AUDITORIA DE INFORMÁTICA

La Informática hoy, forma parte vital la gestión integral de la empresa, las organizaciones informáticas forman parte de lo que se ha denominado el "management" o gestión de la empresa. Debido esta importancia, existe la Auditoria Informática.

La palabra auditoría proviene del latín auditorius, y de esta proviene la palabra auditor, que se refiere a todo aquel que tiene la virtud de oír.

Aplicación

En informática, una aplicación es un tipo de programa informático diseñado como herramienta para permitir a un usuario realizar uno o diversos tipos de trabajos. Esto lo diferencia principalmente de otros tipos de programas como los sistemas operativos (que hacen funcionar al ordenador), las utilidades (que realizan tareas de mantenimiento o de uso general), y los lenguajes de programación (con el cual se crean los programas informáticos), Ciertas aplicaciones desarrolladas «a medida» suelen ofrecer una gran potencia ya que están exclusivamente diseñadas para resolver un problema específico. Algunos ejemplos de programas de aplicación son los procesadores de textos, hojas de cálculo, y base de datos, finanzas, correo electrónico, navegador web, compresión de archivos, presupuestos de obras, gestión de empresas, etc.

“Actualmente, con el uso de dispositivos móviles se ha extendido el concepto APP, Aplicación informática para dispositivos móviles o tablets con multitud de funcionalidades. Desde juegos hasta aplicaciones para realizar tareas cotidianas. Es un abanico enorme que hacen más interactivo los dispositivos móviles”.[1]

1. Controles administrativos en un ambiente de Procesamiento de Datos

La máxima autoridad del Área de Informática de una empresa o institución debe implantar los siguientes controles que se agruparan de la siguiente forma:

- Controles de Preinstalación
- Controles de Organización y Planificación
- Controles de Sistemas en Desarrollo y Producción
- Controles de Procesamiento

[1] http://es.wikipedia.org/wiki/Aplicaci%C3%B3n_inform%C3%A1tica

- Controles de Operación
- Controles de uso de Microcomputadores

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

Objetivos:

- Garantizar que el hardware y software se adquieran siempre y cuando tengan la seguridad de que los sistemas computarizados proporcionaran mayores beneficios que cualquier otra alternativa.

- Garantizar la selección adecuada de equipos y sistemas de computación asegurar la elaboración de un plan de actividades previo a la instalación.

Acciones a seguir:

- Elaboración de un informe técnico en el que se justifique la adquisición del equipo, software y servicios de computación, incluyendo un estudio costo-beneficio.

- Formación de un comité que coordine y se responsabilice de todo el proceso de adquisición e instalación.

- Elaborar un plan de instalación de equipo y software (fechas, actividades, responsables) el mismo que debe contar con la aprobación de los proveedores del equipo.

- Elaborar un instructivo con procedimientos a seguir para la selección y adquisición de equipos, programas y servicios computacionales. Este proceso debe enmarcarse en normas y disposiciones legales.

- Efectuar las acciones necesarias para una mayor participación de proveedores.

- Asegurar respaldo de mantenimiento y asistencia técnica.

1.2 Controles de organización y Planificación: Se refiere a la definición clara de funciones, línea de autoridad y responsabilidad en labores tales como:

- Diseñar un sistema
- Elaborar los programas
- Operar el sistema
- Control de calidad

Se debe evitar que una misma persona tenga el control de toda una operación.

Es importante la utilización óptima de recursos mediante la preparación de planes a ser evaluados continuamente.

Acciones a seguir:

- La unidad informática debe estar al más alto nivel de la pirámide administrativa de manera que cumpla con sus objetivos, cuente con el apoyo necesario y la dirección efectiva.

- Las funciones de operación, programación y diseño de sistemas deben estar claramente delimitadas.

- Deben existir mecanismos necesarios a fin de asegurar que los programadores y analistas no tengan acceso a la operación del computador y los operadores a su vez no conozcan la documentación de programas y sistemas.

- Debe existir una unidad de control de calidad, tanto de datos de entrada como de los resultados del procesamiento.

- El manejo y custodia de dispositivos y archivos magnéticos deben estar expresamente definidos por escrito.

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

Acciones a seguir

- Los usuarios deben participar en el diseño e implantación de los sistemas pues aportan conocimiento y experiencia de su área y esta actividad facilita el proceso de cambio.

- El personal de auditoría interna/control debe formar parte del grupo de diseño para sugerir y solicitar la implantación de rutinas de control.

- Cada fase concluida debe ser aprobada documentadamente por los usuarios mediante actas u otros mecanismos a fin de evitar reclamos posteriores.

- Los programas antes de pasar a Producción deben ser probados con datos que agoten todas las excepciones posibles.

- Todos los sistemas deben estar debidamente documentados y actualizados. La documentación deberá contener:

  - Informe de factibilidad
  - Diagrama de lógica del programa
  - Objetivos del programa

- Listado original del programa y versiones que incluyan los cambios efectuados con antecedentes de pedido y aprobación de modificaciones:

  - Formatos de salida
  - Resultados de pruebas realizadas

- Implantar procedimientos de solicitud, aprobación y ejecución de cambios a programas, formatos de los sistemas en desarrollo.

- El sistema concluido será entregado al usuario previo entrenamiento y elaboración de los manuales de operación respectivos.

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

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

Acciones a seguir:

- Validación de datos de entrada previo procesamiento debe ser realizada en forma automática: clave, dígito auto verificador, totales de lotes, etc.

- Preparación de datos de entrada debe ser responsabilidad de usuarios y consecuentemente su corrección.

- Recepción de datos de entrada y distribución de información de salida debe obedecer a un horario elaborado en coordinación con el usuario, realizando un debido control de calidad.

  - Adoptar acciones necesarias para correcciones de errores.

