).

Estas pruebas aseguran que la operación interna del programa funcione en conformidad con la especificación.

- *Pruebas de Interfaz.*- Una prueba de hardware o de software que evalúa la conexión de dos o más componentes que pasan información desde un área a otra.
- *Pruebas de Sistema.*- Una serie de pruebas diseñadas para asegurar que el programa modificado interactúa correctamente con otros componentes del sistema . estos procedimientos de prueba son normalmente realizados por el personal de mantenimiento del sistema en su librería de desarrollo. Durante la prueba del sistema se pueden realizar las pruebas siguientes:
  - *Pruebas de Recuperación* – Verificar la capacidad del sistema de recuperarse después de una falla de software o de hardware.

- ***Pruebas de Seguridad*** – Asegurarse de que el sistema modificado / nuevo incluya controles de acceso apropiados y no introduzca ningún agujero de seguridad que pudiera comprometer otros sistemas.
- ***Pruebas de Estrés / Volumen*** – Probar una aplicación con grandes cantidades de datos para evaluar su rendimiento durante las horas pico.
- ***Pruebas de Rendimiento*** – Comparar el rendimiento del sistema con otros sistemas equivalentes, usando benchmarks bien definidas.

⇨ *Pruebas de Función / Viabilidad.*- similar a las pruebas del sistema, pero a menudo usadas para probar la funcionalidad del sistema contra los requerimientos detallados.

⇨ *Pruebas de Regresión.*- El proceso de volver a ejecutar una porción de un escenario de pruebas o plan de pruebas para asegurar que los cambios o las correcciones no hayan introducido nuevos errores. Los datos usados para probar la regresión deben ser los mismos que se usaron en la prueba original.

⇨ *Pruebas Paralelas.*- El proceso de introducir datos de prueba en dos sistemas: el sistema modificado y el sistema alternativo (posiblemente el sistema original) y comparar los resultados.

⇨ *Pruebas de Aceptación.*- Después de que el personadle sistemas esté satisfecho con sus pruebas iniciales y/o de sistemas, el sistema modificado debe ser probado por el usuario final. Una prueba realizada por el usuario final se denomina una prueba de aceptación de usuario. Las pruebas de aceptación de usuario respaldan el proceso que asegura que el sistema está listo para ser

implementado y que satisface todos los requerimientos documentados. Los métodos incluyen:

- Definición de las estrategias y los procedimientos de las pruebas.
- Diseño de casos y de escenarios de pruebas.
- Ejecución de las pruebas.
- Utilización de los resultados para verificar si el sistema está listo.

Los criterios de aceptación son criterios definidos que deben ser cumplidos por un producto para satisfacer las necesidades previamente establecidas por el usuario. Un plan de pruebas de aceptación de usuario debe ser documentado para la prueba final del sistema completo. Las pruebas son elaboradas a partir de la perspectiva del usuario y deben probar el sistema como si este se encontrara en producción. Idealmente estas pruebas deben realizarse en una librería segura de un ambiente de pruebas. Un entorno seguro de pruebas donde tanto el código fuente como el ejecutable estén protegidos ayuda a garantizar que no se hagan cambios no autorizados o de último minuto al sistema, sin pasar por el proceso estándar de mantenimiento del sistema. La naturaleza y la extensión de las pruebas dependerán de la magnitud y de la complejidad del cambio al sistema.

Aunque los paquetes de software sean probados por el vendedor antes de su distribución, estos sistemas, así como cualquier cambio posterior deben ser probados exhaustivamente por el usuario final y por el personal de mantenimiento del sistema. Estas pruebas complementarias ayudarán a garantizar que los programas funcionan

como los diseño el vendedor y que los cambios no interactúan de manera adversa con los sistemas existentes.

Muchas organizaciones utilizan la prueba integra (Integrated Test Facility - ITF). Habitualmente, los datos de prueba son procesados en sistemas similares a los sistemas de producción. Esto confirma el comportamiento de la nueva aplicación o de los nuevos módulos en condiciones reales. Estas condiciones incluyen el volumen pico (máximo) y otras restricciones relacionadas con los recursos. En este entorno, SI realizará sus pruebas con un conjunto de datos ficticios mientras que los representantes del cliente estarán usando los datos copiados de producción para cubrir el mayor número posible de combinaciones junto con algunos datos inventados para las situaciones no previstas.

Implementación

Una vez que el sistema ha pasado las pruebas de manera satisfactoria, el sistema esta listo para migrar al ambiente de producción los programas han sido totalmente probados y depurados, los procedimientos programados y la agenda de producción están listos todos los datos requeridos ya han sido satisfactoriamente convertidos y cargados en el nuevo sistema y los usuarios han desarrollado procedimientos y han sido totalmente entrenados en el uso del nuevo sistema. Se determina una fecha o fechas para la migración del sistema y se lleva a cabo la migración a la Producción. La fecha para la migración no debe afectar el procedimiento normal del negocio; por lo tanto, un fin de semana que evite un periodo de cierre o un ciclo pico del negocio, será el más apropiado.

Revisión Posterior a la Implementación

Una vez que se ha implementado el nuevo sistema o que se ha modificado ampliamente el actual, es conveniente verificar que el sistema haya sido debidamente diseñado, desarrollado y que se hayan integrado en el sistema los controles adecuados. Como tal, una revisión posterior a la implementación debe cumplir los objetivos siguientes:

- Evaluar qué tan adecuado es el sistema.
  - ¿Satisface el sistema los requerimientos del usuario y los objetivos de la Gerencia?
  - ¿Los controles de acceso han sido definidos e implementados de manera adecuada?
  - Evaluar el costo-beneficio o el Retorno de la Inversión.
  - Elaborar recomendaciones que traten los aspectos inadecuados y las deficiencias del sistema.
  - Desarrollar un plan para implementar las recomendaciones.

El equipo de desarrollo de proyectos debe efectuar la revisión posterior a la implementación conjuntamente con los usuarios finales apropiados. Típicamente, el enfoque de este tipo de revisión interna es hacer una evaluación y una crítica del proceso del proyecto.

De manera alternativa, un grupo independiente no asociado con la implementación del proyecto (Auditoria Interna o Externa) puede llevar a cabo una revisión posterior a la implementación. Los ASI que realicen esta revisión deben ser independientes del proceso

de desarrollo del sistema. Por lo tanto, los ASI involucrados como consultores en el equipo del proyecto para el desarrollo del sistema no deben estar efectuando dicha revisión. A diferencia de las revisiones internas del equipo del proyecto, las revisiones posteriores a la implementación realizadas por los ASI tienen una tendencia a concentrarse en los aspectos de control de los procesos de desarrollo e implementación del sistema.

Cuando se ha concluido la revisión, el ASI debe emitir una opinión para la Gerencia respecto a si el sistema debe ser puesto en producción. Este informe debe especificar las deficiencias del sistema que necesiten ser corregidas y debe explicar el o los riesgos que corre la organización al implementar el nuevo sistema. Es importante que toda la participación de la Auditoria en el proyecto de desarrollo sea documentada de manera minuciosa en los papeles de trabajo de Auditoria para respaldar todos los hallazgos y todas las recomendaciones del ASI. Este informe y documentación de Auditoria debe ser reutilizado durante el mantenimiento y los cambios para validar, verificar y probar el impacto de cualquier cambio que se haga al sistema. El sistema debe ser sometido a una revisión periódica para asegurar que aun existe control de integridad.

4.3.- Metodologías Alternativas de Desarrollo

Desarrollo de Sistemas Orientados a Datos (DOSD)

El Desarrollo de Sistemas Orientados a Datos (Data –Orient System Development - DOSD) se centra en y reconoce la necesidad que la Gerencia y le personal tenga acceso

a los datos para simplificar y respaldar las decisiones. Los usuarios necesitan y requieren los datos para producir información a partir de éstos. El desarrollo de una base de datos de información accesible que proveerá la base para los informes *ad hoc* es inherente a los sistemas DOSD.

El énfasis sobre los datos debe ser interpretado como la desaparición de los sistemas de procesamientos de transacciones al nivel operativo, sino que es un reconocimiento de que las mayoría de los sistemas de transacción ya han sido desarrollados y que los nuevos sistemas se están ahora encauzando a la necesidad que tienen los usuarios de más información.

Desarrollo de Sistemas Orientados a Objetos (OOSD)

El Desarrollo de Sistemas Orientados a Objetos (Objet-Oriented System Development - OOSD) es el proceso de especificación y modelación de soluciones. Este proceso define como implementar la funcionalidad definida por medio del análisis. El OOSD está habitualmente dividido en dos niveles: el primer nivel, el diseño abstracto, agrega características de solución a los modelos de análisis pero es todavía independiente en gran medida de las herramientas de desarrollo especificas; el segundo nivel, el diseño físico, es un nivel más detallado que considera las especificaciones del entorno de desarrollo y que incorpora esas características o limitaciones en el diseño. Las principales ventajas de un OOSD son las siguientes:

- La capacidad de administrar una variedad de tipos de datos.
- Provee un medio para modelar relaciones complejas.

- La capacidad para satisfacer las demandas de un entorno cambiante.

Tecnología Orientada a Objetos

La tecnología orientada a objetos considera los datos sin procesar (datos en Bruto) y los procedimientos que rigen el uso de los datos como un solo objeto. Un método orientado para la administración de datos define objetos en términos de sus características (por ejemplo, pruebas, gráficos, especificaciones de formato e información para la impresora) y los procedimientos que rigen su uso (como se usan esas características para hacer un documento completo). El objeto es entonces almacenado como un recurso que puede ser reusado o modificado. Las aplicaciones que usan tecnología orientada a objetos son:

- Ingeniería de Software Asistida por Computadora / ordenador (CASE) para el desarrollo de software.
- Automatización de la oficina para el correo electrónico y las ordenes de trabajo.
- La Inteligencia Artificial (IA)
- Fabricación Asistida por Computadora / ordenador (CAM) para producción y control de procesos.

Las principales ventajas de un método orientado a objetos para los sistemas de administración son:

- La capacidad para administrar una variedad limitada de tipos de datos
- Provee un medio para modelar relaciones complejas
- Capacidad para satisfacer las demandas de un entorno cambiante

- Los modelos orientados a objetos pueden ser manipulados con facilidad por los usuarios
- Incrementa la eficiencia en programación a través de la habilidad para reusar elemento de software
- Capacidad para permitir que el usuario o que una aplicación tenga acceso solamente a la información que necesite, ya que almacenan objetos independientemente uno del otro

Prototipos

La creación de prototipos, conocida también como desarrollo heurístico, es el proceso de crear un sistema por medio del método controlado en ensayo y error. Es un método, que usa principalmente herramientas de desarrollo rápido como por ejemplo, 4GLs, que permite que el usuario tenga una visión de alto nivel del funcionamiento del sistema propuesto dentro de un periodo corto de tiempo.

El énfasis inicial durante el desarrollo del prototipo se centra por lo general en los informes y en las pantallas, que son los aspectos del sistema más empleados por los usuarios finales. Esto permite al usuario final ver en funcionamiento un modelo del sistema propuesto dentro de un periodo corto de tiempo.

Hay dos métodos básicos de crear un prototipo:

- Construir el modelo para crear el diseño. Luego, sobre la base de ese modelo, desarrollar el sistema con todas las capacidades de procesamiento que se necesitan.
- Construir gradualmente el sistema real que opera en producción usando un 4GL que se haya determinado que es el apropiado para el sistema que se esta construyendo.

