LA AUDITORÍA INFORMÁTICA: CONCEPTOS Y METODOLOGÍA OPERATIVA

Dr. Julio Vicente Flores Konja*

RESUMEN

La Auditoría Informática es una disciplina de suma importancia que necesita el Contador Público para realizar sus trabajos de auditoría integral: auditorías financieras, auditorías de cumplimiento o auditorías de gestión. El presente artículo nos presenta un modelo llamado Reto EDI y una serie de propuestas y procedimientos que despiertan a la inquietud del tema.

Asimismo, se incluyen novedosos indicadores de apoyo a la realización de la auditoría en general y de la auditoría informática en forma específica.

SITUACIÓN ACTUAL DE LA INFORMÁTICA

Las últimas cuatro décadas se han caracterizado por una carrera vertiginosa en el campo de la informática donde la reducción del costo y el tamaño contrapuesto al aumento de la capacidad de las computadoras han sido los aspectos más significativos.

La probabilidad de que los sistemas de control interno estén autorizados es cada día mayor; de igual modo el software se torna más accesible a los usuarios finales.

Se precisa menos conocimientos de computación para servirse de los resultados de la información, sin embargo se alejan y se dificultan los procesos de revisión y, por tanto, aumenta la vulnerabilidad de los sistemas.

Esto se aprecia por el hecho de que la tendencia es que las herramientas, con las que más rápidamente se logran resultados (Windows 98, Access, Excel, etc.) son las que menos facilidades brindan para garantizar seguridad y control de acceso ya que estas opciones requieren de una administración especializada que un profesional que no domine la informática no puede brindar.

AUDITORÍA INFORMÁTICA: NECESIDAD

En la actualidad resulta casi imposible separar el vocablo sistema en cualquiera de sus manifestaciones del término automatizado y por ende de la palabra informático; podemos pensar en cualquier uso con enfoque sistemático y es difícil que no haya sido automatizado completamente o de forma parcial, o esté en vías de serlo. Lo mismo será relacionado en el género humano en lo que a salud se refiere, al animal o al vegetal, resultando difícil encontrar al menos una función que sea componente de un sistema que no conlleve alguna relación con la computación.

* Profesor Principal y Decano de la Facultad de Ciencias Contables

Es completamente necesario en cualquiera de las variantes de auditoría que deseemos realizar el enfrentamiento a la revisión de control interno de la empresa.

Es de la misma característica si la actividad que desarrolla la organización es de Producción o de Servicios, Comercializadora ya sea mayorista o al detalle o de cualquier otro tipo.

Por lo que inevitablemente tenemos que enfrentarnos en algún punto del proceso a diferentes grados de automatización; es en estos puntos que se hace necesaria la utilización de las técnicas de auditoría informática en cualquiera de sus variantes.

Esta novedosa disciplina se va haciendo cada vez más imprescindible, ya casi no se concibe un sistema contable que no esté automatizado.

Si no queremos pasar como sujetos pasivos que se limitan a pedir información tendremos que hacer uso de la auditoría informática o cuando menos acompañar a los auditores económicos de auditores informáticos, debido a que se podría pasar por alto violaciones internas del funcionamiento del sistema, que si deseamos comprobar debemos utilizar algunas de las siguientes opciones:

Establecer una muestra que alcance un por ciento que asegura la confiabilidad.

Utilizar mecanismos de chequeo automatizado a las operaciones que se realizan.

Muchas firmas de auditores muestran su preocupación por el futuro de los sistemas de control interno y las formas en que se piensa abordar esta tecnología.

Un criterio al respecto nos brinda Alfredo Sneyers, Presidente de EDIFICAS–EUROPE, en representación del Instituto de Auditores-Censores Jurados de Cuentas de España.

En los mercados competitivos actuales las empresas y otras organizaciones necesitan reducir sus costos administrativos, reducir el volumen de errores, controlar su período de cobros, optimizar sus procedimientos administrativos y mejorar sus servicios a los "clientes". En resumen, las entidades requieren ser más competitivas y mejor controladas.

Una solución para cubrir estos objetivos es implantar una solución ***EDI (Intercambio electrónico de datos)*** de una forma inteligente.

Y continúa exponiendo:

EL RETO EDI

Para entender mejor el reto EDI para empresas hemos plasmado a continuación para el circuito de proveedores (pedidos de compras, facturas y pagos) el proceso tradicional y el proceso simplificado que permite el EDI.