  - Analizar conveniencia costo-beneficio de estandarización de formularios, fuente para agilitar la captura de datos y minimizar errores.

  - Los procesos interactivos deben garantizar una adecuada interrelación entre usuario y sistema.

  - Planificar el mantenimiento del hardware y software, tomando todas las seguridades para garantizar la integridad de la información y el buen servicio a usuarios.

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

Los controles tienen como fin:

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

Acciones a seguir:

- El acceso al centro de cómputo debe contar con las seguridades necesarias para reservar el ingreso al personal autorizado.

- Implantar claves o password para garantizar operación de consola y equipo central a personal autorizado.

- Formular políticas respecto a seguridad, privacidad y protección de las facilidades de procesamiento ante eventos como: incendio, vandalismo, robo y uso indebido, intentos de violación y como responder ante esos eventos.

- Mantener un registro permanente (bitácora) de todos los procesos realizados, dejando constancia de suspensiones o cancelaciones de procesos.

- Los operadores del equipo central deben estar entrenados para recuperar o restaurar información en caso de destrucción de archivos.

- Los backups no deben ser menores de dos y deben guardarse en lugares seguros y adecuados, preferentemente en bóvedas de bancos.

- Se deben implantar calendarios de operación a fin de establecer prioridades de proceso.

- Todas las actividades del Centro de Computo deben normarse mediante manuales, instructivos, normas, reglamentos, etc.

- El proveedor de hardware y software deberá proporcionar lo siguiente:

  - Manual de operación de equipos
  - Manual de lenguaje de programación
  - Manual de utilitarios disponibles
  - Manual de Sistemas operativos

- Las instalaciones deben contar con sistema de alarma por presencia de fuego, humo, así como extintores de incendio, conexiones eléctricas seguras, entre otras.

- Instalar equipos que protejan la información y los dispositivos en caso de variación de voltaje como:

  - reguladores de voltaje, supresores pico, UPS, generadores de energía.

  - Contratar pólizas de seguros para proteger la información, equipos, personal y todo riesgo que se produzca por casos fortuitos o mala operación.

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

Acciones a seguir:

- Adquisición de equipos de protección como supresores de pico, reguladores de voltaje y de ser posible UPS previo a la adquisición del equipo.

- Vencida la garantía de mantenimiento del proveedor se debe contratar mantenimiento preventivo y correctivo.

- Establecer procedimientos para obtención de backups de paquetes y de archivos de datos.

- Revisión periódica y sorpresiva del contenido del disco para verificar la instalación de aplicaciones no relacionadas a la gestión de la empresa.

- Mantener programas y procedimientos de detección e inmunización de virus en copias no autorizadas o datos procesados en otros equipos.

- Propender a la estandarización del Sistema Operativo, software utilizado como procesadores de palabras, hojas electrónicas, manejadores de base de datos y mantener actualizadas las versiones y la capacitación sobre modificaciones incluidas.

- Analizados los distintos tipos de controles que se aplican en la Auditoría de Sistemas efectuaremos a continuación el análisis de casos de situaciones hipotéticas planteadas como problemáticas en distintas empresas, con la finalidad de efectuar el análisis del caso e identificar las acciones que se deberían implementar.

2. Auditoría Informática de Desarrollo de Proyectos o Aplicaciones

Revisión del proceso completo de aplicaciones que utiliza la empresa auditada.
El análisis se basa en cuatro aspectos fundamentales.

2.1 Revisión de las metodologías utilizadas: Se analizaran éstas, de modo que se asegure la modularidad de las posibles futuras ampliaciones de la Aplicación y el fácil mantenimiento de las mismas.

2.2 Control Interno de las Aplicaciones: Se deberán revisar las mismas fases que presuntamente han debido seguir el área correspondiente de Desarrollo:

- Estudio de Vialidad de la Aplicación.
- Definición Lógica de la Aplicación.
- Desarrollo Técnico de la Aplicación.
- Diseño de Programas.
- Métodos de Pruebas.
- Documentación.
- Equipo de Programación
- Satisfacción de usuarios

Una Aplicación técnicamente eficiente y bien desarrollada, deberá considerarse fracasada sino sirve a los intereses del usuario que la solicitó. La aquí esencia del usuario proporciona grandes ventajas posteriores, ya que evitará reprogramaciones y disminuirá el mantenimiento de la Aplicación.

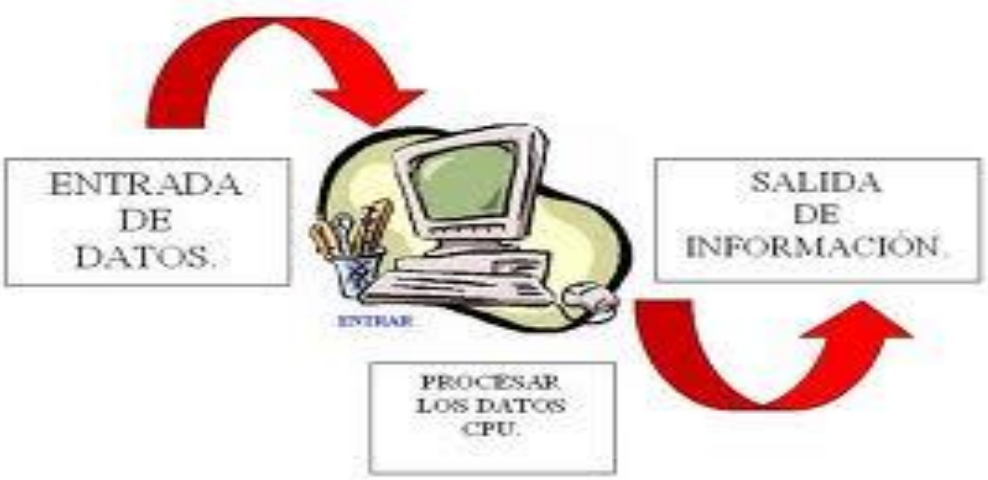
2.3 Control de Procesos y Ejecuciones de Programas Críticos: Se ha de comprobar la correspondencia biunívoca y exclusiva entre el programa codificado y su compilación. Si los programas fuente y los programa módulo no coincidieran podría provocar graves y altos costos de mantenimiento, hasta fraudes, pasando por acciones de sabotaje, espionaje industrial informativo, etc.