El problema que tiene el primer método es que puede haber presión considerable para implementar anticipadamente un prototipo. A menudo, los usuarios que observan un modelo funcionando no pueden entender por qué el primer prototipo tiene que ser depurado aun más. El hecho de que el prototipo tenga que ampliarse para que maneje volúmenes de transacciones, redes de terminales, procedimiento de copias de seguridad y recuperación, así como también proveer la capacidad de que sea auditado y controlado no siempre es comprendido.

Otra ventaja de crear un prototipo es que éste conduce a menudo a que se agreguen al sistema funciones o extras que no estaban incluidas en el documento inicial de requerimientos. Todas las adiciones mayores que trasciendan los requerimientos contenidos en el documento inicial de requerimientos deben ser revisados para asegurar que satisfagan las necesidades estratégicas de la organización y que sus costos sean eficientes. De otro modo, el sistema final puede terminar siendo ventajoso desde el punto de vista funcional pero ineficiente.

Un riesgo potencial con los sistemas creados por prototipo es que el sistema terminado tendrá controles deficientes. Centrándose principalmente en lo que quiere y ve el usuario, los que desarrollan el sistema pueden omitir algunos de los controles que se obtienen mediante le método tradicional de desarrollo de sistemas, como por ejemplo; copias de seguridad / recuperación , seguridad y pistas de Auditoria.

A menudo, el control de los cambios se vuelve mucho más complicado con los sistemas creados por medio de prototipos. Los cambios en los diseños y requerimientos ocurren con tanta rapidez que ellos son documentados o aprobados muy pocas veces y pueden llegar hasta el punto de no poder ser mantenidos.

A pesar de que el ASI debe ser consiente de los riesgos asociados con los prototipos, también debe ser claro que este método de desarrollo de sistemas puede proveer a la organización ahorros significativos de tiempo y costo.

Desarrollo Rápido de Aplicaciones (RAD)

El RAD es una metodología que permite a las organizaciones desarrollar rápidamente sistemas estratégicamente importantes al tiempo que reducen los costos de desarrollo y mantienen la calidad. Esto se logra usando una serie de técnicas probadas de desarrollo de aplicaciones, dentro de una metodología bien definida. Estas técnicas incluyen el uso de:

- Equipos de desarrollo pequeños y bien estructurados
- Prototipos evolutivos

- Herramientas poderosas integradas que soportan el modelamiento, los prototipos y la reutilización de componentes
- Un repositorio central
- Requerimientos y talleres de diseño interactivos
- Limites rígidos para los periodos de tiempos de desarrollo

RAD soporta el análisis, diseño, desarrollo e implementación de sistemas individuales de aplicación. Sin embargo, RAD no soporta la planificación o el análisis requerido para definir las necesidades de información de la empresa como un todo o un área importante del negocio de la empresa. RAD provee un medio para desarrollar sistemas más rápidamente al tiempo que reduce el costo y aumenta la calidad. Esto se hace automatizando grandes porciones del ciclo de vida del desarrollo de sistemas, imponiendo límites rígidos a los periodos de tiempo de desarrollo y reutilizando los componentes existentes. La metodología del RAD tiene cuatro etapas principales:

- La etapa de definición de conceptos establece las funciones del negocio y las áreas de relacionadas con los datos que el sistema soportará y determina el alcance del sistema.
- La etapa del diseño funcional utiliza talleres para diseñar los procesos y los datos del sistema y para construir un prototipo de funcionamiento de componentes críticos del sistema.

- La etapa de desarrollo completa la construcción física de la base de datos y del sistema de aplicación, construye el sistema de conversión y desarrolla ayudas para el usuario y los planes de asignación de trabajos.
- La etapa de despliegue incluye probar y entrenar al usuario final, la conversión de los datos y la implementación del sistema de aplicación.

Reingeniería

La reingeniería es un proceso de actualización de un sistema existente extrayendo y reutilizando los componentes de diseño de programa. Este proceso se usa para soportar los cambios importantes en la forma en que opera una organización, actualmente existe un buen número de herramientas para apoyar un proceso.

Ingeniería Inversa o de Reversa

La ingeniería de reversa es el proceso de descomponer un aplicación o una aplicación de software o un producto, para ver como funciona y para usar esa información para desarrollar un sistema similar. Este proceso puede llevarse a cabo en varias formas:

- Descompilando el código objeto o el ejecutable en código fuente y usándolo para analizar el programa
- Utilizando la aplicación a someter a la ingeniería inversa como una caja negra y desvelando su funcionalidad usando datos de prueba

Las ventajas principales de la ingeniería de reversa son:

- Un desarrollo más rápido y una menor duración del ciclo de vida de desarrollo de sistemas (System Development Life Cycle – SDLC)
- La creación de un sistema mejorado usando los inconvenientes o desventajas de la aplicación sometida a una ingeniería inversa.

El ASI debe estar consciente de los siguientes riesgos:

- Los contratos de licencia de software con frecuencia contienen cláusulas que prohíben, a quien adquiere la licencia, someter el software a ingeniería de reversa, para que no se expongan los secretos comerciales o las técnicas de programación.
- Los descompiladores son herramientas relativamente nuevas cuya función depende de computadoras, sistemas operativos y lenguajes de programación específicos. Cualquier cambio en uno de estos componentes requerirá desarrollar o comprar un nuevo descompilador.

Análisis Estructurado (SA)

El SA es un escenario para los componentes físicos (datos y proceso) de una aplicación de uso que usa diagramas de flujo de datos. Incluye un modelo físico del sistema, datos depurados y asignación de procesos con una interfaz de usuario revisada. Usando SA se puede implementar un proceso de revisión en el que un miembro del equipo de proyectos dirige a uno o más miembros del equipo o a clientes a través de un segmento de un producto que él o ella han producido. Los miembros del equipo hacen preguntas y

comentarios sobre la técnica, el estilo, los errores posibles, la violaciones de normas y otros problemas, en un proceso de SA el desarrollador querría hacer lo siguiente:

- Desarrollar diagramas del contexto del sistema.
- Efectuar una descomposición del flujo jerárquico y del control de los datos.
- Desarrollar la transformación de los controles.
- Desarrollar mini-especificaciones.
- Desarrollar diccionarios de datos.
- Definir todos los casos externos – entradas provenientes del entorno externo.
- Definir los diagramas únicos de transformación del flujo de datos provenientes de cada caso externo.

El siguiente cuadro describe los puntos fuertes y los débiles del Análisis Estructurado SA.

Puntos Fuertes	Puntos Débiles
➢ Comprende rápidamente las inquietudes del usuario. ➢ Soporta herramientas CASE ➢ Es más aplicable al análisis orientado al programa que se diseño.	➢ Representación débil de la solución: la representación estructurada del gráfico es inadecuada para capturar los elementos de la tarea concurrentes y sus interacciones. ➢ No trata el tema de estructurar el sistema en tareas concurrentes.

4.4.- Prácticas de Mantenimiento de los Sistemas de Información

Una vez que se traslada un sistema a producción, éste pocas veces permanece estático. El cambio es un acontecimiento esperado en todos los sistemas independientemente de si los mismos son suministrados por un vendedor o desarrollados internamente. Para

controlar el mantenimiento en curso del sistema, es necesaria una metodología estándar para efectuar y para registrar los cambios. Esta metodología debe incluir pasos para asegurar que los cambios al sistema sean apropiados para las necesidades de la organización, estén debidamente autorizados, documentados, probados exhaustivamente y sean aprobados por la Gerencia.

Los controles de mantenimiento del sistema se refieren al proceso de modificar los programas de aplicación, sobre la base de las necesidades organizativas, al tiempo que mantienen la integridad tanto del código fuente como el del ejecutable en producción.

Administración / Gestión de Cambios

Un nivel apropiado de la Gerencia debe autorizar los cambios para los programas en producción. A pesar de que el equipo de desarrollo / mantenimiento del sistema puede, en algunos casos, iniciar el proceso de cambios para resolver un problema de procesamiento o para ampliar el rendimiento operativo del sistema, aún así se debe obtener la autorización de los niveles apropiados de la gerencia. Para los sistemas adquiridos, el vendedor puede distribuir las actualizaciones periódicamente o las nuevas versiones del software, la Gerencia de usuarios y de sistemas debe revisar dichos cambios. Se debe tomar la determinación de si los cambios son apropiadas para la organización y si los mismos afectarán o no negativamente el sistema existente.

Los usuarios deben trasmitir a la Gerencia de Sistemas las solicitudes de cambio al sistema, usando algún tipo de correspondencia formal como por ejemplo un formulario

estándar de solicitud de cambio, un memorando o un mensaje de correo electrónico. La solicitud del usuario debe incluir, como mínimo, el nombre del solicitante, la fecha de solicitud, la fecha en que se necesita el cambio, la prioridad de la solicitud, una minuciosa descripción del cambio que se solicita y una descripción de cualquier efecto o efectos anticipados sobre los otros sistemas o programas. El usuario podría también dar una razón para el cambio, un análisis de justificación del costo y de los benéficos que se esperan del cambio. Además, la solicitud debe brindar evidencia de que ha sido revisada y autorizada por la Gerencia de usuarios. Dicha evidencia la provee por lo general una firma en el formulario o memorando de solicitud.

Las solicitudes de cambio deben hacerse en un formato que asegure que todos los cambios sean considerados para llevar a cabo una acción y que permita que el personal de la Gerencia de Sistemas rastree con facilidad la situación de la solicitud. Esto se hace habitualmente asignando un número único de control a cada solicitud y entrando la información de la solicitud de cambio a un sistema computarizado. Esto también se puede hacer manualmente. Con información detallada en relación en cada solicitud , la Gerencia puede identificar las solicitudes que han procesado y las que todavía están en proceso o que aún no han sido tratadas. La Gerencia puede también usar esta información para ayudar a asegurar que las solicitudes de usuario sean atendidas a su debido tiempo.

Todas las solicitudes de cambios y la información relacionada deben ser mantenidas por el equipo de mantenimiento del sistema como parte de la documentación permanente del sistema.

Deben existir registros de mantenimiento de todos los cambios a programas ya sean manuales o automáticos. Varios productos de software de administración de librerías proveen este tipo de pista de Auditoria. La información de mantenimiento está por lo general constituida por la ID del programador, la hora y la fecha del cambio, el número de proyecto de solicitud de asociado con el cambio, y las imágenes antes y después de las líneas de código que fueron cambiadas.

Este proceso se vuelve cada vez más importante cuando el programador que crea el programa es también el operador del mismo. En este caso se asume que el departamento de SI es o bien muy pequeño o el número de aplicaciones que se están procesando es muy pequeño. Los procedimientos de administración de cambios se deben seguir muy estrictamente ya que la segregación de las funciones no pueden establecerse en este entorno. Requerirá que la gerencia de usuarios preste más atención a los cambios y actualizaciones que haga el programador; se debe dar la debida autorización al programador antes de poner cualquier cambio en el entorno de producción. Además del proceso manual de la Gerencia aprobando los cambios antes que el programador pueda ponerlos en producción, la Gerencia podría hacer instalar un software automático de control de cambios para impedir cambios no autorizados a programas. Haciendo esto, el programador ya no es responsable de la migración de los cambios a producción. El software del control de cambios se convierte en el operador que migra los cambios del programador a producción sobre la base la aprobación de la Gerencia.