LA MANERA EDI

EMPRESA A

RED DE TELECOMUNICACIONES

MENSAJE EDI

- Pedidos
- Facturas
- Pagos

LAS VENTAJAS EDI

- Simplificación de procedimientos
- Supresión del papel
- Seguridad en los intercambios
- Ahorro de tiempo
- Sin intermediarios
- Sin errores

Continúa diciendo:

El EDI facilita, a partir del uso de una estructura común de mensajes, la comunicación de informaciones entre sistemas informáticos con interdependencia de la tecnología usada por los emisores y receptores de los mensajes.

Los mensajes EDI pueden ser leídos, entendidos y explotados sin intervención humana. Permite ***ELIMINAR EL PAPEL correspondiente a diversas transacciones económicas: pedidos, facturas, órdenes de pago.***

Adicionalmente, el EDI es independiente del tamaño del negocio. De hecho, para implantar EDI solamente es necesario disponer de un PC, de un paquete de software y de una conexión telefónica.

Como se puede observar, esta tendencia se ha convertido en una revolución completamente irreversible, mientras más se avance en el tiempo mayor será la incidencia sobre los sistemas organizativos de las empresas.

En la actualidad un ejemplo de EDI que crece y se incorpora en todas las actividades empresariales es la INTERNET, donde se espera que para el presente milenio el volumen de operaciones interempresas sea monumental.

NIVELES DE RIESGOS

Asociado al triángulo del entorno informático se presentan, lo que podemos llamar, niveles de riesgo y constituyen lo que podemos denominar como riesgo inherente a cada ángulo de triángulo explicado.

SISTEMAS DE COMUNICACIÓN

En el gráfico anterior se ha querido resaltar de forma abreviada el entorno informático donde participan de una manera u otra todos los elementos que contribuyen a la seguridad de los sistemas de control interno y por ende los portadores de riesgo.

ANÁLISIS DE RIESGOS

Estos niveles constituyen elementos a considerar por la auditoría informática, cada uno de ellos se diversifican y constituyen verdaderas especialidades en sí mismos y, a su vez, interactúan entre sí adoptando la forma de una red donde cada uno depende del otro.

Cada uno en sí mismo incorpora diferentes niveles de riesgo, la interacción de ellos incremento el efecto multiplicador como será explicado posteriormente.

- El equipamiento empleado. (1er nivel)
- La plataforma a utilizar. (2do nivel)
- Los sistemas de comunicación. (Nivel opcional)
- Los sistemas de aplicación elegidos. (3er nivel)
- La información. (Elemento presente en todos los niveles.)
- Las personas que utilizan esta información. (4to nivel)
- Los especialistas que atienden esta actividad. (interactúan en todos los niveles)

Como subdivisión se puede apreciar los distintos niveles donde se concentran los elementos que contribuyen a la exposición de posibles peligros.

En el análisis de los niveles de riesgo podemos apreciar:

EL PRIMER NIVEL

Comenzamos con los soportes físicos (asociado al nivel 1).

Que está relacionado con el hardware en toda su expresión, como consecuencia se encuentra sujeto a la fórmula de

equilibrio de costo y calidad. En él se encuentran los sistemas de almacenamiento (externos e internos), las máquinas, los sistemas de respaldo tanto para la energía eléctrica asi como los de información.

Es necesario destacar que esta inversión se hace por lo regular una sola vez y debemos tener en cuenta que el excesivo abaratamiento de los costos de los componentes sin tener en cuenta la calidad puede acarrear graves problemas muy difíciles de solucionar con posterioridad.

Los errores que se producen por causa del hardware suelen resistirse a la detección debido a que no poseen una cadencia uniforme de aparición, por lo regular ocurren de forma aleatoria resultando en extremo difícil de diagnosticar.

Éste debería contar con el análisis detallado de los esquemas fundamentales de una red.

- Seguridad
- Capacidad de modificación (aumento o disminución)
- Respuesta de los servidores ante posibles contingencias.

La seguridad abarca todos los aspectos en los cuales el sistema pueda ser interrumpido mediante una falla ya sea eléctrica, de los equipos, del sistema operativo o de las aplicaciones.

Deben observarse las posibilidades disponibles para afrontar un intento de acceso ilegal, una caída de voltaje, que se deteriore una tarjeta de la red o que se inutilice una línea física de conexión, por mencionar algunos ejemplos.

Además, debemos tener en cuenta la situación física de los equipos y fundamentalmente del o de los servidores, como se ejecuta la salvaguarda y las posibilidades reales de su restauración.

La capacidad de modificación constituye un elemento que debe estar presente desde el mismo momento de la concepción de la red; este elemento no puede convertirse en un freno al desarrollo de la actividad y por ende al inminente movimiento de equipos, personal y funciones.