3. TÉCNICAS

3.1 AUDITORIA AL REDEDOR DEL COMPUTADOR

En este enfoque de auditoría, los programas y los archivos de datos no se auditan.

La auditoría alrededor del computador concentra sus esfuerzos en la entrada de datos y en la salida de información. Es el más cómodo para los auditores de sistemas, por cuanto únicamente se verifica la efectividad del sistema de control interno en el ambiente externo de la máquina. Naturalmente que se examinan los controles desde el origen de los datos para protegerlos de cualquier tipo de riesgo que atente contra la integridad, completitud, exactitud y legalidad.



3.1.1 DATOS DE PRUEBA

La auditoría alrededor del computador no es tan simple como aparentemente puede presentarse, pues tiene objetivos muy importantes como:

- Verificar la existencia de una adecuada segregación funcional.

- Comprobar la eficiencia de los controles sobre seguridades físicas y lógicas de los datos.

- Asegurarse de la existencia de controles dirigidos a que todos los datos enviados a proceso estén autorizados.

- Comprobar la existencia de controles para asegurar que todos los datos enviados sean procesados.

- Cerciorarse que los procesos se hacen con exactitud.

- Comprobar que los datos sean sometidos a validación antes de ordenar su proceso.

- Verificar la validez del procedimiento utilizado para corregir inconsistencias y la posterior realimentación de los datos corregidos al proceso.

- Examinar los controles de salida de la información para asegurar que se eviten los riesgos entre sistemas y el usuario.

- Verificar la satisfacción del usuario. En materia de los informes recibidos.

- Comprobar la existencia y efectividad de un plan de contingencias, para asegurar la continuidad de los procesos y la recuperación de los datos en caso de desastres.

Se puede apreciar la ambición de los objetivos planteados, pues solamente faltarían objetivos relacionados con el examen de los archivos y los programas, lo cual es parte de otro enfoque.

3.1.2 Informe de esta Auditoría: deberá redactarse en forma sencilla y ordenada, haciendo énfasis en los riesgos más significativos e indicando el camino a seguir mediante recomendaciones económicas y operativamente posibles.

Pasos que se deben seguir en la auditoría:

- Metodología de la auditoría.
- Objetivos de la auditoría.
- Evaluación del sistema de control interno.
- Procedimientos de auditoría.

- Papeles de trabajo.
- Deficiencias de control interno.
- Informe de auditoría.

3.2 Técnicas para la Auditoría Informática

3.2.1 Cuestionarios: Listado de preguntas a las que el entrevistado puede responder oralmente o por escrito, su finalidad es evidenciar determinados aspectos. Estos cuestionarios no pueden utilizarse en distintas áreas, deben ser específicos para cada situación.

Los informes finales de los auditores dependen de sus capacidades para analizar las situaciones de debilidad o fortaleza de los diferentes entornos. El trabajo de campo del auditor consiste en lograr toda la información necesaria para la emisión de un juicio global objetivo, siempre amparado en hechos demostrables, llamados también evidencias.

3.2.2 Entrevistas: En ellas se obtiene información, y mejor matizada, que la proporcionada por medios propios puramente técnicos o por las respuestas escritas a cuestionarios. El auditor informático experto entrevista al auditado siguiendo un cuidadoso sistema previamente establecido, consistente en que bajo la forma de una conversación correcta y lo menos tensa posible, el auditado conteste sencillamente una serie de preguntas variadas, también sencillas.

3.2.3 Trazas y/o Huellas: El auditor informático debe verificar que los programas, realicen exactamente las funciones previstas, y no otras. Para ello se apoya en productos Software muy potentes y modulares que, entre otras funciones, rastrean los caminos que siguen los datos a través del programa. Las trazas se utilizan para comprobar la ejecución de las validaciones de datos previstas. Las mencionadas trazas no deben modificar en absoluto el Sistema.

3.3 TÉCNICAS DE AUDITORIA ASISTIDAS POR COMPUTADOR TAAC

Incluyen distintos tipos de herramientas y de técnicas se pueden utilizar varios procedimientos de auditoría que incluyan pruebas de los detalles de las operaciones, saldos, procedimientos de revisión analíticos pruebas de cumplimiento de los controles generales de sistemas de información y pruebas de cumplimiento de los controles de aplicación.

"Programas de computador y datos que el auditor usa como parte de sus procedimientos de auditoría para procesar datos de significancia"[2]

3.4 Técnicas para evaluar los controles de aplicaciones de producción

Utilizadas para verificar la exactitud en cálculos de aplicaciones complejas en forma global.

3.4.1 Método de datos de prueba: Consiste en la elaboración de una matriz de riesgos materiales de una o varias transacciones que son realizadas por la aplicación en evaluación.

3.4.2 Facilidad de prueba integrada (ITF): Similar a la de datos de prueba, con la diferencia de que en esta se trabajan con datos reales y ficticios. Es una técnica para probar los sistemas de aplicación en producción con datos reales evaluándolo en un ambiente normal de producción. Se procesan las transacciones de prueba de una entidad ficticia junto con las transacciones reales de producción, por tal razón se llama prueba integrada.

Ventajas:

- Se requiere poco entrenamiento técnico.
- Costo de procedimiento bajo debido a que los datos de prueba se procesan junto con los datos de entrada normales.
- Posibilidad el sistema real, tal como opera normalmente.