Los programadores no deben tener acceso a escribir, modificar o eliminar datos de producción. Dependiendo del tipo de información que este en producción, los programadores no pueden ni siquiera tener acceso de lectura (read – only) (acceso a los números de tarjetas de crédito del cliente, números de seguridad social u otra información sensitiva que pueda requerir seguridad adicional).

Cambios de Emergencia

Puede que algunas veces se requiera llevar a cabo cambios de emergencias para resolver problemas del sistema y para posibilitar la continuidad de un procedimiento critico. Deben existir procedimientos para asegurar que se puedan realizar los arreglos de emergencia sin comprometer la integridad del sistema. Esto implica por lo general el uso de login-IDs especiales que otorgan acceso temporal al entorno de producción durante estas situaciones de emergencia. Como los IDs de emergencia tienen privilegios poderosos, su uso debe ser registrado y monitoreado/supervisado con minuciosidad. Los arreglos de emergencia deben realizarse usando procedimientos de seguimiento después del hecho que aseguren que se aplicaron retroactivamente todos los controles normales.

Aprobación

Después que el usuario final esté satisfecho con los resultados de la prueba del sistema y con las adecuaciones del sistema, se deberá obtener la aprobación de la Gerencia de usuarios. La aprobación de usuario podría ser documentada en la solicitud original del cambio o en alguna otra forma (memorandum o correo electrónico). Sin embargo, la

evidencia que verifique que la aprobación de usuarios ha sido otorgada debe ser mantenida por el personal de mantenimiento del sistema.

Documentación

Para asegurar la utilización efectiva y el mantenimiento futuro de un sistema, es importante que toda la documentación relevante del sistema este actualizada. Debido a las limitaciones del tiempo y de los recursos, a menudo de descuidan las actualizaciones minuciosas de la documentación. La documentación que requiere revisión puede estar constituida por diagramas de flujo del programa y/o del sistema, narrativa de programas, diccionarios de datos, modelos de entidad – relación, Diagramas de Flujos de Datos (DFDs), manuales de ejecuciones o corridas del operador y manuales de procedimiento del usuario final.

Deben estar establecidos procedimientos para asegurara que la documentación almacenada fuera de lugar para fines de recuperación de desastres también este actualizada. Esta documentación es a menudo pasada por alto y si se requiere durante una situación de desastre es posible que no esté actualizada.

Pruebas de los cambios a programas

Para evaluar si los cambios a los programas son los adecuados, el ASI debe asegurarse de que estén establecidos controles para proteger los programas de aplicaciones en producción, de cambios no autorizados. Los objetivos del control son:

- Se debe restringir el acceso a las librerías de programas
- Se deben llevar a cabo revisiones de supervisión
- Las solicitudes de cambio debe estar documentada en un formulario estándar, prestando especial atención a los siguiente:
  - Las especificaciones de cambio deben estar descritas de manera adecuada con un desarrollo de análisis de los costos y con una fecha establecida.
  - El formulario de cambio debe estar firmado por el usuario para indicar la aprobación
  - El formulario de cambio debe ser revisado y aprobado por la Gerencia de Programación
  - El trabajo debe ser asignado a un analista, un programador y un jefe de grupo de programación para su supervisión
- Escoger una muestra de los cambios a programas efectuados durante el periodo de Auditoria y rastrearlos hasta el formulario de mantenimiento para determinar si los cambios están autorizados, verificar que el formulario tenga las aprobaciones debidas y comparar la fecha del formulario con la fecha de actualización de producción para la aceptación.
- Si un grupo independiente actualiza los cambios a programas en producción, el ASI debe determinar si existen procedimientos para asegurar que se cuenta con el formulario de solicitud del cambio antes de la actualización. (Esta se realiza observando a los grupos realizar su trabajo).

Un cambio no autorizado puede ocurrir por varios motivos:

- El usuario responsable de la aplicación no tenia conocimiento del cambio (ningún usuario firmo la solicitud de cambio de mantenimiento aprobando el inicio del trabajo).
- Un formulario y procedimientos de solicitud de cambio, no fueron establecidos formalmente.
- El gerente de programación no firmó el formulario de cambio aprobando el inicio del trabajo.
- El usuario no firmó el formulario de cambio evidenciando su aceptación antes de que el cambio fuera actualizado.
- El código fuente cambiado no fue debidamente revisado por el personal apropiado de programación.
- El gerente de programación no firmó el formulario de cambio aprobando la actualización del programa en producción.
- El programador introdujo un código adicional para beneficio personal (es decir, cometió fraude).

La revisión detallada del ASI puede localizar los puntos débiles en el procedimiento que permitirían que ocurrieran de manera inadvertida una de las anteriores situaciones. Si el ASI encontrara que los procedimientos apropiados están establecidos, se deben diseñar pruebas de cumplimiento para encontrar evidencias de que los controles identificados funcionaron debidamente durante el periodo de la revisión. La revisión detallada debe

también determinar si los procedimientos de control podrían ser burlados intencionalmente, permitiendo que un cambio no autorizado pase sin ser detectado.

Proceso de Migración de Programas

Una vez que la Gerencia de usuarios haya aprobado el cambio, los programas modificados pueden ser trasladados al entorno de producción. Un grupo que sea independiente de la programación de computadora debe efectuar la migración de programas desde el entorno de pruebas de producción. Los grupos como por ejemplo los operadores de computadora, aseguramiento de calidad o un grupo designado de control de cambio, deben efectuar esta función.

Para asegurar que los únicos individuos autorizados tengan la posibilidad de migrar los programas de producción, se deben establecer restricciones apropiadas de acceso. Dichas restricciones pueden ser implementadas por medio del uso de seguridad del sistema operativo o de un paquete externo de seguridad.

Software de Control de Bibliotecas / Librerías

El software de control de bibliotecas / librerías se debe usar para separar las librerías de pruebas de la bibliotecas / librerías de producción, tanto en un entorno mainframe como en uno de cliente / servidor. El objetivo principal del software de bibliotecas / librerías es asegurar que los cambios a programas hayan sido autorizados. El control mínimo necesario es la autorización de los cambios a la librerías de producción, que requiere un procedimiento de autorización entre las librerías de pruebas y las de producción. Se

deben aplicar controles de autorización, tanto a las librerías de pruebas, como a las de producción. El riesgo de no tener controles sobre ambas librerías es que una versión en prueba puede contener código no autorizado o fraudulento que podría ser usado en el cambio siguiente a producción. Después de ser vinculado a un objeto de producción, el código fraudulento sería colocado en producción.

El propósito primario del software de control de bibliotecas / librerías es:

- Prohibir a los programadores acceder a las librerías de fuentes y de objetos de producción
- Prohibir la actualización de los programas en lote (batch)
- Exigir que le grupo de control o el operador liberen el código fuente y lo coloquen en la biblioteca / librería del programador
- Exigir que el programador devuelva el código fuente modificado al grupo de control o al operador que actualiza la biblioteca / librería de objetos o las pruebas del programador
- Exigir que el grupo de control o el operador actualice la biblioteca / librería de objetos con la versión de producción después que se haya realizado la prueba
- Permitir el acceso solamente a la lectura (read – only) al código fuente
- Exigir que las convenciones de nombre de programas tengan un identificador único para distinguir las versiones de prueba de las de producción.

- Implementar controles de Filtrado del Lenguaje de Control (JCL) para prevenir la ejecución en producción de un programa en pruebas ocasionado por el uso de un nombre equivocado de programa.

Integridad del Código Ejecutable y del Fuente

Cada módulo ejecutable de producción deben tener un módulo fuente correspondiente. Cada vez que un programa sea trasladado a la biblioteca / librería de código fuente en producción, una versión ejecutable y compilada de ese programa debe ser traslada a la biblioteca / librería en producción. Usualmente este es un procedimiento manual realizado por el grupo o por la persona responsable de la migración de programas. Un procedimiento óptimo sería que se cree automáticamente un modulo de código ejecutable cada vez que se traslade un módulo fuente a producción. Este procedimiento es a veces una función de los productos de software de administración de bibliotecas / librerías que están disponibles para muchas plataformas computacionales.

Asegurar la integridad del ejecutable y del fuente es vital parta el debido control de los sistemas en producción porque provee garantía de que no está ejecutando una versión indebida de un programa. La fecha de actualización (timestamp) del módulo fuente no debe ser posterior al del módulo ejecutable correspondiente. En ningún momento debe el usuario o el programador de aplicaciones tener acceso al código fuente en producciones o a las bibliotecas / librerías de carga en el entorno de mainframe. Esto se usa para minimizar el riesgo de la segregación indebida de funciones en el proceso de control de cambios. Sin embargo, es un desarrollo de aplicación controlado por el usuario, los usuarios desarrollan sus propias aplicaciones independientemente del departamento de

SI. En algunos casos, los usuarios trabajan con PC monousuario (stand-alone), en otros, utiliza terminales conectadas a mainframes dedicados o compartidos o a entornos cliente / servidor. Los ASI deben revisar con especial cuidado las aplicaciones desarrolladas por los usuarios finales autónomos, en especial cuando las aplicaciones pueden ser usadas para entrar a los archivos centrales de datos o para manipularlos. Sin la orientación de desarrolladores profesionales los usuarios pueden potencialmente desarrollar programas con errores, generar informes de engañosos para la Gerencia o incluso introducir errores en los archivos de datos.

Comparación del Código Fuente

El software de comparación del código fuente es un método efectivo y fácil de usar para rastrear los cambios hechos a los programas. El ASI debe primero obtener y almacenar (en cinta o en disco) una copia de control del código fuente del programa que va a ser aprobado. En alguna fecha futura (en una semana o en un mes), el ASI ejecuta el programa de comparación de fuentes para rastrear las diferencias entre la fuente de control y la fuente actual. El Auditor imprime la lista de adiciones, eliminaciones y cambios y la usa para revisar la documentación de aprobación de la autorización de los cambios así como las solicitudes de trabajo, aprobaciones y pruebas de programas.

Los programas de comparación de fuente permiten al ASI examinar los cambios y los controles de los programas fuente sin la ayuda del personal de SI que posiblemente sea engañosa. Esta técnica, sin embargo, no detecta un programa fuente que haya sido cambiado y restituido a su forma original durante el tiempo entre la obtención de la copia

de control y la ejecución de la comparación. Los métodos para detectar los cambios a los módulos de carga deben usarse con el software de comparación de código fuente.

Una revisión manual de los cambios en el código fuente es considerado valido pero no totalmente efectiva. El ASI obtiene un listado del módulo fuente que esta siendo auditado y escanea el programa para localizar sentencias (statements) de pistas de Auditoria.

4.5.- Herramientas y Técnicas para la Administración de Proyectos

Hay numerosos técnicas y herramientas para la administración de proyectos disponibles para asistir al gerente de proyectos en el control de tiempos y de recursos utilizados en el desarrollo de un sistema. Estas técnicas pueden variar desde un sencillo esfuerzo manual hasta un proceso más elaborado. El tamaño y la complejidad del proyecto pueden requerir diferentes enfoques.

Estas herramientas por lo general proveen asistencia en las áreas siguientes:

Planeación de Programas, Programación (scheduling) y Medición del Rendimiento
Hay técnicas automatizadas para desarrollar descripciones de tareas y estimaciones de costos y para monitorear y controlar, predecir e informar sobre el rendimiento. Estos paquetes utilizan a menudo las técnicas tradicionales de PERT y CPM.