Constituye un quehacer diario que por motivos inherentes a la dinámica de la empresa se haga necesario modificar el estado de los accesos al servidor y el diseño debe estar preparado para el aumento y/o disminución de equipos que accedan al servidor debiéndose constituirse lo suficientemente capaz de asimilar tales modificaciones sin afectar la disponibilidad original.

Otra propiedad a observar en este tipo de sistema informática es la respuesta que pueden dar los servidores o la disposición que se obtuvo al analizar el diseño de la red para que nunca se detenga al 100% y sea posible mantener un nivel mínimo de los servicios que oferta.

Estas características se analizarán directamente en proporción al efecto que tenga una interrupción en la imagen de la empresa y el costo que esto acarrea.

Independiente de la calidad de los equipos debemos contar con los técnicos que se encarguen de la instalación que por lo regular están separados en dos ramas o vertientes, los asociados con el hardware que corren con la adecuación y prueba de los equipos preventa (es bastante usual que las compañías que venden hardware brinden la posibilidad de ensamblar componentes para formar un equipo que reúna las características que demanda el cliente).

Resulta casi imperativo la existencia de especialistas que sean capaces de producir un equipo que a partir de unos componentes básicos tenga la posibilidad de incorporarle elementos a sugerencia del cliente. Y por otro lado se rrequiere especialistas de software que generen los sistemas operativos con que vienen los equipos del suministrador.

También asociado de manera muy directa a las compañías que venden equipos están los especialistas que tienen que garantizar la reparación y el «mantenimiento» de éstos.

En este nivel, que podemos calificar de primario, contamos con reglas de seguridad de acceso que deben ser vigiladas y *cumplimentadas.*

EL SEGUNDO NIVEL

Se conforma con los sistemas operativos, los cuales tienen una escala de confiabilidad y seguridad que varían de uno a otro, interactúan en dependencia del nivel anterior y de las características que éste posea, así será el grado de confiabilidad.

Existen diferentes variantes cuando hablamos de los sistemas operativos, en su forma más sencilla indicando un monopuesto nos encontramos una serie de sistemas operativos que pueden ser utilizados y que serán los encargados de establecer barreras de acceso ya que contaremos con posibilidades que podemos considerar como de bajo nivel y de características superiores con accesos más elaborados y que dan la posibilidad de mantener leves chequeos de acceso.

Otro nivel de especialistas está constituido por los que producen todo el software necesario para que los equipos funcionen, y están asociados a los sistemas operativos. Si hacemos un símil con un antiguo equipo tocadiscos las máquinas se asocian a la computadora como tal y los discos a los programas con que se trabaja el equipo.

Esta función cada día se hace más reservada a un grupo élite destacado en las grandes transnacionales que por una parte cuenta con años de experiencia en estas lides y con suficientes posibilidades para mantener investigaciones de alto costo constituyendo verdaderos monopolios que garantizan que ningún novato pueda incursionar en este mundo.

Las facilidades que incorporan los nuevos sistemas operativos impulsan a los conocedores a desarrollar intentos de automatización de tareas aisladas, trayendo por consecuencia los aumentos de riesgos antes mencionados.

NIVEL INTERMEDIO OPCIONAL

Existe un nivel de riesgo intermedio que por un problema de presentación hemos decidido situarlo asociado a los niveles físico y de sistema operativo y es el que se conforma por la comunicación intermáquinas ya sea de características local o externa y a su vez puede ser nacional o internacional.

Nos encontramos que una facilidad constituye una complejidad en dependencia del riesgo que se desee correr o de la información que se trate, debido a que la posibilidad de compartir recursos presupone un juego de reglas y procedimientos para normar el acceso y el ¿QUIÉN?, ¿CUÁNDO?, ¿CÓMO?, ¿DÓNDE? y ¿POR QUÉ? Se accede a la información.

El especialista que se encargue de la administración de la red debe ser capaz de conocer en detalle todos los niveles de software mencionados; pero, además, debe conocer a profundidad las características del hardware instalado detallando sus puntos débiles cuando se entrelazan con el software escogido.

Se hará responsable de los accesos tanto internos como externos y es el primer guardián de la integridad de la información que está siendo procesada.

Deberá conocer las prioridades que han sido asignadas a cada puesto de trabajo no sólo en lo concerniente al acceso, sino además a aquellos puestos que suelen

denominarse estratégicos debido a que siempre requieren de un porcentaje mayor de atención.

Es por lo antes expuesto que en el administrador de una red recaen todos los aspectos que interesan a la auditoría informática debido a que es la única persona que conoce los mecanismos internos del sistema y está capacitado para transgredir en nombre de cualquier usuario la integridad de los sistemas.