Desventajas:

- Alto costo si los programas deben modificarse para eliminar los efectos de los datos de prueba.
- Posibilidad de destruir archivos.

Aplicación de la Técnica:

- Establece registros falsos en los archivos reales.
- Establecer el método para eliminar los efectos de los datos de prueba.
- Calcula los resultados previsto para el procesamiento.
- Compara los resultados previstos contra reales.

[2] http://www.virtual.unal.edu.co/cursos/sedes/manizales/4060035/und_5/html/taacs.html

3.4.3 Simulación paralela: Esta es una técnica en la que el auditor elabora, a través de lenguajes de programación o programas utilitarios avanzados, una aplicación similar a la que va a ser auditada.

3.5 Técnicas para análisis de transacciones

Consiste en la selección y análisis de transacciones materiales de forma permanente, utilizando procedimientos analíticos y técnicas de muestreos.

3.5.1 Método de Archivo de Revisión SCARF

Consiste en incorporar aplicaciones de auditoría en el sistema de producción para que ejecute distintos tipos de supervisiones y control permanentemente.

La aplicación de este software se la conoce como subrutina que supervisa la selección de datos mediante muestreos previamente definidos por el auditor. Las actividades de control, muestreo y reportes de excepción son controladas por parámetros, el diseño e implementación de tales módulos son altamente dependientes de la aplicación y son generalmente ejecutados como una parte integral del proceso de desarrollo de aplicación.

Ventaja:

- Proveer muestras estadísticas de producción incluyendo la entrada y las transacciones generadas internamente.

Desventaja:

- Su alto costo de desarrollo y mantenimiento y las dificultades asociadas con la independencia del auditor.

Implantación de la Técnica SCARF.

- Los requerimientos del auditor se implantan en los programas de aplicación junto con el resto del desarrollo de la aplicación.
- Una vez que se ha implementado el nuevo sistema de las excepciones a estas pruebas se registran en un archivo.

- El auditor sigue acción que considera apropiada basado en las excepciones que descubre.[3]

3.5.2 Registros extendidos: "Técnica muy particular y útil para los auditores que han desarrollado ciertas destrezas en el análisis de datos y en la conservación histórica de todos los cambios que haya sufrido una transacción en particular".[4]

3.6 Técnicas administrativas

A través de ellas el auditor establece el alcance de la auditoria, define las áreas de interés y la metodología a seguir para la ejecución de la investigación.

3.6.1 Selección de muestras: Mediante esta técnica, el auditor establecer las aplicaciones críticas o módulos específicos dentro de dichas aplicaciones que necesitan ser revisadas periódicamente, que permitan obtener información relevante respecto a las operaciones normales del negocio.

3.6.2 Modelaje: la única diferencia con la selección de muestra es en los objetivos y criterios de selección de las áreas de interés.

3.6.3 Sistema de puntajes: A través de esta técnica el auditor analiza los riesgos inherentes de las aplicaciones y que están directamente relacionados con la naturaleza del negocio asignándole a cada riesgo un puntaje de ocurrencia para las aplicaciones críticas de la organización.

3.6.4 Software de auditoria multisitio: aplica a una organización con varias sucursales u oficinas remotas tomando como base el concepto de los sistemas distribuidos. El software de seguridad permite restringir el acceso al microcomputador, de tal modo que solo el personal autorizado pueda utilizarlo.

Adicionalmente, este software permite reforzar la segregación de funciones y la confidencialidad de la información mediante controles para que los usuarios puedan acceder solo a los programas y datos para los que están autorizados.

3.7. Centro de competencia: Un centro de competencia (CdeC) es un equipo especializado en un área de conocimiento concreta, estratégica y que tiene una aplicación transversal y crítica.

[3] http://www.dspace.espol.edu.ec/bitstream/123456789/4043/1/6571.pdf

[4] http://auditoriadesistemasi.blogspot.com/2012/06/tecnicas-de-auditoria-asistidas-por.html

- Estrategia: acumular conocimiento, comunicar buenas prácticas, formar/divulgar, redactar y consensuar normativas, etc.

- Ayuda a proyectos: aportar conocimiento, asegurar la coherencia de los proyectos con la normativa establecida, etc.

- Centro de competencia de seguridad: es responsable de promover normativas y acciones con el fin de minimizar los riesgos tanto internos como externos.

- Centro de competencia de innovación: es responsable de hacer una prospección constante con el fin de asegurar la incorporación de las últimas tecnologías al servicio del aprendizaje virtual.

3.8. Análisis Matricial de Riesgo: La Tecnología de Información (TI) se ha convertido en el corazón de las operaciones de cualquier organización, desde los sistemas transaccionales hasta las aplicaciones enfocadas a la alta gerencia que ayudan tanto a las operaciones transaccionales diarias como a definir el rumbo que tiene que seguir una organización. Una de las situaciones que se está presentando con mayor relevancia en las organizaciones, es el outsourcing de procesos que están en la cadena de valor de una organización pero que los directivos deciden colocarla a cargo de un tercero, esta es una situación que se documenta en el presente trabajo. Por otro lado las operaciones de una organización tienen que seguir ciertos estándares y lineamientos y a su vez esto puede provocar cambios en la manera de realizar las cosas, todos estos criterios se detallan en este documento.

Importancia de Tecnología de Información

En este mundo globalizado y de constantes cambios, las empresas obligadamente requieren ser cada vez más ágiles y se deben adaptar con mayor facilidad a estos cambios.

Actualmente, las organizaciones dependen en su totalidad de tener la información exacta en el momento preciso, las compañías que no son capaces de alcanzar esto, están en peligro de extinción porque con el paso de los años, la información se ha convertido en el arma más potente para la toma decisiones, y es aquí donde radica la prioridad de desarrollar nuevas tecnologías que permitan tener la información requerida y lista para ser utilizada. Sin embargo, la mayoría de las organizaciones han fallado al no aprovechar el ambiente existente e implementar

ideas innovadoras para mejorar el papel que juegan los sistemas de información dentro de sus organizaciones, algunos de estos errores son:

- **Riesgo según Fernando Izquierdo Duarte:** "El Riesgo es un incidente o situación, que ocurre en un sitio concreto durante un intervalo de tiempo determinado, con consecuencias positivas o negativas que podrían afectar el cumplimiento de los objetivos".