Estimación del Costo del Software

Hay técnicas automatizadas para estimar el costo de los proyectos en cada etapa de desarrollo del sistema. Para usar estos productos, un sistema se divide usualmente en componentes principales y se establece un conjunto de parámetros de costos (cost drivers).

- Lenguaje de código fuente
- Limitaciones de tiempo de ejecución
- Limitaciones de almacenamiento principal
- Limitaciones de almacenamiento de datos
- Acceso a las computadoras
- Máquina destinada para ser utilizada para el desarrollo
- Entorno de seguridad
- Experiencia personal
- Una vez que todos los parámetros (drivers) del costo estén definidos, el programa desarrollará estimaciones del costo del sistema y del proyecto total.

Administración / Gestión de la Configuración del Software

Estas son herramientas automatizadas para identificar y documentar la configuración de los sistemas de información y para monitorear y controlar los procedimientos de control de cambios. Esto se logra de la siguiente manera:

- Estableciendo configuraciones iniciales aprobadas para los programas y documentación soporte

- Manteniendo el control de cambios de configuración para todos los programas bajo el control inicial.
- Asegurando que todas las modificaciones y los problemas reportados para los programas bajo el control inicial tengan una pista apropiada de Auditoria

Documentación

Estas son herramientas para gestionar la producción, la validación y el mantenimiento de la documentación del sistema y del programa. Estas herramientas permiten a menudo que el usuario introduzca parámetros de programa y de sistema sin tener que conocer funciones muy avanzadas de procesamiento de palabras. El paquete entonces genera narrativas de programas y diagramas de flujo a partir de los datos introducidos por el usuario.

Administración / Gestión de Proyectos

Estas son técnicas automáticas para mejorar propuestas, puntos de acción de proyectos, solicitudes de cambios, correo electrónico, etc. Muchos de estos productos son suministrados como Sistemas de Apoyo para la Toma de Decisiones (DSS) para planificar y controlar los recursos del proyecto. Ellos pueden realizar funciones que van desde requerimientos de personal hasta sistemas de presupuesto. Esto productos a menudo incorporan las técnicas PERT.

Automatización de Oficinas

Estas son herramientas para reducir la participación del programador en funciones generales como por ejemplo políticas de personal y reuniones del personal. Los tipos de herramientas automatizadas de oficinas que han demostrado ser útiles y productivas son los sistemas de correo electrónico, los sistemas de mensajes de voz, las herramientas automatizadas de administración de tiempo como por ejemplo los calendarios electrónicos y recordatorio de fechas, bibliotecas / librerías automatizadas y sistemas de archivo y recuperación.

Presupuestos y Cronogramas (scheduling)

Un proyecto de desarrollo de sistemas debe ser analizado con el fin de estimar el grado de esfuerzo que se requerirá para realizar cada tarea. Las tareas individuales pueden consumir tanto el esfuerzo humano como el tiempo de maquina. Las estimaciones para cada tarea deben contener algunos o todos los elementos siguientes:

- Horas hombre por tipo (analista de sistema, programador, oficinista)
- Horas maquina (principalmente tiempo de computadora, así como también recursos de duplicación, equipos de oficina, equipos de comunicación)

El análisis de Punto de Función es una medida del tamaño de un sistema de información basado en el número y complejidad de los datos que se ingresan, los resultados obtenidos y los archivos que ve el usuario y con los cuales éste interactúa.

Habiendo establecido la mejor estimación de los esfuerzos esperados por tarea (horas efectivas, mínimo / máximo) la elaboración de un presupuesto es ahora un proceso de dos etapas para:

1. Obtener una estimación del esfuerzo humano y de máquina, etapa por etapa, sumando el esfuerzo esperado por las tareas dentro de cada etapa.
2. Proyecte la suma de esfuerzos expresada en horas por la tasa de horas apropiada para obtener una estimación del gasto de desarrollo de los sistemas, etapa por etapa.

Mientras que la elaboración del presupuesto consiste en totalizar el esfuerzo humano y de maquina que involucra cada tarea, la preparación de los cronogramas consiste en establecer la relación secuencial entre las tareas. Esto es ordenar las tareas de acuerdo con:

- La fecha de inicio más temprana considerando la relación secuencial lógica entre las tareas tratando de ejecutar las tareas paralelamente siempre que sea posible.
- La fecha de terminación más tardía que se espera considerando la estimación de horas según el presupuesto y la disponibilidad esperada de personal o de otros recursos teniendo en cuenta consideraciones de tiempo que se sabe que ha transcurrido (vacaciones, tiempo de incorporación, empleados a tiempo completo / tiempo real)

El cronograma puede ser representado por gráficamente usando varias técnicas de elaboración de gráficos como por ejemplos los gráficos de GANTT o los diagramas de PERT. En los puntos / meta calves dentro del proyecto, el presupuesto y el cronograma deben ser revisados para verificar su cumplimiento y para identificar variaciones. Cualquier variación en el presupuesto y en el cronograma debe ser analizado para determinar la causa y para emprender una acción correctiva que minimice o que elimine la variación total del proyecto. Las variaciones y el análisis de variaciones deben ser reportados a la Gerencia oportunamente.

El negocio de crear sistema ha sufrido cambios dramáticos a través de los últimos años. En la actualidad las organizaciones de TI deben concentrarse en la evaluación de la tecnología y en la integración de cambios con practicas y comportamientos ya aprendidos.

Método de la Ruta Critica (CPM)

Todas las técnicas de administración / gestión de proyectos calculan lo que se llama una Ruta Critica (RC). Como un proyecto esta constituido por un conjunto ordenado de actividades independientes, se le puede representar como una red en la que las actividades se muestran como ramas conectadas en nodos que proceden y que se siguen inmediatamente a las actividades.

Una ruta a través de la red es cualquier conjunto de actividades sucesivas que va desde el principio al fin del proyecto. Asociado con cada actividad en la red hay un solo número que estima mejor el tiempo que consumirá esa actividad. Las diferencias en la forma de obtener este número distinguen las principales variantes de la técnica.

La RC, entonces, es una ruta cuyo tiempo total de actividad es mayor que el de cualquier otra ruta a través de la red. Esta ruta es importante porque, si todo se realiza en conformidad con el cronograma, su duración da el tiempo más corto posible de terminación del proyecto total.

Además, se puede asociar un tiempo de holgura (slack time) con cada actividad del proyecto. Esta es la diferencia entre el tiempo más tardío posible de conclusión de cada actividad, la cual no demorará la conclusión del proyecto total y el tiempo más temprano posible para la conclusión basado en todas las actividades del predecesor, las actividades en una ruta critica no tienen tiempo de holgura y a la inversa, las actividades que no tienen tiempo de holgura (slack time) están en una RC.

La RC y los tiempos de holgura (slack time) asociados para un proyecto se encuentran simplemente avanzando el trabajo a través de la red, calculando el tiempo mínimo posible para concluir cada actividad, hasta que se encuentre el tiempo de conclusión mínimo posible para la totalidad del proyecto. Luego retrocediendo en el proceso a través de la red, se encuentra el tiempo máximo de conclusión de cada actividad, el tiempo de holgura computado y la ruta critica identificada. Este procedimiento se programa habitualmente en una computadora para facilitar el cálculo y los diferentes escenarios posibles.

El cálculo de la RC se realiza asumiendo primero un tiempo nominal o teórico para cada actividad. Las actividades en la RC se convierten en candidatas para ser eliminadas, o,

para ser reducido su tiempo mediante el pago de una prima por conclusión anticipada. Relajando sucesivamente las actividades en la RC, se puede obtener una curva que refleje los costos de todo el proyecto frente al tiempo de realización del mismo.

Gráficos de GANTT

Los Gráficos de GANTT pueden construirse para asistir en la programación de las actividades (tareas) que se necesiten para realizar un proyecto. Los Gráficos muestran también que actividades cuando debe comenzar una actividad y cuando esta debe terminar. Los Gráficos muestran también que actividades pueden estar realizándose el mismo tiempo y cuales deben llevarse a cabo en seria. Los Gráficos de GANTT también ayudan a identificar lo que ocurrirá si una actividad es concluida anticipadamente o con retraso. El progreso de un proyecto puede reflejarse en los gráficos y de ese modo se puede ver si el proyecto está atrasado, adelantado o conforme con lo programado.

Técnica de Revisión y Evaluación de Programas (PERT)

PERT es una técnica de administración de red usada ampliamente en las industrias de la defensa y de la construcción y que ha sido adoptada por muchas organizaciones de Sistemas de Información. PERT asume que el proyecto es un conjunto de actividades o tareas. Las actividades pueden ser iniciadas y detenidas de manera independiente una de la otra (en contraste con un flujo secuencial de procesamiento) o tienen relaciones precedentes. Las relaciones precedentes excluyen el inicio de ciertas actividades hasta

que otras se realicen (por ejemplo, preparar la superficie de una carretera debe preceder a la colocación de la plancha)

Las técnicas se pueden usar tanto para la planificación como en el control de proyectos. La planificación en este contexto comprende el diseño (layout) general del proyecto, con un estimado general del tiempo y de los recursos que se requieren y con la programación detallada del tiempo y del orden de las actividades. Por consiguiente, trata sobre el conjunto de decisiones tomadas antes del inicio del proyecto. En contraste con esto, el control se realiza durante el proyecto. A medida que se obtiene información sobre el uso de los recursos y los tiempos de realización efectivos, se pueden usar técnicas de administración de proyectos para reasignar los recursos de conformidad con los niveles revisados de importancia de las actividades.

El PERT requiere que los componentes desarrollo de sistemas sean desglosados en una o más categorías. Cada proceso del ciclo de vida del desarrollo de sistemas es considerada como una actividad. Una actividad requiere recursos y tiempo para llevarla a cabo, cada actividad inicia y termina con un evento, el evento no tiene su propio tiempo asignado y no consume recursos. Un evento o resultado puede ser la realización del estudio de factibilidad / viabilidad operativa o el punto en el cual el usuario acepta el diseño detallado. Cuando se diseña un diagrama PERT, el primer paso es identificar todas las actividades del proyecto y su secuencia relativa, el analista debe tener cuidado de no pasar por alto ninguna actividad. La listad de actividades determina el detalle del

diagrama PERT. El analista puede preparar cualquier programa que provea estimaciones de tiempo cada vez más detalladas.

PERT supone un conocimiento imperfecto de los tiempos de las actividades individuales de desarrollo es por eso que incorpora un nivel de incertidumbre en la estimación de tales tiempos. Para esto, se obtiene una estimación de tres escenarios: el optimista, el pesimista y el más probable para cada actividad. Estos escenarios luego son utilizados para estimar la desviación estándar de cada actividad y un tiempo de holgura, y de esta manera se deduce si una actividad determinada es o no critica. Luego continuando con el supuesto de que las actividades son independientes, las estimaciones de la desviación estándar de la actividad individual se usan para estimar la desviación estándar del tiempo de realización de todo el proyecto.

4.6.- Herramientas para el Desarrollo del Sistema y Ayudas a la Productividad.

Generadores de Código

Los generadores de código son herramientas, a menudo incorporadas con los productos CASE, que generan un código de programa basado en los parámetros definidos por una analista de sistemas o basados en los diagramas de flujo de datos /entidades desarrolladas por el módulo de diseño de un producto CASE, éstos productos permiten a la mayoría de los desarrolladores implementar, con eficiencia, programas de software.