Cuando nos situamos ante el tercer nivel vemos que está constituido por el o los sistemas de la aplicación en cuestión de que se trate y que conviven en el mismo soporte físico que los sistemas descritos en el nivel anterior; pero, hay que tener en cuenta que le incorporan un nivel de riesgo proporcionado por la pericia o previsión de los que confeccionaron el sistema y si se auxiliaron o no de especialistas en control interno informático y de entendidos de la actividad en específico.

Éste constituye un paso en cual se suele incluir un poco que en pedestal de la ignorancia se erige la estatua del atrevimiento porque nos encontramos ante una disyuntiva. Es decir, los especialistas en la actividad que queremos automatizar conocen a profundidad la materia que será objeto de computarizar, pero no conocen las técnicas elementales de control y seguridad; por otra parte los especialistas en informática dominan estas últimas pero no tienen el dominio de la especialidad que conlleva la actividad.

Esto nos sitúa en una zona o terreno donde la falta de observación del trabajo en grupo puede acarrearnos serias dificultades; en los procesos sencillos se recomienda que el personal que automatizará la actividad antes ejecute la tarea de que se trate. Esto no es posible en sistemas complejos porque conllevaría un excesivo consumo de tiempo y debería cuidarse además que este especialista fuese el que desarrollará el trabajo posterior de esta actividad una vez automatizada.

EL TERCER NIVEL

Como un elemento que se podría ubicar entre el tercer nivel y el que se describe a continuación es el que afecta o interactúa con la capacidad y profesionalidad de los encargados de desarrollar sistemas y está constituido por las herramientas de programación.

Con una buena herramienta se puede hacer un sistema malo y viceversa, pero está desgraciadamente muy relacionado con la profesionalidad de quién la utiliza y de la exigencia y autoestima de estas personas.

El 90% de las aplicaciones que están relacionadas con aplicaciones del control interno con bases de datos y cuando observamos detenidamente herramientas como FOXPRO, DBASE y se comparan con otras, podemos notar que la diferencia es abismal tanto desde el punto de vista de la integridad de los datos (transacciones) así como del control de acceso.

Para describir un ejemplo analicemos una transferencia entre dos cuentas que está constituida de al menos dos operaciones programáticamente independientes.

Hay que disminuir de una cuenta, que constituye una operación, y aumentar en la otra, pero que como sistema es una única operación de «todo o nada». Es decir si en el justo momento que se rebaja de una cuenta sucede una interrupción la operación queda incompleta y a efectos del sistema introduce un error que ya proporciona un desbalance.

Otro ejemplo se observa en los procesos asociados con la afectación de un registro transaccional y la actualización de un maestro si sucede una alteración del proceso en ese momento puede ocurrir que cuando comprobamos ha actualizado un fichero y otro no.

Esto se logra solamente si nos cercioramos, que la operación ha sido completa si no es así no se procedería a efectuar el paso primario. Resulta difícil de garantizar por programa si la plataforma del software (sistema operativo más la herramienta de programación) no brinda posibilidades al respecto ya que sería necesario para lograr un efecto similar efectuar una programación de muy bajo nivel la cual acarrea que el tiempo ahorrado en programar la aplicación en cuestión se pierde en garantizar la seguridad y la integridad de la información.

Encontramos otro nivel de especialistas que desarrollan su trabajo en el campo de las aplicaciones donde el mercado se encuentra más repartido y en el que podemos encontrar diferentes niveles de integración encontrándonos que en algunas materias se desarrollan excelentes sistemas que permiten recoger todas las variantes posibles, para mencionar un ejemplo:

Los sistemas integrados de contabilidad realizan casi todas las funciones que requiere el control de esta actividad.

Es bastante frecuente que compañías que posean un cierto nivel de importancia cuenten con especialistas para desarrollar un software propio adecuado con sus necesidades, aunque es poco frecuente que exista una actividad por disímil donde no se haya concebido un sistema computarizado que recoja las expectativas de la rama en cuestión, pero infiere en estos casos los elementos de precio.

Existe un nivel de programas intermedio entre los sistemas operativos y las aplicaciones en cuestión que está conformado por herramientas que a partir de los ambientes amistosos que se generan en las pantallas gráficas han evolucionado mucho en la ultima década.

Estos programas constituidos en lo fundamental por una trilogía compuesta por un procesador de texto, una hoja de cálculo y un administrador de bases de datos, han permitido que usuarios con poca o ninguna experiencia informática elaboren informaciones a su gusto y que además posean un nivel de presentación impresionante.

A partir de esta base programática las posibilidades que brinda la computadora para acercar cada vez el usuario final a su trabajo son incontables.

