CARRERA: Especialización en Contabilidad Superior y Auditoría.

TRABAJO FINAL DE ESPECIALIDAD

AUDITORÍA DE SISTEMAS DE INFORMACIÓN EN UN ENTORNO INFORMÁTICO.

AUTOR:

Pro, Diego Gabriel

DIRECTOR:

Castello, Ricardo Justo

CO-DIRECTOR:

Morales, Héctor Rubén

ASESOR METODOLÓGICO:

Argüello, Juan Alberto

Córdoba, 30 de Junio de 2016

AGRADECIMIENTOS

Primero, me gustaría agradecer al director de Tesis, Castello Ricardo Justo, y al co-director de Tesis, Morales Héctor Rubén, por sus conocimientos, sus orientaciones, su manera de trabajar y por el esfuerzo realizado, los cuales sirvieron de guía y asesoría para la realización de este Trabajo de Tesis.

Segundo, y con la misma importancia, agradecer al Asesor Metodológico, Arguello Juan Alberto, y a la Directora de la Carrera, Werbin Eliana, por su dedicación, su persistencia, su paciencia y su manera de trabajar los cuales han inculcado en mí un sentido de seriedad y responsabilidad dándome una formación completa como investigador.

Mi total admiración y respeto, a todos ellos, por todo lo recibido durante el periodo de realización de esta Tesis de Especialización.

DEDICATORIAS

Dedico esta Tesis a mis padres, Pro Eduardo Diego y Galloppa Miriam Mabel, Quienes fueron el principal cimiento para la construcción de mi vida profesional, Sentando en mí las bases de responsabilidad y deseo de superación. A mi hermano, Pro Leonardo Ariel, quien me enseño sobre la calidad profesional y el esfuerzo que se debe realizar en lo que uno quiere crecer. A mis abuelos, por sus enseñanzas, los valores inculcados y su amor incondicional. A mis compañeros de postgrado quienes han sido de gran apoyo en los momentos de incertidumbre. Por último, a mis amigos quienes siempre me han acompañado estando en todo momento.

RESUMEN

El presente trabajo final pretende abordar sobre los alcances e implicancias de un trabajo de auditoría en un Sistema de Información computarizada. De lo analizado hay que tener en cuenta, como ejes principales, las falencias que se presentan de control en cuanto la gestión informática, visibles principalmente en la falta de un Plan Estratégico, la inexistencia de una Política de Seguridad Informática y en la carencia de un Plan de Contingencias que asegure la continuidad empresarial. En el mismo orden, es importante tener en cuenta, la falta de definición de una única área responsable de las actividades relacionadas con la Tecnología de Información. Por consiguiente, el auditor debe tomar de base la eficiencia de los controles organizativos y de gestión de Tecnología de la Información existentes del ente auditable. En ese sentido, el auditor debe recomendar, al ente o área auditada, desarrollar un plan de acción que contemple la superación de los distintos posibles hallazgos, designando en todos los casos, los responsables, tareas, plazos y recursos necesarios para su regularización.

Palabras claves: Técnicas y procedimientos de auditoría, Contingencias en un ambiente informático, Medidas de Seguridad Informática, Sistema de Control Interno, Gestión de Tecnología de la Información.

ABSTRACT

This Final work aims to approach on scope and implications of an audit in a computerized information system. Of the analyzed must take into account, as principal axes, the shortcomings presented control as IT management, mainly visible on the lack of a Strategic Plan, the absence of an Information Security Policy and in the absence of a contingency plan to ensure business continuity. In the same order, it's important to have on mind, the lack of definition of a single area responsible for activities related to Information Technology. Therefore, the auditor should take of base the organizational efficiency and management controls existing Technology Information of the auditable entity. In that sense, the auditor should recommend, to the audited entity or área, develop an action plan that includes overcoming the various possible findings, designating in all cases, responsible, tasks, deadlines and resources required for their regularization.

Keywords: Techniques and audit procedures. Contingencies in a computer environment, measures Security, Internal Control System, Management Information Technology.