Como se señaló, el ASI debe estar conciente de los orígenes no tradicionales del código fuente.

Ingeniería de Software Asistida por Computadora (CASE)

Los esfuerzos de desarrollo de las aplicaciones requieren recopilar, organizar y presentar una cantidad substancial de datos en los niveles de aplicaciones, sistemas y programas. Una buena parte del esfuerzo de desarrollo de aplicaciones comprender traducir esta información en lógica y código de programa para posteriormente probarla, modificarla e implementarla. A menudo, este es un proceso que lleva tiempo, pero es necesario si se desea desarrollar, usar y mantener aplicaciones de computadora.

CASE es el uso de herramientas automatizadas pata asistir en el proceso de desarrollo de software. Su uso incluir la aplicación de herramientas de software para analizar los requerimientos de software, el diseño de software, la producción de códigos, pruebas, generación de documentos y otras actividades de desarrollo de software.

Los productos CASE se dividen generalmente en tres categorías..

1. *CASE Superior.*- Estos productos se usan para describir y documentar los requerimientos del negocio y de aplicación. Esta información incluye definiciones y relaciones de objetos de datos y definiciones y relaciones del proceso.
2. *CASE Medio.*- Estos productos se usan para desarrollar los diseños detallados. Estos incluyen diseños diseño (layouts) de pantallas y de informes, criterios de edición, organización de los objetos de datos y flujos del procesó. Cuando los

elementos o las relaciones cambian de diseño, es necesario solo hacer alteraciones menores al diseño automatizado y todas las demás relaciones quedan actualizadas automáticamente.

3. CASE Inferior.- Estos productos se emplean para la generación de definiciones de código de programa y definiciones de bases de datos. Estos productos usan información detallada de diseño, reglas de programación y reglas de sintaxis de bases de datos para generar lógica de programa, formatos de archivos de datos o aplicaciones enteras.

Las herramientas CASE están disponibles para entornos de mainframe, de mini y de microcomputadoras. Esas herramientas pueden proveer sistemas de mayor calidad mas rápidamente. Los productos CASE impulsan un enfoque uniforme para el desarrollo de sistemas, posibilitan al almacenamiento y la recuperación de documentos y reducen el esfuerzo manual para desarrollar y presentar información del diseño de los sistemas. éste poder de automatización cambia la naturaleza del proceso de desarrollo eliminando o combinando algunos pasos y alterando la forma de verificar especificaciones y aplicaciones.

El ASI necesita reconocer los cambios en el proceso de desarrollo introducidos por CASE. Algunos sistemas CASE permiten que un equipo de productos produzca un sistema completo a partir de los Diagramas de Flujo de los Datos (DFDs) y de los elementos de de datos sin código alguno de fuente tradicional. En estos casos, los DFDs y los elementos de datos se convierten en código fuente.

El ASI debe obtener la seguridad de que se obtendrán las aprobaciones para las especificaciones apropiadas, que los usuarios continuaran participando en el proceso de desarrollo y que las inversiones en las herramientas CASE rindan beneficios en lo que respecta a calidad y velocidad. Los otros aspectos clave que necesita considerar el ASI con respecto a CASE incluyen los siguientes:

- Las herramientas CASE ayudan en el proceso de diseño de aplicaciones, pero no aseguran que el diseño, los programas y el sistema sean los correctos o satisfacen totalmente las necesidades de la organización.
- Las herramientas CASE deben complementar y encajar en la metodología de desarrollo de aplicaciones; es necesario que esté establecida una metodología para que CASE sea efectiva. La metodología debe ser entendida y usada de manera eficiente por los desarrolladores de software de la organización.
- Es necesario que la integración de los datos trasladados entre los productos CASE o entre los procesos manuales y CASE sea monitoreada, supervisada y controlada
- Los cambios a la aplicación deben estar reflejados en los datos almacenados del producto CASE
- Al igual que una aplicación tradicional, es necesario diseñar los controles para la aplicación.
- Es necesario que el repositorio de CASE (la base de datos que almacena y organiza la documentación, los modelos y otros productos de las diferentes epatas) sean protegidos y solo estén disponibles para los que los necesiten

para su trabajo. Se debe mantener un control estricto de versión sobre esta base de datos.

El ASI puede también convertirse en usuario de las herramientas CASE ya que varias de sus características ayudan al proceso de Auditoria. Los diagramas de flujo de datos, que pueden ser el producto de las herramientas superiores y medias de CASE, pueden ser usados como una alternativa de otras técnicas de diagramas de flujo. Los ASI cuyos departamentos de SI estén empezando a utilizar CASE, deben usar documentación generada por CASE como parte de la Auditoria. Algunos están incluso experimentando con el uso de las herramientas de CASE para crear documentación de Auditoria. Además las herramientas CASE se pueden usar para desarrollar software de consultas no programadas y módulos integrados de Auditoria. Los informes del repositorio se deben usar para lograr entender el sistema y para revisar los controles sobre el proceso de desarrollo.

4.7.- Auditoría al Desarrollo, Adquisición y Mantenimiento de los Sistemas

La tarea del ASI en el desarrollo, adquisición y mantenimiento de sistemas incluyen generalmente lo siguiente:

- Determinar los componentes, objetivos y requerimientos principales del sistema para identificar las áreas que requieren controles, reuniéndose con los

miembros claves del área de desarrollo de sistemas y del equipo de usuarios del proyecto.

- Determinar y clasificar por prioridad los riesgos principales y las exposiciones, del sistema por medio de discusiones con los miembros del equipo de desarrollo de sistemas y de equipo de usuarios del proyecto para permitir la selección de controles apropiados.
- Identificar los controles para mitigar los riesgos y las exposiciones, del sistema utilizando frecuencias de fuentes autorizadas y por medio de discusiones con los miembros del equipo de desarrollo de sistemas y de usuarios del proyecto.
- Aconsejar al equipo del proyecto respecto al diseño del sistema y a la implementación de los controles evaluando los controles disponibles y participando en discusiones con los miembros el equipo de desarrollo de sistemas y de usuarios del proyecto.
- Monitorear, supervisar y controlar (realizar el seguimiento) al proceso de desarrollo de sistemas para asegurar que se hayan implementado los controles, que se cumplan los requisitos de usuario y del negocio y que se siga la metodología de desarrollo / adquisición de sistemas, reuniéndose periódicamente con los miembros del equipo de desarrollo de sistemas y de usuarios del proyecto y revisando la documentación y los productos a ser entregados. También revisar y evaluar las pistas de auditoria del sistema de aplicación para asegurar que existen controles documentados que consideran todos los controles de seguridad, edición y procesamiento. Las pistas de auditoria son mecanismos de rastreo que pueden ayudar a los auditores de IS a

asegurar que se asignan las responsabilidades de los cambios a programas. La información de rastreo en un sistema de administración / gestión de cambios incluye:

- Historial de toda la actividad de las órdenes de trabajo (la fecha de la orden de trabajo, la asignación del programador, los cambios efectuados y la fecha en que se cerró)
- Historial de log-ins y log-outs por programador
- Historial de eliminación de programas.

- Participación en las revisiones posteriores a la implementación
- Evaluar las normas y procedimientos de mantenimiento del sistema para asegurar su adecuación por medio de la revisión de la documentación apropiada, la discusión con el personal clave y la observación
- Probar los procedimientos de mantenimiento del sistema para asegurar que se estén aplicando como se describe en las normas por medio de la discusión y del examen de los registros que los respaldan.
- Evaluar el proceso de mantenimiento del sistema para determinar si se lograron los objetivos de control analizando los resultados de las pruebas y otras evidencias de auditoria.
- Determinar la adecuación de la seguridad de la biblioteca / librería de producción para asegurar la integridad de los recursos de producción identificando y probando los controles existentes.

Administración / Gestion de Proyectos

En todo el proceso de administración de proyectos, el auditor de IS debe analizar los riesgos y exposiciones asociados inherentes a cada etapa de la SDLC y debe asegurar que estén establecidos los mecanismos apropiados de control para minimizar estos riesgos en una forma eficiente y teniendo en cuenta el costo / beneficio de los controles. Se debe tener precaución para evitar recomendar controles que sean más costosos de administrar que los riesgos asociados que se pretende minimizar.

Cuando se esté revisando el proceso de SDLC, el ASI debe obtener documentación de las distintas etapas y asistir a las reuniones del equipo de proyectos ofreciendo asesoramiento al equipo de proyectos durante todo el proceso de desarrollo de los sistemas. El ASI debe también hacer una estimación de la capacidad del equipo de proyectos para producir resultados claves en las fechas prometidas.

La documentación adecuada y completa de todas las etapas del proceso de SDLC debe ser evidente. Los tipos característicos de documentación deben incluir pero no limitarse a lo siguiente:

- Objetivos que definan que es lo qué se va a realizar durante esa etapa.
- Los resultados claves de la etapa con el personal de proyectos al que se le asignaron responsabilidades directas sobre estos resultados.
- Cronograma del proyecto con fechas destacadas para la concusión de los resultados claves.

- Previsión económica de esa etapa definiendo los recursos y el costo de los recursos que se requieren para concluir la etapa.
- Como mínimo, aprobaciones firmadas por la gerencia de desarrollo de sistemas y del usuario, responsable del costo del proyecto y/o el uso del sistema.

Estudio de Factibilidad / Viabilidad

- El ASI debe revisar la documentación producida con esta fase para verificar si es razonable.
- Se debe poder verificar la justificación / beneficios de todos los costos y los mismos deben ser presentados mostrando los beneficios anticipados que se van a obtener.
- Identificar y determinar la importancia crítica de la necesidad que se desea satisfacer.
- Determinar si se puede alcanzar una solución con los sistemas ya existentes. En caso contrario, revisar la evaluación de las soluciones alternativas para verificar si éstas son razonables.
- Determinar si la solución escogida es razonable.

Definición de los Requerimientos

- El ASI debe obtener el documento de definición detallada de los equipos y verificar si son correctos por medio de entrevistas con los departamentos relevantes de usuario.

- Identificar los miembros claves en el equipo del proyecto y verificar que todos los grupos de usuarios afectados estén debidamente representados.
- Verificar que la iniciación del proyecto y el costo del mismo hayan recibido la debida aprobación de la gerencia.
- Revisar las especificaciones conceptuales del diseño (transformaciones, descripciones de datos) para asegurar que el mismo atiende a las necesidades del usuario.
- Revisar el diseño conceptual para asegurar que se hayan definido las especificaciones de control.
- Determinar que un número razonable de vendedores recibió una propuesta que cubra el alcance del proyecto y los requerimientos del usuario.
- Determinar si la aplicación es una candidata para el uso de rutina(s) integradas de auditoria. En caso afirmativo, solicitar que la rutina sea incorporada en el diseño conceptual del sistema.

Proceso de Adquisición de Software

- Analizar la documentación a partir del estudio de factibilidad para determinar que la decisión de adquirir una solución fue apropiada.
- Revisar la Solicitud de Propuesta (SP) para asegurar que este cubre los puntos enumerados es esta sección.
- Determinar si el vendedor seleccionado está respaldado por documentación de SP.

- Revisar el contrato del vendedor antes de su firma para asegurarse que incluye los puntos enumerados.
- Asegurarse de que el contrato sea revisado por el asesor legal antes de que sea firmado.