Se abren los procesadores de texto con diccionarios incorporados, el diseño en todas sus facetas es ampliamente abordado por las técnicas actuales, la composición y administración musical. Es prácticamente imposible enumerar todos los campos en los cuales una aplicación específica permite a un usuario no profesional desarrollar un programa o grupo de instrucciones que satisfaga su demanda.

CUARTO NIVEL

Contamos, además con los especialistas que dominan las técnicas de redes que se pueden complicar, incluso hasta niveles complejos cuando se salen del marco de una instalación local hasta cuando hacen uso de otro grupo de expertos que permiten entrelazar estas redes con las comunicaciones.

El cuarto nivel está constituido por el elemento vital e imprescindible sin el cual no existirían los demás, es la información propiamente dicha. Por su parte ésta le añade un volumen de riesgo atendiendo a sus clasificaciones más generales.

Hasta aquí la gran mayoría de estos especialistas están vinculados a firmas relacionadas con la informática; pero, se comprueba una verdad muy grande, a pesar de que la informática ya constituye una especialidad adulta, desde hace mucho más tiempo, la actividad empresarial funciona y desde mucho más tiempo aún, la humanidad.

Esto se lleva a cabo por dos razones muy poderosas: una que seguiremos teniendo a un personal que necesita intérpretes para la computación y otra que cuando alcanza un nivel de complejidad en nuestro negocio el uso de las computadoras se hace indispensable contar con un grupo de especialistas que atiendan de forma casi simultánea todos los niveles que mencionamos en los puntos anteriores, destacándose una actividad muy importante en lo que respecta a los administradores de la información.

Como se puede observar en el gráfico hay usuarios que consultan información no determinando esta función un riesgo añadido por sí mismo, pero por el contrario existen usuarios que modifican información estando divididos en dos tipos:

- Información maestra por lo regular única.
- Información repetitiva, denominada transacciones.

Para cada tipo enunciado con anterioridad se confirma:

Actividad	Maestra	Detalle
Control de Seguridad	Menor	Mayor
Efecto Posterior	Mayor	Menor
Dificultad en su localización	Mayor	Menor
Posibilidad de error	Menor	Mayor

En la división de las informaciones contamos con:

Información Maestra Única

Se corresponde con el tipo de información que se define por lo regular una sola vez y constituye los patrones para validar las del tipo detalle, reúnen las siguientes características.

- Menor posibilidad de error

Debido a la característica de ser única en su tipo contiene chequeos iniciales de validación, que si se elaboran bien no deberán contener errores conceptuales.

- Más difícil de encontrar

Como mencionamos en el punto anterior una vez constituidos como información maestra y por ende pasadas las pruebas preliminares si se introduce un error. éste resulta más complejo para detectarlo.

- Mayor impacto posterior

Hay que tener en cuenta que si en la definición de una información maestra se comete un error, éste va a ser reproducido cada vez que utilizamos estos datos.

Pongamos como ejemplo un sistema contable que permite al definir sus cuentas. enmarcar la naturaleza de las mismas y que por error se defina un activo con naturaleza acreedora, todas las operaciones que se hagan al saldo de esta cuenta serán erróneas y en la medida que transcurra el tiempo se multiplicarán los efectos del error inicial.

- Tiene menor control de seguridad

Este tipo de información en muchas ocasiones no conlleva un mecanismo que permita una validación exhaustiva ya que no tiene las características en sí mismas que permitan su control.

Por ejemplo, la cuenta que totaliza los ingresos de un mes no tiene validación en suma contra ella misma, solamente se podrá verificar contra las facturas y devoluciones que se han hecho en el período.

Transacciones Repetitivas

- Mayor posibilidad de error
- Posee control de seguridad
- Por lo regular posee mecanismos que acortan el tiempo para detectar errores y que resulte menos complejo su hallazgo.

- Los especialistas que atienden la actividad informática:

Dentro de este nivel encontramos diferentes ramas y a cada una está asociada a diferentes técnicos:

POSIBILIDAD RIESGO

En el gráfico anterior se destaca la relación que existe entre el costo de protección y la posibilidad a la cual debemos llegar por un punto de equilibrio que no alcance ninguno de los cuadrantes denominados como de *desastre* y el de *gastos necesarios*.

Se observa, además, que en la medida que se asciende hacia el cuadrante proporcional la curva de riesgo va en aumento y en este punto un error conceptual de control interno resulta difícil para detectar y tiene un efecto multiplicador. Para encontrar este error por lo regular se requiere de una auditoría informática que revi ce el proceso y los procedimientos empleados.