- **Riesgos de Tecnología de Información:** El concepto de riesgo de TI puede definirse como el efecto de una causa multiplicado por la frecuencia probable de ocurrencia dentro del entorno de TI. Surge así, entonces la necesidad del control que actúe sobre la causa del riesgo para minimizar sus efectos. Cuando se dice que los controles minimizan los riesgos, lo que en verdad hacen es actuar sobre las causas de los riesgos, para minimizar sus efectos.

Objetivo General del Análisis de Riesgo

Su objetivo es establecer una valoración y priorización de los riesgos con base en la información ofrecida por los mapas elaborados en la etapa de identificación, con el fin de clasificar los riesgos y proveer información para establecer el nivel de riesgo y las acciones que se van a implementar.

3.8.1 Determinación del Nivel del Riesgo: La determinación del nivel de riesgo es el resultado de confrontar el impacto y la probabilidad con los controles existentes al interior de los diferentes procesos y procedimientos que se realizan. Para adelantar esta etapa se deben tener muy claros los puntos de control existentes en los diferentes procesos, los cuales permiten obtener información para efectos de tomar decisiones, estos niveles de riesgo pueden ser: Alto, Medio y Bajo.

3.8.2 Matriz de Riesgos: Utilidad del Método Matricial para el análisis de Riesgos: Este método utiliza una matriz para mostrar gráficamente tanto las amenazas a que están expuestos los sistemas computarizados como los objetos que comprenden el sistema. Dentro de cada celda se muestran los controles que atacan a las amenazas.

3.8.3 Administración de Riesgos: Es un proceso interactivo e iterativo basado en el conocimiento, evaluación y manejo de los riesgos y sus impactos, con el propósito de mejorar la toma de decisiones organizacionales. Es aplicable a

cualquier situación donde un resultado no deseado o inesperado pueda ser significativo o donde se identifiquen oportunidades de mejora.

3.8.4 Administración de Riesgos de TI: Es el proceso continuo basado en el conocimiento, evaluación, manejo de los riesgos y sus impactos que mejora la toma de decisiones organizacionales, frente a los riesgos de TI.

3.8.4.1 Metodología: Según el Diccionario, Método es el "modo de decir o hacer con orden una cosa". Asimismo define el diccionario la palabra Metodología como "conjunto de métodos que se siguen en una investigación científica". Esto significa que cualquier proceso cinético debe estar sujeto a una disciplina de proceso defina con anterioridad que llamaremos Metodología.

Una vez revisadas las definiciones conceptuales, iniciaremos el desarrollo del proceso de administración de riesgo.

Proceso de Administración de Riesgos de TI:

A continuación se describen las principales etapas definidas para el Proceso de Administración de Riesgos de TI.

- Establecimiento de la Metodología de TI
- Identificación de Riesgos de TI
- Análisis del Riesgo de TI
- Evaluación y Priorización de Riesgos de TI
- Tratamiento de Riesgos de TI (Controles Definitivos)
- Monitoreo y Revisión

3.8.4.2 Establecer Metodología: Luego de una evaluación de las diferentes metodologías que existen para analizar y administrar el Riesgo de Tecnología de Información, la decisión se inclinó por considerar la del criterio de los expertos, que es la metodología Delphi, que consiste en reunir un grupo de personas que conozcan del negocio y tengan noción mínima de los riesgos.

La directiva de la empresa se inclinó por esta metodología ya que consideraron que para poder establecer soluciones en la empresa era imprescindible que se considere la opinión de las personas que colaboran en la organización, en este caso, los expertos del departamento de Sistemas, que son cuatro personas conjuntamente con el jefe del departamento de sistemas, las que participan en el desarrollo de la metodología.

3.8.4.3 Identificar Riesgos de TI: Una vez definidos los objetivos y el alcance del trabajo a realizar, se desarrollaron criterios de evaluación de riesgos de TI, que es el aspecto en el que se va a centrar esta evaluación, para el Área de Informática. Para la identificación de los riesgos, se entrevistó a cada uno de los expertos, donde analizando los problemas que afectan al departamento, se estableció la Matriz de Ponderaciones y se determinaron los riesgos más relevantes.

3.8.4.4 Análisis del Riesgo de TI

- **Valorar el Riesgo Inherente:** Para la valoración de los riesgos que se analizan, se definió una escala de valoración Cualitativa, que es la asignación de las características Alto, Medio y Bajo a los diferentes riesgos encontrados.

- **Determinar Controles Existentes:** El Departamento tiene ciertos controles, pero carece de otros controles que son necesarios ya sea para prevenir, detectar o corregir la materialización de los Riesgos.

- **Identificar Nivel de Exposición:** Cabe recalcar que el Nivel de Exposición es igual a decir Riesgo Inherente menos Controles. Teniendo en cuenta esta definición, se puede decir que la empresa tiene un nivel de exposición medio-alto, ya que no tiene los suficientes controles necesarios para restarle a los riesgos inherentes.

3.8.5 Evaluación y Priorización de los Riesgos: Método Matricial para el Análisis de Riesgos: Este método utiliza una matriz que muestra gráficamente tanto las amenazas a que están expuestos los sistemas computarizados y la información del departamento, como los objetos que comprenden el departamento de Sistemas. Se describe a continuación los pasos para el desarrollo del método:

- **Crear la matriz de amenazas y de objetos:** Luego de ponderar los riesgos existentes dentro del Departamento, trabajo realizado por el grupo de experto, se determinaron los que compondrán la Matriz de Control de Riesgos (Amenazas y Objetos).