Diseño Detallado y Etapas de la Programación

- Revisar los diagramas de flujo del sistema para verificar si se ajusta al diseño general. Verificar que hayan obtenido las debidas aprobaciones para cualquier cambio y que todos los cambios hayan sido discutidos y aprobados por la gerencia de usuario apropiada.
- Revisar los controles para el ingreso de los datos, del procesamiento y de los resultados, diseñados en el sistema para verificar si son los apropiados.
- Entrevistar a los usuarios claves del sistema para determinar su comprensión de cómo opera el sistema y determinar su nivel de participación en el diseño de los formatos de pantalla y reportes de salida.
- Evaluar si las pistas de auditoria son adecuadas para permitir que se rastreen y se evidencie la responsabilidad por las transacciones del sistema.
- Verificar la integridad de los cálculos y procesos claves
- Verificar que el sistema pueda identificar y procesar los datos erróneos correctamente.
- Revisar los resultados de aseguramiento de calidad de los programas desarrollados durante esta etapa.

- Verificar que se hayan efectuado todas las correcciones de los errores de programación y que se hayan codificado las pistas de auditoria o los módulos integrados de auditoria recomendados, en los programas apropiados.

Etapas de Pruebas

La etapa o fase de pruebas es crucial para determinar que se hayan validado los requerimientos del usuario, que el sistema esté funcionando como se anticipo y que los controles trabajen como se pretendía.

Por lo tanto, es esencial que el auditor de SI participe en la revisión de esta fase.

- Revisar el plan de pruebas para verificar si esta completo y con evidencia que indique la participación del usuario como por ejemplo en la definición de los escenarios de pruebas y la aprobación de los resultados obtenidos. Considerar una repetición de la ejecución de las pruebas Críticas.
- Se debe efectuar una reconciliación de los totales de control y de los datos convertidos
- Revisar los informes de errores para verificar su precisión para reconocer los datos erróneos y para la resolución de errores.
- Verificar el procesamiento cíclico para verificar si está correcto (procesamiento del fin de mes, fin de año etc.)
- Entrevistar a los usuarios finales del sistema para verificar si entienden los nuevos métodos, los nuevos procedimientos y las instrucciones de operación.

- Revisar, durante la fase de pruebas, la documentación del sistema

Fase de Implantación

Esta fase o etapa se inicia únicamente después de que se haya pasado exitosamente la fase de pruebas. El sistema debe estar instalado en conformidad con los procedimientos de control de cambios de la organización. El ASI debe verificar que se hayan obtenido las firmas de aprobación apropiadas antes de la implementación.

- Revisar los procedimientos planificados y usados para programar y poner en funcionamiento el sistema junto con los parámetros del sistema usados para la ejecución del cronograma de producción.
- Revisar toda la documentación del sistema para asegurar que está completa y para asegurarse de que la totalidad de las actualizaciones recientes, a partir de la fase de pruebas, hayan sido incorporadas.
- Verificar todas las conversaciones de datos asegurarse de que estén correctas y completas antes de implementar el sistema en producción.

Revisión Posterior a la Implementación

Después de que el nuevo sistema se haya establecido en el ambiente de producción, se debe de efectuar una revisión posterior a la implementación. Antes de esta revisión, es importante que se de tiempo suficiente para que el sistema se estabilice en producción. De éste modo habrá oportunidad para que aparezca cualquier problema significativo.

- Determinar si se lograron los objetivos y requerimientos del sistema. Durante la revisión posterior a la implementación, se debe presentar mucha atención a la utilización que hace el usuario del sistema y la satisfacción general de éste con el sistema. Esto indicará si se lograron los objetivos y requerimientos del sistema.
- Determinar si se están midiendo y analizando el costo-beneficio identificado en el estudio de factibilidad, y si los mismos son reportados a la Gerencia con exactitud.
- Revisar las solicitudes de cambio a programas efectuadas para evaluar para evaluar el tiempo de cambios que requiere el sistema. El tipo de cambios solicitado puede identificar problemas en el diseño, en la programación o en la interpretación de los requerimientos de los usuarios.
- Revisar los controles integrados en el sistema para asegurar que los mismos estén operando en conformidad con el diseño. Si se incluyó un módulo integrado de auditoría en el sistema, usar éste módulo para probar las operaciones claves.
- Revisar los registros de error de operación para determinar si hay algún problema de recursos o de operación inherentes en el sistema. Los registros pueden indicar una planificación o prueba inapropiadas del sistema antes de su implementación.
- Revisar los balances / cuadres de control de entrada y salida y demás reportes para verificar que el sistema esté procesando los datos correctamente.

Procedimientos de Cambios al Sistema y Proceso de Migración de Programas

A continuación de la implementación y de la estabilización de un sistema, el mismo entra en una etapa de desarrollo o mantenimiento continuado. Esta fase continúa hasta que el sistema sea reemplazado o discontinuado. Comprende las actividades que se requieren para corregir los errores en el sistema o para aumentar las funcionalidades del sistema.

Cuando revise estas actividades, el auditor de SI debería:

- Evaluar si los procedimientos de la organización para autorizar, dar prioridad y rastrear los cambios al sistema son los apropiados.
- Identificar los cambios al sistema y verificar que se haya dado la autorización debida para efectuar el cambio en conformidad con las normas de la organización.
- Revisar la documentación permanente del programa para asegurarse de que se retiene la evidencia (pista de auditoria) en relación con los cambios del programa.
- Evaluar si los procedimientos que están establecidos son adecuados para asegurarse de que se han hecho las actualizaciones apropiadas a la documentación del sistema.
- Revisar la documentación técnica y del usuario para asegurarse de que está al día y que refleja con exactitud la funcionalidad del sistema actual.
- Evaluar si los procedimientos de la organización son adecuados en relación con el control de cambios a programas.

- Evaluar si las restricciones de acceso de seguridad a los módulos fuentes y los ejecutables en producción son adecuadas.
- Evaluar si los procedimientos de la organización para atender los cambios de emergencia a los programas son adecuados.
- Evaluar si las restricciones de acceso de seguridad en el uso de los logon_Ids de emergencia, son adecuadas.
- Evaluar si los procedimientos establecidos para probar los cambios a los sistemas son adecuados.
- Revisar la evidencia (los planes de pruebas y los resultados de las pruebas) para asegurarse de que se llevan a cabo los procedimientos prescritos por las normas organizativas.
- Revisar los procedimientos establecidos para asegurar la integridad del código ejecutable y fuente.
- Revisar los módulos ejecutables en producción y verificar que haya una y sólo una versión correspondiente al código fuente del programa.

5.- CASO PRÁCTICO

Compañía RICO's, S.A. de C.V

Revisión de Controles Generales en el Área de Desarrollo y Mantenimiento de Sistemas

La actividad principal de la Compañía RICO's, S.A. de C.V. (en adelante RICO's) es la elaboración de frutas deshidratadas, que exporta principalmente a Estados Unidos y ahora, bajo Tratados Comerciales con la Unión Europea.

Actualmente RICO's utiliza hojas de cálculo de "Excel" para el proceso de producción (materias primas, inventario de producto terminado y movimientos de almacén) y no tienen planeado adquirir un sistema que les permita tener la certeza de que la información es confiable, íntegra, etc.

La aplicación "Contabilidad y Finanzas Integral" procesa la información bajo la plataforma de Novell NetWare 4.10, en una PC Server 310 y los módulos que la conforman son:

- Contabilidad
- Bancos
- Nómina
- Facturación
- Clientes
- Inventarios
- Proveedores
- Compras

La aplicación es un software adquirido desde Mayo de 1996 al proveedor "Software y Sistemas a su Medida, S.A. de C.V." el cual funciona como intermediario de la casa matriz del proveedor "Proyectos Computacionales, S.A. de C.V.", este se encuentra en Guadalajara, y es el responsable de custodiar la aplicación.

Comunicación entre sistemas

Debido a que el sistema "Contabilidad y Finanzas Integral", como su nombre lo indica es integral, todos lo módulos mantienen una comunicación constante y en línea, de tal forma que cuando se captura información o se hace un cambio en un módulo automáticamente la transacción se registra en el módulo correspondiente.

Es importante comentar que la aplicación para el proceso de producción de la planta que se lleva en hojas de Excel genera un reporte, el cual se le proporciona al Área de Contabilidad quien se encarga de cargar la información en el sistema "Contabilidad y Finanzas Integral".

Estructura Orgánica

La estructura orgánica del Área de Sistemas se encuentra integrada únicamente por el Jefe de Informática. (Responsable de Informática).

Adquisición, implementación y mantenimiento de Sistemas

El objetivo del proceso de adquisición, implementación y mantenimiento de Sistemas, es el de adquirir (incluyendo el desarrollo y/o compra), implementar y mantener (ej. actualizar o modificar) los sistemas de Tecnologías de Información (TI) y el software de aplicación que soporta la estrategia, metas y objetivos de RICO's.

En la compañía se observó lo siguiente:

El Jefe de Sistemas (Responsable de Informática) es la única persona con acceso a todos los recursos del sistema, ya que el área de Sistemas se integra por una sola persona. *Ver punto en Carta de Oportunidades de Mejora.*

Actualmente, no se utiliza una aplicación para el proceso de producción de la planta, el control de los movimientos de almacén, materia prima y producto terminado se lleva en hojas de cálculo de "Excel". *Ver punto en Carta de Oportunidades de Mejora.*

La aplicación "Contabilidad y Finanzas Integral", fue desarrollado por el proveedor Proyectos Computacionales, S.A. de C.V., el cual es el propietario de los programas fuente, sin embargo éste no ofrece el servicio de mantenimientos y modificaciones a la aplicación de forma directa a la Compañía, sino a través de un proveedor intermediario (Software y Sistemas a su Medida, S.A. de C.V.).

Solicitud de mantenimiento de sistemas

Se cuenta con dos tipos de solicitudes:

- Los requerimientos de los usuarios que pueden ser atendidos por el Responsable de Informática son para extraer información de la base de datos, las cuales son realizadas de forma verbal. *Ver punto en Carta de Oportunidades de Mejora.*
- Los requerimientos para la realización de mantenimientos y/o modificaciones a la aplicación, en ocasiones son solicitadas por el Área Usuaria y en otras son sugeridas por el proveedor. Cabe mencionar que las solicitudes por parte del usuario no son muy frecuentes.

Si es un mantenimiento solicitado por los usuarios, el responsable del Área Usuaria lo solicita vía telefónica al Jefe de Sistemas, quién lo canaliza con el Proveedor de forma verbal, la modificación que se requiere realizar. *Ver punto en Carta de Oportunidades de Mejora.*

En el caso de sea una modificación a la aplicación sugerida por el proveedor, éste le llama por teléfono al Responsable de Sistemas sugiriéndole el cambio, si este es aceptado, el proveedor realiza la modificación a la aplicación. *Ver punto en Carta de Oportunidades de Mejora.*

Control de versiones

La custodia del código fuente de la aplicación "Contabilidad y Finanzas Integral" es responsabilidad del proveedor por lo que el Jefe de Informática no lleva este control.

Pruebas con los usuarios

El proveedor es el encargado de realizar las pruebas en el sistema "Contabilidad y Finanzas Integral", pero los usuarios no participan en ellas. *Ver punto en Carta de Oportunidades de Mejora.*

Traspaso a producción

Una vez que el proveedor realiza las modificaciones y prueba los cambios, le llama por teléfono al Responsable de Sistemas, avisándole que ya puede recoger el disco que contiene la modificación (parche) a las oficinas del proveedor, así como un documento en Word en donde indica los cambios realizados al sistema (es un anexo al manual del usuario).