CONCEPTO DE CONTINUIDAD

Cuando nos referimos a los conceptos de continuidad debemos observar el funcionamiento de la aplicación en su conjunto dentro de un proceso automatizado, no deba existir una operación que sea interrumpida por un proceso manual; es decir un resultado obtenido de un proceso automatizado, alimenta a otro por diferentes razones ya sea que no se ha construido la nterfase de los dos procesos automatizados porque radican en máquinas diferentes y no están comunicadas entre sí, porque responden a diferentes niveles en la organización empresarial etc.

En resumen podemos afirmar que si existen módulos de programas o subsistemas que se interconectan por procesos manuales que no responden a una verificación visual o de otro tipo, podemos afirmar que el sistema carece de continuidad.

Pongamos un ejemplo:

Un sistema con alto grado de integración puede hacer el proceso de facturación de un producto, éste se rebaja de inventario. se produce la factura, se actualizaran las cuentas por cobrar del cliente y es elaborado el asiento contable que se necesita para actualizar las cuentas de ingresos, costos, inventarios y cuentas correspondientes por cobrar.

Sin embargo, pudiera ser interrumpido en cualquiera de los puntos anteriores de dos formas o maneras distintas:

- Produciendo un disco o salida en soporte externo que sirva para alimentar otro sistema que se encargue del registro contable.
- Elaborar una salida en papel para registrar posteriormente este resultado en el sistema que atiende a los clientes.

La falta de observación del concepto de continuidad facilita la posibilidad de introducir errores por la intervención de la mano del hombre.

En ambos casos se deben tener en cuenta las reglas de acceso de los datos con la consiguiente validación de secuencia y chequeo de contrapartidas para lograr la disminución de errores, detalle éste muy complejo debido a que debe permitirse al sistema receptor la posibilidad de aceptar valores de forma bastante consecuente.

CONCEPTO DE INTEGRACIÓN

Constituye una extensión del concepto de continuidad ya que se refiere a la posibilidad de que no existan procesos aislados que produzcan salidas que alimentan a otro proceso.

Un ejemplo bastante frecuente de este concepto se observa en el entorno contable

de una empresa, ya que resulta difícil de disponer de un sistema automatizado que contenga los elementos necesarios para el control de dicha empresa.

A pesar de que constituyen procesos regulares o comunes en el control de una empresa no aparecen integrados en un sistema único, éstos son:

- Nóminas
- Medios básicos
- Costos
- Producción

Si a estos procesos considerados comunes le agregamos aquellos que de forma particular pertenecen a la actividad fundamental de la empresa, el sistema ya se complica, como por ejemplo pudieran ser:

- Agencias de Viajes
- Talleres

Servicios en general que dependen de la conformación de un producto.

Partimos del supuesto que queramos automatizar la empresa, pero no queremos invertir en un software y con la supervisión de un personal profesional.

Pero terminamos enfrentándonos ante un monstruo de 100 cabezas donde cada módulo tiene un fabricante distinto, con una filosofía diferente al concebir los programas y sistemas. Esto trae como consecuencia la posibilidad de que ocurran omisiones y/o errores en los puntos de conexión entre una actividad y otra.

Si no observamos estos dos conceptos en el análisis del sistema se pueden incorporar riesgos al sistema y fisuras en el control interno de la entidad que se revisa.

ANÁLISIS DE INDICADORES

Entre los aspectos a considerar para la toma de decisiones en la Auditoría Informática contamos con el análisis de indicadores que pueden resultar de gran utilidad en las diferentes etapas del proceso de una Auditoría.

Un juego de indicadores que permite medir la aplicación de los diferentes sistemas automatizados a las áreas de cualquier empresa son:

1. PARTICIPACIÓN DE LAS CUENTAS POR COBRAR

TOTAL DE CUENTAS POR COBRAR/TOTAL DE ACTIVOS

Este primer indicador nos muestra el peso que constituyen las Cuentas por Cobrar dentro de los activos.

El análisis que nos proporciona este indicador unido a la cantidad de clientes y al volumen de las cuentas por cobrar nos indica que en los diferentes casos que se nos presentan tienen diferentes comportamientos.

Por ejemplo:

Si determinamos que el indicador es superior a 50%, esto representa un peso considerable dentro de los activos; debemos analizar que es una compañía que trabaja fuertemente las líneas de crédito con sus clientes. Si además posee un volumen considerable y una gran cantidad de clientes se hace obligatorio el contar con un sistema que como mínimo cuente con un módulo que atienda a los clientes, que tenga bien detallados los estados de cuentas y que permita el análisis por edades de dichos saldos.

A su vez debe proporcionar una forma de limitar los créditos y de avisar cuando se haga una oferta o una venta sobre el crédito asignado.