- **Categorización de Riesgos:** Se categorizan las amenazas por niveles de riesgo, de mayor a menor en orden de importancia, como haya sido determinado por el grupo Delphi. Luego los cinco expertos proceden a votar. La votación se realiza de manera vertical y horizontal. Después se

suman los votos derechos de las columnas y los votos izquierdos de las filas; y para la cifra total se suman los resultados antes obtenidos. Paso a seguir, se procede a categorizar la sensibilidad de los objetos. Proceso que se inicia pasando los objetos que registra la matriz de control de riesgos en una hoja de comparación de categorías de riesgos. Para categorizar la sensibilidad de los objetos se utiliza como criterio la percepción que tenga cada uno de los miembros del equipo Delphi sobre objetos que puedan causar mayor pérdida económica si se daña o causa demoras en el procesamiento. A seguir, se procede a la votación del grupo de igual manera como se realizó con la categorización de las amenazas. De igual manera se procede a sumar de la misma manera que se realizó con las amenazas. Con la categorización tanto de las amenazas como los objetos, se realiza la combinación de las dos categorías, elaborando una matriz de combinaciones, colocando los totales en orden de mayor a menor (de izquierda a derecha y de arriba abajo), en los dos casos.

Después se procede a realizar los cálculos correspondientes, multiplicando los valores de las amenazas con los de los objetos para así poder obtener el nivel de riesgo / sensibilidad de las celdas de acuerdo con el valor del producto. Puede que al terminar este proceso se presenten repeticiones, las cuales no son consideradas para determinar el nivel de riesgos de las celdas. Luego dividimos las celdas en regiones de mayor, menor y mediano riesgo. Como en este caso no existen repeticiones en los productos, se consideran las 36 celdas para la determinación del nivel de riesgo. Se procede a dividir las 36 celdas para el número de expertos (36 / 5 = 7,2 = 7). La escala de valoración es Semicuantitativa ya que se asignan rangos numéricos a las características Alto, Medio y Bajo. Se toman las siete celdas con los productos más altos para determinarlas con un nivel de riesgo alto, las siete celdas con los productos más bajos para determinarlas con un nivel de riesgo bajo; y las veinte y dos celdas restantes se las determina con un nivel de riesgo medio.

3.8.5.1 Diseñar los controles definitivos: Finalmente, con el resultado del trabajo realizado, apoyados en el Método Delphi y en el modelo matricial Riesgo / Sensibilidad, se diseñan y documentan definitivamente los controles a nivel: preventivo, detectivo y correctivo; de acuerdo al área informática del Departamento de Sistemas.

3.8.5.2 Presentar los Resultados: La Gerencia de la empresa debe de conocer el resultado del análisis de riesgo de manera oportuna, el cual será presentado en

un informe detallado. De esta manera la Gerencia podrá tomar las acciones necesarias para su implantación.

4. Herramientas de Auditoría de Aplicaciones

4.1 Simuladores: Esta herramienta es una de las más utilizadas para el análisis y diseño de sistemas, pero también puede ser de mucha utilidad para la auditoría de sistemas computacionales, ya que mediante el uso de un modelo, conceptual o físico, se simula el comportamiento de un sistema computacional, de un programa, de una base de datos, de una operación, de una actividad o de cualquier tarea de sistemas que tenga que ser revisada, con el propósito de investigar cuál es, fue o será el comportamiento del fenómeno de sistemas en estudio, bajo ciertas condiciones y características concretas, en las que se presentan todas las simulaciones necesarias que se asemejen al medio ambiente real en donde actúa dicho fenómeno para valorar su auténtico aprovechamiento, sus eficiencias y deficiencias de funcionamiento, sus principales problemas, etcétera.

El uso de esta técnica de simulación es indispensable para el trabajo de los desarrolladores de nuevos sistemas, ya que permite elaborar un ambiente análogo al del nuevo sistema, con el fin de estudiar su posible comportamiento. Una vez estudiado el posible comportamiento del sistema, se pueden sacar conclusiones para corregir sus fallas de funcionamiento, así como sus principales problemas antes de implantar dicho sistema. De hecho, todos los analistas de sistemas utilizan modelos conceptuales antes de programar (codificar) un sistema computacional, mientras que los programadores elaboran su programación con base en estos modelos.

En el caso concreto de auditoría de sistemas computacionales, la simulación es la elaboración de modelos, conceptuales o físicos, muy similares a los sistemas institucionales de las empresas; inclusive pueden ser los mismos que éstas utilizan actualmente.

Muchos se prueban con bases de datos ficticias o con datos reales pero sin validez. El auditor hace pruebas en esos modelos de simulación, para verificar el comportamiento y funcionamiento de los sistemas computacionales, la forma en que se realiza el procesamiento de datos, la emisión de informes, la captura de datos o cualquier otro aspecto de dichos sistemas.

Esta simulación se puede hacer para evaluar cualquier fenómeno de sistemas computacionales, lo mismo para el análisis, diseño y programación de sistemas,

para la instalación y liberación de un nuevo sistema, o para evaluar el comportamiento de las bases de datos, el comportamiento del hardware, el mobiliario y equipo, el diseño e instalación de una red de cómputo o cualquier otro aspecto de sistemas.

A continuación se presentan algunas definiciones de esta herramienta, con el fin de entender mejor su utilidad:

- Simular**:** “Del latín simular, de similis: Semejante. Aparentar, fingir.”

- Simulacro: “Imagen hecha a semejanza de una cosa [...] Cosa que forma la fantasía. Ficción, imitación, falsificación.”

- Modelo: “Lo que se sigue, imita o reproduce [...] Representación en pequeño de una cosa.