Posteriormente el Responsable de sistemas lo recoge y procede a su instalación en el servidor.

Cuando se presenta algún error en el sistema, el Responsable de Sistemas solicita ayuda al proveedor, quien sólo puede asesorar al Responsable de Sistemas para poder reestablecer los sistemas. El proveedor no puede accesar al sistema remotamente.

Manuales de usuario

Actualmente, se cuenta con los manuales de usuario del sistema "Contabilidad y Finanzas Integral", así como de los anexos de las modificaciones y/o mantenimientos que son realizados.

Identificación de Controles Relevantes

Los controles relevantes detectados en operación relativos al proceso de Adquisición, implementación y mantenimiento de las soluciones de TI, son los siguientes:

- *Acceso remoto del proveedor*

  Cuando el sistema presenta algún error, el Jefe de Sistemas solicita ayuda al proveedor, quien sólo puede asesorar al Jefe de Sistemas para poder reestablecer los sistemas. El proveedor no puede accesar al sistema remotamente.

- *Manuales de usuario*

  Compañía Engrande cuenta con los manuales de usuario del sistema "Contabilidad y Finanzas Integral".

Ejecución del Recorrido de los Controles Detectados

Debido a que no existe evidencia de las solicitudes de mantenimientos al sistema "Contabilidad y Finanzas Integral", se corroboró con el proveedor vía telefónica, que las solicitudes así como el aviso que éste le da al responsable de sistemas informándole que el cambio fue realizado y que puede pasar a recoger el disco a las oficinas del proveedor, son de forma verbal. Adicionalmente, verificamos los sobres y los discos en los cuales el proveedor envía el cambio realizado al sistema (parche). El Responsable de Sistemas nos mostró el contenido de uno de los discos que le proporciona el proveedor, en el cual verificamos que contiene dos archivos: el ejecutable (parche) y un archivo de word.

Revisamos cada uno de los manuales de usuario de los módulos del sistema "Contabilidad y Finanzas Integral", los cuales incluyen información detallada sobre el uso de cada uno de los mismos.

Posteriormente, entrevistamos a un usuario, quien nos comentó que solicitan reportes de explotación de información al Responsable de Informática de forma verbal, los cuales son realizados por el Responsable de Informática, también comentó que estas peticiones no son muy frecuentes.

Evaluación Preliminar de la efectividad de los Controles sobre los procesos de Adquisición, Implementación y Mantenimiento de las soluciones de TI.

En base a los resultados, es nuestra opinión que NO existen controles en el Área de Sistemas que aseguren que los desarrollos y mantenimientos de programas son autorizados, probados y aprobados antes de ser traspasados a producción, por lo que concluimos que los controles sobre el proceso de Adquisición, Implementación y Mantenimiento de Sistemas de TI son INEFECTIVOS.

Compañía RICO's, S.A. de C.V

Revisión de Controles Generales en el Área de Desarrollo

y Mantenimiento de Sistemas

Auditoría al 27 de Febrero de 2002

CARTA DE OPORTUNIDADES DE MEJORA

Hemos revisado los controles generales del Área de Desarrollo y Mantenimiento de Sistemas para asegurarnos de que los cambios a programas son autorizados, probados y aprobados antes de ser liberados en producción de las aplicaciones financieras consideradas significativas.

Nuestra revisión no tuvo por objeto verificar exhaustivamente todos los controles del Área de Desarrollo y Mantenimiento de Sistemas, sino sólo aquellos que protegen la integridad de la información financiera de la Compañía.

Para llevar a cabo la revisión de los controles generales en la Área de Sistemas sostuvimos entrevistas con:

L.I. Juan Carlos Basillo Olivares Responsable de Informática

A continuación describimos los aspectos en los que creemos que existen oportunidades de mejora:

Solicitud para mantenimientos al sistema "Contabilidad y Finanzas Integral"

La Compañía no elabora peticiones por escrito para solicitar una adecuación al sistema de "Contabilidad y Finanzas Integral". Actualmente, el Área de Sistemas informa verbalmente al Proveedor cuando desean que se realice una adecuación al mismo.

Lo anterior provoca que no exista evidencia de los cambios solicitados y su debida autorización de las áreas usuarias.

Establecer como procedimiento, que cualquier cambio a los sistemas o reportes que requieran los usuarios debe ser solicitado por escrito y debidamente autorizado por el usuario responsable de la información. Si las solicitudes se llegan a realizar por medio de correo electrónico, recomendamos que sean respaldadas en un medio magnético, de esta forma se tendrá evidencia de la petición de los usuarios.

Participación del usuario en las pruebas del sistema

El proveedor es el encargado de realizar las pruebas en el sistema "Contabilidad y Finanzas Integral", pero los usuarios no participan en ellas.

Lo anterior no permitiría asegurar que los cambios o mantenimientos a los programas, se realicen de acuerdo al requerimiento del usuario.

Recomendamos que en todos los casos participe el usuario y que al final de cada una de las pruebas realizadas, se obtenga la autorización correspondiente que los cambios, efectivamente son los que se solicitaron.

Solicitud para extraer información del sistema "Contabilidad y Finanzas Integral"

Los requerimientos de los usuarios que pueden ser atendidos por el Responsable de Informática son para extraer información de la base de datos, pero no hay evidencia de las peticiones.

Lo anterior provoca que no exista evidencia de las solicitudes y su debida autorización de las áreas usuarias.

Establecer como procedimiento, que cualquier reporte que requieran los usuarios debe ser solicitado por escrito y debidamente autorizado por el usuario responsable de la información. Si las solicitudes se llegan a realizar por medio de correo electrónico, recomendamos que sean respaldadas en un medio magnético, de esta forma se tendrá evidencia de la petición de los usuarios.

Conclusión

En base a los resultados obtenidos en la aplicación de nuestros procedimientos de auditoría, es nuestra opinión que NO existen suficientes controles en el Área de Sistemas que aseguren que los desarrollos y mantenimientos de programas son autorizados, probados y aprobados antes de ser traspasados a producción.

Por lo tanto la evaluación de los controles programados NO podrán ser evaluados como EFECTIVOS, ya que no se puede confiar en que éstos funcionaron como fueron diseñados durante todo el periodo auditado.

CONCLUSIÓN

Con el presente trabajo, podemos concluir que es de gran importancia para las Compañías privadas, así como para las públicas, la realización de las Auditorías en Sistemas en el Área de Desarrollo Mantenimiento de Sistemas, debido a que en estos (los sistemas) es en donde se procesa la mayor parte de la información más sensitiva (financiera) de las compañías.

Y que el contar con una Auditoría en Sistemas en el Área de Desarrollo y Mantenimiento de Sistemas, trae consigo beneficios en la minimización de costos en la adquisición y/o mantenimiento de sistemas, así como una mayor eficiencia y eficacia en el personal y en los sistemas.

En la Auditoría en Sistemas en el Área de Desarrollo y Mantenimiento de Sistemas, el Auditor es uno de los elemento más importantes, por ende, debe tener los conocimientos técnicos básicos, así como conocer y aplicar las normas y principios éticos aplicables a los sistemas de Auditorías de Información, que le permitan un desarrollo pleno y una eficiencia en su trabajo.

Con los conocimientos adquiridos el Auditor de Sistemas, será capaz de revisar y evaluar los controles detectados, de acuerdo al riesgo que represente dentro de la operatividad de la compañía, así como de generar un reporte, en el cual se le informe a la Dirección, el

estado actual del Área de Desarrollo y Mantenimiento de Sistemas, así como las oportunidades de mejora para minimizar los riesgos detectados dentro de la Compañía.

Con lo anterior podemos considerar como provechosa la conclusión obtenida en el presente trabajo.

Como conclusión personal me permitió con este trabajo de investigación solidificar los conocimientos adquiridos durante mi estancia dentro de la Facultad de Estudios Superiores Cuautitlán, así como ver la importancia de estos dentro de mi campo laboral.

Me resultará gratificante que este trabajo se convierta en una fuente de información que proporcione las bases necesarias a todos aquellos a los que les interese adentrarse en este mundo de la Auditoría de Sistemas, sembrando así la inquietud de seguir investigando y capacitándose para un desarrollo profesional que siga fortaleciendo el buen nombre de nuestra institución.

ANEXO A

HOJA DE TRABAJO PARA CLASIFICAR LAS AUDITORÍAS A LOS SISTEMAS APLICATIVOS EN PRODUCCIÓN, EN CATEGORÍAS DE AUDITORÍA

		CLASIFICACIÓN DE LAS ÁREAS DE AUDITORÍA					
ÁREA DE AUDITORÍA	CATEGORÍA DE CALIFICACIÓN	MUY IMPORTANTE 5	IMPORTANTE 4	IMPORTANTE, PERO NO CRÍTICO. 3	NO IMPORTANTE 2	REALMENTE SIN IMPORTANCIA 1	CALIFI-CACIÓN
Procedimientos, estándares y regulaciones.							
Controles internos.							
Datos.							
Documentaciones.							
Pistas de auditoría.							
Operación del sistema en producción.							
Necesidades de los usuarios.							

HOJA DE TRABAJO PARA CLASIFICAR LA AUDITORÍA INFORMÁTICA COMO SOPORTE A LAS DEMÁS ÁREAS DE AUDITORÍA, EN CATEGORÍAS DE AUDITORÍA

		CLASIFICACIÓN DE LAS ÁREAS DE AUDITORÍA					
ÁREA DE AUDITORÍA	CATEGORÍA DE CALIFICACIÓN	MUY IMPORTANTE 5	IMPORTANTE 4	IMPORTANTE, PERO NO CRÍTICO. 3	NO IMPORTANTE 2	REALMENTE SIN IMPORTANCIA 1	CALIFI-CACIÓN
Consejo técnico.							
Extracción de reportes.							
Entrenamiento técnico.							
Guías de auditoría.							
Apoyo en la dirección de auditorías.							
Operación del sistema en producción.							
Necesidades de los usuarios.							

HOJA DE TRABAJO PARA CLASIFICAR LAS AUDITORÍAS A LA INFRAESTRUCTURA, EN CATEGORÍAS DE AUDITORÍA

		CLASIFICACIÓN DE LAS ÁREAS DE AUDITORÍA					
ÁREA DE AUDITORÍA	CATEGORÍA DE CALIFICACIÓN	MUY IMPORTANTE 5	IMPORTANTE 4	IMPORTANTE, PERO NO CRÍTICO. 3	NO IMPORTANTE 2	REALMENTE SIN IMPORTANCIA 1	CALIFICACIÓN
Controles administrativos.							
Operaciones computacionales.							
Controles en el hardware.							
Controles en los sistemas operativos y en el software.							
Selección en el software y en el hardware.							
Estándares, políticas, procedimientos y convenciones.							
Seguimiento de errores.							
Seguridad y privacía.							
Planes de contingencia, respaldos y recuperaciones.							

HOJA DE TRABAJO PARA CLASIFICAR LAS AUDITORÍAS A LOS SISTEMAS EN DESARROLLO, EN CATEGORÍAS DE AUDITORÍA

		CLASIFICACIÓN DE LAS ÁREAS DE AUDITORÍA					
ÁREA DE AUDITORÍA	CATEGORÍA DE CALIFICACIÓN	MUY IMPORTANTE 5	IMPORTANTE 4	IMPORTANTE, PERO NO CRÍTICO. 3	NO IMPORTANTE 2	REALMENTE SIN IMPORTANCIA 1	CALIFICACIÓN
Consejo técnico.							
Extracción de reportes.							
Entrenamiento técnico.							
Guías de auditoría.							
Apoyo en la dirección de auditorías.							