No obstante se puede analizar en conjunto los indicadores de liquidez y de solvencia para reafirmar los conceptos que

aunque la empresa cumpla los planes de ventas y de rentabilidad puede ir a la quiebra si no está pendiente de sus Cuentas por Cobrar. Esto tiene que estar avalado por un sistema-automatizado lo suficientemente ágil que permita la toma de decisiones por la dirección de la entidad.

2. PARTICIPACIÓN DE LOS INVENTARIOS

TOTAL DE INVENTARIOS/TOTAL DE ACTIVOS

Este indicador nos muestra el peso que tiene dentro de los activos las cuentas de inventario, que unido a los conceptos de cantidad de item o artículos, productos, servicios y el volumen real del valor, nos dan una idea de la seriedad del módulo de control de inventario que como mínimo debe contar con la rebaja o el aumento de las cantidades en físico y en valor, proporcionando la existencia real con el almacén. Además debe tener los mecanismos mínimos indispensables para que el almacén recepcione las cantidades y poder aumentar de forma automática y al unísono las existencias y los compromisos de pago a los suministradores.

Si además este análisis se conjuga con el indicador de Rotación de Inventario debe brindar la posibilidad a la esfera comercial de conocer de forma muy ágil los productos que contengan poco movimiento, sin movimiento y por ende los que tienen buena salida.

3. PARTICIPACIÓN DEL EFECTIVO EN BANCO

TOTAL DE EFECTIVO EN BANCO / TOTAL DE ACTIVOS

Este análisis va a mostrar muy claramente la definición de la empresa en relación con su liquidez.

Esto puede acarrear dos variantes, que ese efectivo esté en Banco, pero además de que tiene una rotación alta debido a que la empresa tiene acceso al comer- cio al detalle y por lo tanto tendrá diferen-tes observaciones.

El sistema para el caso de que el dinero esté en Banco deberá contemplar aspectos relacionados con el manejo financiero de la empresa, analizar en dependencia del caso de que se trate de un buen control de Plazos Fijos, Cuentas de Banco, vencimientos de documentos de pagos y control de cartas de crédito.

Si además influye en este indicador la actividad minorista debemos analizar un buen sistema de cobros, si es preciso un sistema de cajas registradoras con la consiguiente conexión on line o una central.

4. ACTIVOS FIJOS

TOTAL DE ACTIVOS FIJOS /TOTAL DE ACTIVOS

Por igual representa el peso de los activos fijos dentro del total de activos de la compañía y tendremos en cuenta que si es un indicador fuerte y además analizamos el volumen en cantidad e importe arrojado que son considerables, es preciso que se cuente con un buen sistema que proporcione el registro y control de estos activos.

PASIVOS

Al igual que en los activos mediante un ligero análisis de participación podemos inferir la necesidad de determinados sistemas automatizados para el control y efectividad de estos pasivos.

5. CUENTAS POR PAGAR

TOTAL DE CUENTAS POR PAGAR/TOTAL DE PASIVOS

Representa el peso de las cuentas por pagar o capital ajeno con relación al total de pasivos en dependencia del volumen de las operaciones, los montos de los saldos

y cantidad de proveedores. Resulta muy importante que mantengamos una vigilancia de nuestros compromisos de pagos debido a que este aspecto va a constituir la imagen de nuestra empresa.

Se puede agregar varios indicadores asociados a estos análisis y para cada uno de ellos existe un razonamiento y un nivel de automatización a medir.

FASES DE LA AUDITORÍA INFORMÁTICA

La elaboración de un plan para acometer una Auditoría Informática requiere de acciones muy similares a las que se realizan cuando nos enfrentamos a una auditoría financiera o de balances por lo que a continuación se relacionan los pasos que de forma general deben tenerse en cuenta para iniciar una certificación del grado de utilización y protección de la información automatizada en una entidad.

Una versión preliminar de los pasos que se deben dar para acometer la evaluación de la organización interna de una empresa cuando ésta tiene componentes de su control interno automatizados y enfocada desde el punto de vista de las sociedades de ser vicios, pudiera ser:

I. Fase Contractual

Denominada así debido a que en este período se establecen los primeros vínculos con el cliente potencial encaminados a conocer de forma abreviada los principales rasgos mediante los cuales se puedan determinar la magnitud del riesgo al que se encuentra sometido el cliente y por ende el estimado de tiempo que se requiere para elaborar un dictamen de la situación informática.