4.1.1 Simulación: La imitación formal del sistema computacional, mediante un modelo simulado, en cuanto al funcionamiento del hardware, software, información, instalaciones o aplicaciones, en la cual se representan sus principales características de operación, forma de captura, procesamiento de datos y emisión de resultados del sistema original, con el propósito de estudiar el comportamiento del sistema y evaluar su funcionamiento real. En estos modelos se pueden aplicar datos ficticios o datos reales, pero sin que esta simulación llegue a influir en la actividad normal del sistema original.

El uso de modelos para la simulación es una de las principales formas de evaluación del funcionamiento de un sistema computacional, ya que permiten aplicar pruebas de su comportamiento, sin afectar su operación normal. Lo mismo sucede cuando se aplican para simular la operación de los sistemas computacionales, el acceso, manejo y protección de las bases de datos, el uso del software, hardware, datos, equipos e instalaciones, alguna contingencia de sistemas o cualquier otro tipo de pruebas que permitan imitar el funcionamiento del sistema original, con el propósito de compararlo con el sistema simulado.

Con dichas comparaciones se pueden sacar conclusiones importantes, sin afectar la operación normal de los sistemas de la empresa; además, estas simulaciones también ayudan a vislumbrar las posibles problemáticas del sistema computacional, si afectar el funcionamiento del mismo. Con el uso de modelos concretos o de pruebas de simulación también se pueden evaluar la integridad, seguridad y confiabilidad de la información contenida en las bases de datos originales, así como verificar la existencia de redundancias, alteraciones y

comportamientos irregulares de la información contenida en esas bases de datos; además, también se puede simular, por medio de modificaciones controladas en el prototipo del sistema original, el acceso al sistema, la protección del mismo, el ingreso a las bases de datos, e incluso el comportamiento de los usuarios del sistema o el manejo de los datos. En algunos casos, cuando el sistema lo permite y con ello no se alteran sus datos originales, se pueden hacer todo tipo de pruebas de evaluación, ya sean con datos ficticios o con datos reales del sistema.

Si las pruebas de simulación lo requieren, se pueden hacer alteraciones controladas del funcionamiento normal del sistema, para medir el comportamiento y conducta de los datos, la operación o cualquier otro aspecto del sistema que se quiera evaluar.

Debemos señalar que el auditor responsable de la auditoría debe supervisar estrictamente la aplicación de esta herramienta, e incluso debe tomar las medidas preventivas, de seguridad y de control necesarias para salvaguardar la información antes de aplicar cualquier prueba o simulacro al sistema, con el propósito de contar con un respaldo del sistema original, por si su funcionamiento se llegara a alterar debido a las pruebas que se le realicen. La importancia de la simulación radica en que se pueden confeccionar pruebas controladas o libres que permiten realizar una buena evaluación al sistema, sin necesidad de alterar el funcionamiento del sistema original. En este tipo de observación se pueden hacer las pruebas en sistemas paralelos; uno es el propio sistema con datos reales o ficticios y el otro es un modelo semejante al sistema que será evaluado. Estas pruebas en sistemas paralelos se realizan con el propósito de comparar ambos resultados y, si es necesario, modificar la conducta del modelo para cotejarlo con el sistema original. Con los resultados se puede obtener información muy valiosa para emitir conclusiones sobre el comportamiento de ambos.

4.1.2 Simulación a través de modelos de metodología de sistemas: Debido a que existen muchos modelos de simulación para evaluar el comportamiento de un sistema, únicamente citaremos algunos; el propósito es ejemplificar las posibles aplicaciones de los modelos que se pueden utilizar como apoyo en la evaluación de sistemas. Asimismo, solamente presentaremos las principales etapas y fases de estas metodologías, sin entrar en mayores detalles, ya que cada desarrollo de sistemas es especial y sería irrelevante señalar ejemplos específicos para cada caso.

- **Ciclo de vida de los sistemas:** Este modelo, también conocido como el ciclo de vida tradicional de los sistemas, es el que más se utiliza para el desarrollo de sistemas computacionales, ya que es considerado como la metodología fundamental y puede contener variaciones menores dentro de las fases que citaremos a continuación, siempre y cuando se conserven dentro del esquema que presentaremos:

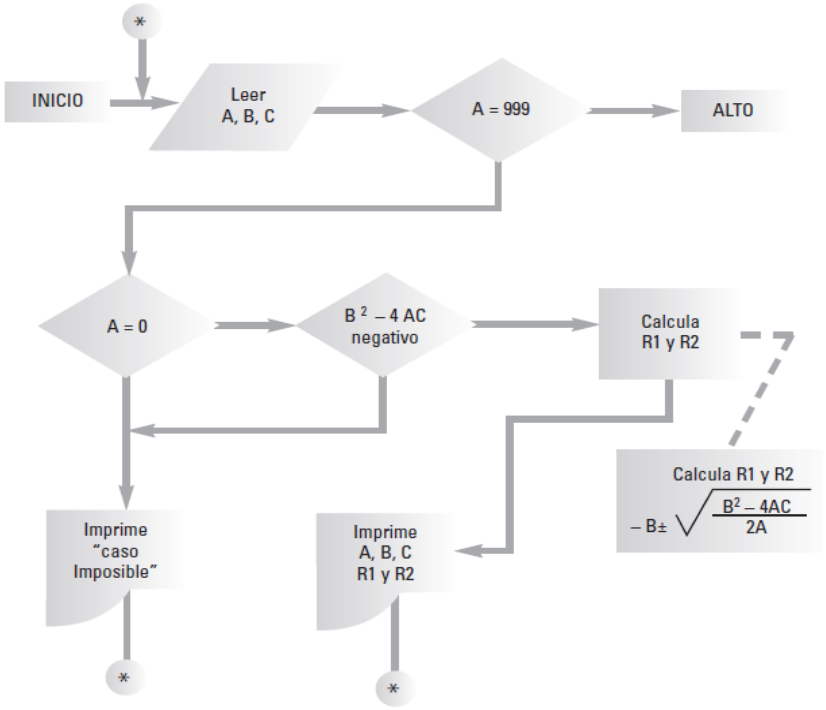
  - Análisis del sistema actual
  - Diseño conceptual del sistema
  - Diseño detallado del sistema
  - Programación
  - Pruebas y correcciones
  - Implantación del sistema
  - Liberación del sistema
  - Mantenimiento del sistema