ANEXO B

HOJA DE TRABAJO PARA PRIORIZAR LAS ÁREAS AUDITABLES DE AUDITORÍA INFORMÁTICA

CLASIFICACIÓN POR PUNTAJE (Indicando el nombre de la tasa)		CLASIFICADO POR

ÁREA DE AUDITORÍA							PUNTAJE TOTAL	PUNTAJE	JUICIO
AUDITORÍA A LOS SISTEMAS APLICATIVOS EN PRODUCCIÓN.									
Procedimientos, estándares y regulaciones.									
Controles internos.									
Datos.									
Documentaciones.									
Pistas de auditoría.									
Operación del sistema en producción.									
Necesidades de los usuarios.									
AUDITORÍA COMO SOPORTE A LAS DEMÁS ÁREAS DE AUDITORÍA.									
Consejo técnico.									
Extracción de reportes.									
Entrenamiento técnico.									
Guías de auditoría.									
Apoyo en la dirección de auditorías.									

AUDITORÍA A LA INFRAESTRUCTURA									
Controles administrativos.									
Operaciones computacionales.									
Controles en el hardware.									
Controles en los sistemas operativos y en el software.									
Selección en el software y en el hardware.									
Estándares, políticas, procedimientos y convenciones.									
Seguimiento de errores.									
Seguridad y privacía.									
Planes de contingencia, respaldos y recuperaciones.									
AUDITORÍA A LOS SISTEMAS EN DESARROLLO									
Consejo técnico.									
Extracción de reportes.									
Entrenamiento técnico.									
Guías de auditoría.									
Apoyo en la dirección de auditorías.									

ANEXO C

MATRIZ DE PRODUCTOS FINALES

FASE	ACTIVIDAD	PRODUCTO
1. PLANEACIÓN	1.- Definición. de objetivos y alcances.	Lista de Objetivos y alcances. Carta de inicio de la revisión.
	2.- Recabación de información básica	Lista de requerimientos de información básica. Programa. de entrevistas iniciales. Resumen de entrevistas.
	3.- Análisis de información básica.	Descripción narrativa de las características principales. Resumen del análisis de la información inicial.
	4.- Diagnóstico de viabilidad.	Resumen de Viabilidad.
	5.- Planeación del Desarrollo.	Plan de desarrollo de la revisión.
2. DESARROLLO	1.- Obtención de Información. detallada.	Documentación de auditoría (legajo de auditoría, conteniendo los productos finales de las fases anteriores).
	2.- Detallar Plan Original.	Programa de trabajo.
	3.- Evaluación de controles.	Lista de controles. Matrices de evaluación (cuestionarios de control interno). Resumen de situación de control interno.
	4.- Diseño de pruebas de auditoría.	Programa de pruebas de auditoría.
	5.- Aplicación de pruebas de auditoría.	Papeles de trabajo de las pruebas. Lista de observaciones. Resumen de hallazgos.
3.- COMUNICACIÓN	1.- Evaluación y documentación de Resultados.	Borrador observaciones y sus recomendaciones. Carpeta de apoyo actualizada.
	2.- Elaboración de informe.	Borrador de informe. Borrador de informe para comentar. Documentación de sustento a las observaciones (carpeta económica).
	3.- Autorización de la Subdirección. Auditoría.	Informe autorizado.

FASE	ACTIVIDAD	PRODUCTO
	4.- Comentar con áreas involucradas.	Documentación que sustente los cambios al informe. (en caso de diferencias). Informe confirmado por las áreas involucradas (levantando minuta formal).
	5.- Documentación de acuerdos y ajustes.	Carpeta de apoyo actualizada. Informe final.
	6.- Autorización de la Dirección de Auditoría.	Informe final autorizado.
	7.- Emisión del informe.	Memorándum para envío del informe y copias correspondientes. Copias ciegas (del informe final).
4. SEGUIMIENTO	1.- Obtención de Respuesta del informe.	Solicitud de respuesta al informe (en caso necesario). Respuesta al informe.
	2.- Revisión de Respuesta.	Comunicación de desacuerdos (En caso de existir).
	3.- Planeación del seguimiento.	Programación del seguimiento.
	4.- Desarrollo del seguimiento.	Resumen de observaciones. Informe del seguimiento. Carpeta de apoyo del informe del seguimiento.

ANEXO D

ABREVIATURAS

Análisis Estructurado	SA
Aseguramiento de la Calidad	AC
Auditor Informático	AI
Auditores de Sistemas de Información	ASI
Auditoría en Sistemas	AS
Control Objetives for Information and Related Technologies	COBIT
Ciclo de Vida del Desarrollo de Sistemas	CVDS
Desarrollo de Sistemas Orientados a Datos (Data –Orient System Development - DOSD)	DOSD
Desarrollo de Sistemas Orientados a Objetos (Objet-Oriented System Development)	OOSD
Desarrollo Rápido de Aplicaciones	RAD
Diagramas de Flujos de Datos	DFDs
Dirección General de la Organización	DGO
Diseño Detallado	DD
Fabricación Asistida por Computadora	CAM
Factores / Criterios / Métricas	FCM
Filtrado del Lenguaje de Control	JCL
Identificador	ID
Information Systems Audit and Control Association / Foundation	ISACA
Ingeniería de Software Asistida por Computadora	CASE
Inteligencia Artificial	IA
Intercambio Electrónico de Información	EDI
Lenguajes de Programación de Cuarta Generación	4GLs
Método de la Ruta Critica	CPM
Modelos Específicos de Evaluación de Procesos de Software	CMM o SIPCE
Número de Identificación Personal	NIP
Organization for International Standarization	ISO
Programación Estructurada	PE
Ruta Critica	RC
Sistemas de Apoyo para la Toma de Decisiones	DSS
Sistemas de Información	SI
Software Engineering Institute	SEI
Solicitud de Propuesta (Request for Proposal R.F.P.)	SP
System Development Life Cycle	SDLC
Técnica de Revisión y Evaluación de Programas	PERT
Transferencia Electrónica de Fondos	EFT
Tecnologías de Información	TI

BIBLIOGRAFÍA

A.J. Tomas, Is Douglas / David H. Li
Auditoría Informática
Editorial Trillas, 1999

Calvo-Manzano, J.A. y Fernández, L.,
Hacia la calidad del software a través de la mejora de procesos
Novatica (http://www.ati.es/PUBLICACIONES/novativa), nº 123, 1996

Cassel-Jackson
Introduction to Computers & Information Processing

Corporación Salazar y Asociados S.C.
Apuntes de Diplomado
1991, México

Echenique García José Antonio
Auditoría en Informática
Editorial McGraw-Hill Interamericana de México S.A. de C.V., 1990.

Gonick Larry
Computación
Editorial Harla, 1985.

Gonzalo Cuevas Agustín
Ingeniería de Software: Práctica de la Programación
Editorial ra-ma, serie paradigma, 1991.

H. Fine Leonard
Seguridad en Centros de Cómputo, Políticas y Procedimientos
Edit. Trillas, 1988.

Hernández Hernández Enrique
Auditoría en Informática. Un enfoque metódico y práctico
Editorial Continental, S.A. de C.V., 1996.

Hernández Sampieri Roberto / Fernández Collado Carlos / Baptista Pilar
Metodología de la Investigación
Editorial McGraw-Hill
Segunda edición, 1998.

IEEE Std 1061-1992.
Standard for a software quality metrics methodology

IEEE Std-1995
Standard for developing software life cycle processes

Institute of Internal Auditors Foundation
Systems Auditability and Control Report

ISACA (Information Systems Audit and Control Association / Foundation)
COBIT (Control Objetives for Information and Related Technologies)
OBJETIVOS DE CONTROL
2a. edición.

ISACA (Information Systems Audit and Control Association / Foundation)
Manual de Información Técnica para la preparación al examen CISA 2001
(Certified Information Systems Auditor)

ISO 9126, 1991
Software product evaluation. Quality characteristics and guidelines for their use

ISO 9001:1994.
Quality systems -- Model for quality assurance in design, development, production, installation and servicing

ISO 9002:1994.
Quality systems -- Model for quality assurance in production, installation and servicing

ISO 9000-3, 1997 (ISO, Part 3:)
Guidelines for the application of ISO 9001:1994 to the development, supply, install and maintenance of computer software

ISO 15504-1: 1998
Software process assessment. Part-1: Concept and introductory guides

J.R. Santillana G.
Conoce las Auditorías
Ediciones Contables y Administrativas

Jann Derrien
Técnicas de la Auditoría Informática
Editorial Alfaomega, 1994.

Jeffrey L. Whitten, Lonnie D. Bentley, Victor M. Barlow
Análisis y Diseño de Sistemas
Editorial Prentice-Hall Hispanoamericana, S.A.
México, 1994.

Joyanes Aguilar Luis
Metodología de la Programación
Editorial McGraw-Hill, 1988.

Kendall, Kenneth E. / Kendall, Julie E.
Análisis y Diseño de Sistemas de Información
Editorial Pearson Educación
Tercera edición, 1997.

Luis Fernández Sanz, Miren Idoia Alarcón Rodríguez
Necesidades de medición en la gestión y el aseguramiento de calidad del software
Universidad Europea de Madrid
Universidad Autónoma de Madrid

Dr. Mercado H. Salvador
¿Cómo hacer una Tesis?
Editorial Limusa, 1994.

Mora José Luis / Molino Enzo
Introducción a la Informática
Editorial Trillas

Piattini Velthuis Mario Gerardo / del Peso Navarro Emilio
Auditoría Informática. Un enfoque práctico
Editorial Alfaomega ra-ma, 1999.

Pratt W. Terrence / Zelkowitz V. Marvin
Lenguajes de Programación Diseño e Implementación
Editorial Prentice-Hall, Hispanoamericana, S.A.
Tercera edición, 1996.

Pressman S. Roger
Ingeniería del Software. Un enfoque práctico
Editorial McGraw-Hill
Tercera edición, 1992.

Ramón García / Pelayos y Gross
Pequeño Larousse Ilustrado
Ediciones Larousse, S.A., 1985.

Richard Fairley
Ingeniería de Software
Editorial McGraw-Hill, 1988.

Rodrígues Beristain Luis Manuel
Auditoría al Área de Telecomunicaciones (Tesis)
Universidad del Valle de México, 1995.

Rodríguez, Luis Angel
Seguridad de la Información en Sistemas de Cómputo
Ediciones Ventura, 1995.

Santillana Gonzáles J.R.
Conoce las Auditorías
Ediciones Contables y Administrativas S.A. de C.V.
Quinta edición, 1992.

Senn James, A.
Análisis y Diseño de Sistemas de Información
Editorial McGraw-Hill

Squire, Enid
Introducción al Diseño de Sistemas
Editorial Fondo Educativo Interamericano, 1984

Páginas de INTERNET consultadas al 27 de Febrero de 2002

- http://www.asc.unam.mx
- http://www.ati.es/PUBLICACIONES/novativa
- http://www.isaca.org
- http://www.iso.ch/cate/35080.html
- http://www.webdi.cem.itesm.mx