ÍNDICE

INTRODUCCIÓN…….1

METODOLOGÍA…….5

RESULTADOS Y DISCUSIÓN. ……7

1. Estudio exploratorio sobre Técnicas y procedimientos para la realización de trabajos de auditoría informática en un Sistema de Información……..……7

   Normas……...……....7

   Técnicas…….……8

   Procedimientos……...……...……9

   Archivos Logs……..……10

   Técnicas de auditoría Computarizadas……..……..……12

2. Descripción de las contingencias en un ambiente informático, medidas de resguardo y la auditoría como herramienta de seguridad……..……..17

   Amenazas…….……18

   Medidas de Seguridad…….19

   IRAM-ISO EC 1779/27001...……..……20

   Sistema de Gestión de la Seguridad de la Información (SGCI)....…….23

   Ciclo Demmings PDCA…….…….25

   Plan de Contingencia……...……27

3. Análisis sobre la Metodología de revisión y evaluación de un sistema de Control interno. ……28

   Controles Internos sobre la Organización del área Informática…….……..30

   Controles Internos sobre el desarrollo e implementación de sistemas……....32

Controles internos sobre la operación del sistema……...33

Controles Internos sobre los procedimientos de entrada de datos, el procesamiento de información y la emisión de resultados…….…….34

Controles Internos sobre la seguridad del área de sistemas…….36

CONCLUSIONES…….……...38

BIBLIOGRAFÍA……..…40

- Introducción

Los Sistemas de Información y las Tecnologías de Información (TI) han cambiado la forma en que operan las organizaciones actuales. A través de su uso se logran importantes mejoras, pues automatizan los procesos operativos, suministran una plataforma de información necesaria para la toma de decisiones y, lo más importante, su implantación logra ventajas competitivas o reducir la ventaja de los rivales.

Las Tecnologías de la Información han sido conceptualizadas como la integración y convergencia de la computación, las telecomunicaciones y la técnica para el procesamiento de datos, donde sus principales componentes son: el factor humano, los contenidos de la información, el equipamiento, la infraestructura, el software y los mecanismos de intercambio de información, los elementos de política y regulaciones, además de los recursos financieros.

La informática tiende en forma manifiesta a suprimir el papel como soporte de las operaciones que procesa y la telemática a eliminar la necesidad de la presencia física de los operadores. En forma obvia, la transferencia electrónica de fondos (cuya técnica se funda en la informática y la telemática) estaba destinada a colisionar con la estructura jurídica correspondiente la cultura del papel, basada sobre la instrumentación y firma de los actos. Los aspectos legales más críticos en esta materia son los que se refieren a la identificación de la parte que cursa la transacción y al valor de los registros de las memorias electrónicas como medio de prueba legal. (Mille, 1989)

El sistema de tratamiento de la información, especialmente si se trata de sistemas integrados, capta la información una sola vez, la que es objeto de numerosas

transacciones, para convertirse en información elaborada a distintos niveles. Ello supone que las transacciones iniciales pueden ser sometidas a procedimientos muy complejos, haciendo difícil establecer la correspondencia entre resultados y transacciones iniciales. (Pérez Gómez, 1988)

Uno de los riesgos asociados con la utilización del computador, desde el punto de vista del auditor que va a emitir su opinión sobre las cifras de un estado financiero, es que la información que le sirve de base… puede estar contaminada. … Lo sutil de un fraude por computadora es que siempre podremos hacer la columna A igual a la B… exclusivamente para los auditores. (Lambarri, 1988)

De los riegos mencionados nace la importancia del control. Éste último se define como el proceso de ejercitar una influencia directiva o restrictiva, es decir, las posibilidades de dirigir actividades hacia objetivos buscados o de evitar que se produzcan resultados no deseados. (FACPCE, 1985)

El control interno es uno de los aspectos que más interesa en la evaluación de los sistemas de información. Se refiere a los métodos, políticas y procedimientos adoptados dentro de una organización para asegurar la salvaguarda de los activos, la exactitud y confiabilidad de la información gerencial y los registros financieros, la promoción de eficiencia administrativa y la adherencia a los estándares de la gerencia. (Yann, 1994)