1. Contacto inicial con el cliente.
2. Investigación preliminar.
3. Cálculo del riesgo de Auditoría.
4. Determinar:
   - Tipo y alcance del trabajo a realizar.
   - Fecha de realización del trabajo.
   - Fijación de honorarios.
5 Envío de propuesta inicial y firma del contrato.

II Fase Preliminar

6 Confección preliminar del calendario de trabajo.

7. Conocimiento del Cliente.
   - Organigrama.
   - Planes de contingencia.
   - Normas y procedimientos.
   - Bases jurídicas.
   - Suministradores del hardware (incluye alternativas energéticas).
   - Suministradores del software.
   - Características, si existe del centro de diseño propio.
   - Sistemas operativos en funcionamiento.
   - Niveles de seguridad.

   Revisión analítica preliminar (R.A.P)
   - Sistemas operativos instalados
   - Control del software
   - Inventario detallado de equipos vs. software sontrol de antivirus
   - Acceso a las computadoras
   - Acceso a locales donde se encuentran los equipos

9 Descripción del control interno administrativo.
   - Organigrama de la actividad
   - Esquema computacional
   - Cruce de los puntos anteriores
   - Balance de carga y capacidad
   - Alcance de los sistemas implantados

- Determinar suficiencia del equipamiento
- Necesidad de automatización

10. Evaluación del control interno
    - Sistemas instalados
    - Actividades y funciones
    - Procedimientos organizativos y/o manuales del sistema informativo computacional
    - Uso de cuestionarios
    - Ficheros traza con cruzamiento de puestos de trabajo y claves de acceso.
    - Uso flujogramas
    - Chequeo de salvaguardas
    - Chequeo de claves de acceso y accesos remotos (teniendo en cuenta que para algunos sistemas operativos no tienen diferencias)
    - Evaluación de la confiabilidad de la información
    - Destacar puntos débiles y fuertes (incluir apuntes para el Memorándum de revisión interna.

III Fase Final

11. Preparación del informe y Memorándum de revisión interna
12. Discusión con el cliente de ambos documentos
13. Entrega informe final (dictamen) y Memorándum de revisión interna.

Destacar iguales términos que para los informes de Auditoría de Balances:

- Confiable
- Con salvedades
- No confiable

Facturación - Cobro.

CONCLUSIONES

Como se ha podido observar a lo largo del trabajo realizado, no encontramos condiciones en las empresas actuales que definan aspectos a los cuales nuestros auditores se tienen que enfrentar irremediablemente; existen características propias inherentes a entidades en particular en lo que a equipamiento y personal que labora alrededor de ellas.

Por otra parte consideramos como un tema poco probable que en la actualidad el mayor porciento de los auditores de cuentas puedan convertirse en informáticos y, en una medida menor, que puedan operar herramientas como las que se utilizan en las técnicas asistidas por computadora.

Y también resulta en menor medida que los auditores utilicen computadoras ya sean personales o de mesa, siendo una práctica común que elaboren sus informes y tablas y posteriormente una operadora con alguno de los paquetes de tratamiento de texto y hojas de cálculo sea la que confeccione el dictamen en forma automatizada.

Como planteamos en el desarrollo del trabajo, las características de formación del informático le hacen difícil pensar como un contador y en la mayoría de los casos no se explican cómo funcionan las cuentas por su naturaleza y cuándo es que aumentan por el DEBE y disminuyen por el HABER, por la única y sencilla razón de que quieren aplicar la lógica y no siempre es posible.

Es más frecuente encontrarse a contadores que trabajan como informáticos, debido a la bondad de los nuevos sistemas de programación, que a informáticos que se desempeñen como contadores.

Esta experiencia no constituye una práctica exclusiva en cualquier país, ni de nuestra profesión y nos la encontramos en los despachos de abogados y auditores de otros países que plantean que estos programas resultan una camisa de fuerza y que

les resta iniciativa en el trabajo; esta situación en gran medida se relaciona con aquellos profesionales que hacen rechazo a la computación, esto se manifiesta en casi todas las profesiones donde la informática está presente.

Las razones detalladas anteriormente constituyen las causas fundamentales para el análisis de la profesión del auditor informático y la posible formación de un profesional con esas características, por lo que a mi criterio se puede reafirmar el concepto mostrado en el desarrollo del trabajo de que la auditoría informática, como su nombre indica, no puede ser desarrollada por una sola persona, debe ser abordada por un equipo que al menos tenga profesionales de ambas especialidades. Además, debemos darnos la tarea de preparar a los actuales auditores de cuentas o balances mediante la asimilación de los conceptos y herramientas aportadas en este trabajo que le permitan tener una visión más exacta del entorno que auditan y puedan comprender, trasmitir y dialogar en un lenguaje similar a los informáticos.