- **Metodología de Kendall & Kendall:** Los desarrolladores de sistemas computacionales tienen que utilizar forzosamente la metodología de estos autores, considerada como clásica para el análisis y diseño de los sistemas computacionales, ya que se aplica fácilmente y es muy completa. Los propios autores presentan las siete fases del desarrollo de sistemas, las cuales presentamos a continuación:

  - Identificación de problemas, oportunidades y objetivos
  - Determinación de requerimientos de información
  - Análisis de las necesidades del sistema
  - Diseño del sistema recomendado
  - Desarrollo del sistema
  - Pruebas y mantenimiento de sistemas
  - Implementación y evaluación del sistema

4.1.3 Simulación a través de diagramas de flujo de sistemas: En este tipo de simulaciones se utilizan diagramas con símbolos universalmente aceptados, los cuales tienen un significado específico y determinado previamente por convención, a fin de que todos los entiendan de la misma forma.

A continuación mostraremos un ejemplo de este tipo de modelos, el cual es un diagrama de flujo para programación BASIC; debemos señalar que en este capítulo también trataremos la diagramación, ya que es una de las técnicas especiales de auditoría de sistemas computacionales:



4.1.4 Simulación a través de otros documentos gráficos: Es evidente que se puede utilizar un sinnúmero de modelos gráficos, conceptuales o físicos para simular el comportamiento de un sistema computacional; incluso los planes, diagramas de planeación y control de proyectos, así como otros documentos de apoyo para la gestión administrativa se pueden tomar como ejemplos de modelos de simulación utilizables en una auditoría de sistemas computacionales; por esta razón, a continuación mencionaremos únicamente algunos de los posible modelos de sistema que se pueden utilizar para simular el comportamiento de cualquier fenómeno de sistemas computacionales que se desee evaluar:

- Modelos para planeación y control de proyectos
  - Gráfica de Gantt
  - Método de la ruta crítica
  - PERT costo/tiempo
  - Project
  - Gráficas de proyecciones financieras
  - Gráficas de líneas de tiempo
  - Tablas de decisiones
  - Árboles decisionales

- Modelos de simulación de diagramas administrativos

  - Organigramas
  - Diagramas de métodos y procedimientos
  - Gráficas de tiempos y movimientos
  - Estudios ergonómicos
  - Planos de distribución de la planta
  - Planos de instalaciones
  - Planos de rutas de evacuación
  - Planos de configuración de centros de cómputo

- Modelos de simulación por medio de gráficas financieras y estadísticas

  - Curvas de tendencias
  - Gráficas de Pie, horizontales, verticales, de área, circulares y semicirculares
  - Gráficas de punto de equilibrio

- Otros modelos de simulación

  - Gráficas de pantalla
  - Planes de contingencia informática
  - Digitalización de imágenes
  - Procesamiento de datos ficticios

Evidentemente existen muchos más modelos que se pueden utilizar para simular el comportamiento de los sistemas en evaluación, pero la intención es destacar la importancia de utilizar los modelos de simulación en una auditoria de sistemas computacionales.

CONCLUSIONES

- Con la realización de una Auditoria de Aplicación se pueden implementar mejoras en los funcionamientos operativos de las entidades, así como garantizar la seguridad en la información que se genera gracias a una evaluación del recorrido que lleva la información para que pueda ser expresada en resultados. Para lograrlo se deben tener sistematizadas las operaciones; donde la intervención de las personas sea mínimo y así garantizar confianza en el proceso de datos.

- Las aplicaciones pueden resultar una solución informática para la automatización de ciertas tareas complicadas como los procesadores de textos, hojas de cálculo, y base de datos, la diferencia entre los programas de aplicación y los de sistema está en que los de sistema suponen ayuda al usuario para relacionarse con el computador y hacer un uso más cómo del mismo, mientras los de aplicación son programas que cooperan con el usuario para la realización de las actividades.

- La auditoría en sistemas debe evaluar los documentos y registros usados en la elaboración de las aplicaciones, así como todas las salidas y reportes, la descripción de las actividades de flujo de la información y de procedimientos, los archivos almacenados, su uso y su relación con otros archivos, sistemas y aplicaciones; asimismo, la revisión y la evaluación de los controles, los equipos de cómputo, su utilización, eficiencia y seguridad, a fin de que se logre obtener información eficiente y segura que servirá para una adecuada toma de decisiones.

- La realización de este trabajo nos fue de mucha satisfacción como Contadores Públicos y Auditores debemos especializar nuestros conocimientos en el campo de la informática, ya que en la actualidad la informática es el corazón de las empresas.

BIBLIOGRAFÍA:

1. Echenique G. J.A. (2001). Auditoría en Informática. 2da. Ed. Mc Graw-Hill
2. http://es.wikipedia.org/wiki/Aplicaci%C3%B3n_inform%C3%A1tic
3. http://www.virtual.unal.edu.co/cursos/sedes/manizales/4060035/und_5/html/taacs.htm
4. http://www.dspace.espol.edu.ec/bitstream/123456789/4043/1/6571.pdf
5. http://auditoriadesistemasi.blogspot.com/2012/06/tecnicas-de-auditoria-asistidas-por.html
6. http://www.monografias.com
7. http://www.es.wikipedia.org/
8. Piattinni, G. M & Peso del E. Auditoría Informática. Un enfoque práctico. Alfaomega