La auditoría convencional, referida siempre a los sistemas de información económico-financieros y contables, goza en la actualidad de un bagaje histórico suficiente como para considerarla como una actividad cuasi ordinaria. La irrupción de la

informática en el tejido empresarial y social, propició el uso de ésta como herramienta para la realización de aquellas. Se llegaba así al concepto de Auditoría con el auxilio de la informática. En efecto existen excelentes auditores y excelentes informáticos, pero no es habitual la simbiosis necesaria de ambos… y la falta de principios y reglas de uso generalizado admitidos en el entorno informático y por el informático. (Acha Iturmendi, 1996)

Auditoría de sistemas es un término con varias aceptaciones: en este trabajo entendemos por ella a las actividades de evaluación y control de los sistemas de información de una organización. (Castello, 2008)

El acelerado proceso de informatización de la sociedad a escala mundial, exigen metodologías de control organizadas y permanentemente actualizadas, apoyadas en parámetros normativos, que aseguren niveles deseables de confiabilidad en los resultados de los procesos. (Dagoberto Pinilla, 1994)

Por ello es de suma importancia abordar en forma práctica y concisa los principales aspectos vinculados a la auditoria aplicada a los sistemas computarizados. Algunos de los temas que se trataran en el trabajo son de gran relevancia, como las técnicas y procedimientos de auditoría aplicada en un sistema de información, la evaluación de un sistema de Control interno, las contingencias en un ámbito informático y las medidas de seguridad necesarias, entre otros.

El presente trabajo tiene como objetivo analizar el desarrollo de la auditoría de Sistemas de Información de manera tal que permita encuadrar trabajos de auditoría y de control interno a sistemas de información en entornos computarizados.

–Metodología

El presente trabajo se llevó a cabo mediante el estudio exploratorio en los siguientes ejes temáticos:

a) Estudio exploratorio sobre Técnicas y procedimientos para la realización de trabajos de auditoría de Sistema de Información.

Se realizó una descripción analítica, de lo elaborado por el Instituto Mexicano de Contadores Públicos sobre normas y procedimientos de auditoría y por lo expuesto por Ricardo Castello en su libro Auditoría de Sistema Computarizados, sobre las técnicas y procedimientos de auditoría aplicadas en un sistema de información.

El mismo utilizó como bases bibliográficas:

- Instituto Mexicano de Contadores Públicos (2010)
- Castello (2008)
- Zavaro y Martinez (2012)

b) Descripción de las contingencias en un ambiente informático, medidas de resguardo y seguridad.

Se revisó analíticamente, lo descripto por diferentes autores, sobre aquellas contingencias relevantes en un ambiente informático, sus medidas de protección y como relaciona a la auditoría como herramienta de resguardo.

El mismo utilizó como bases bibliográficas:

- San Román (2012)
- *IRAM-ISO IEC 17799 (2002) y 27001/27002*
- Rocha Vargas (2015)

c) Análisis sobre la Metodología de revisión y evaluación de un sistema de Control interno del Área de Sistemas.

Se describe lo expuesto por Muñoz Razzo en su libro Auditoria en Sistemas Computacionales. De esta manera se determinó un adecuado sistema de control interno que se adapte ante cualquier contingencia del sistema de información de una entidad.

También se repasó sobre lo expuesto por Ricardo Castello en su libro Auditoría de Sistema Computarizados, el cual aborda temas como la organización del área de sistemas y sobre el desarrollo e implementación de Sistemas.

El mismo utilizó como bases bibliográficas:

- Muñoz Razzo (2002)
- Castello (2008)

RESULTADO Y DISCUSIÓN

1. Estudio exploratorio sobre Técnicas y procedimientos para la realización de trabajos de auditoría de Sistemas de Información.

Todo el análisis que se detalla a continuación corresponde con el Instituto Mexicano de Contadores Públicos (IMCP, 2010).

El desarrollo de una auditoría se basa en la aplicación de normas, técnicas y procedimientos de auditoría. Para nuestro caso, estudiaremos aquellas enfocadas a la auditoría en informática.

Es fundamental mencionar que para el auditor en informática conocer los productos de software que han sido creados para apoyar su función aparte de los componentes de la propia computadora resulta esencial, esto por razones económicas y para facilitar el manejo de la información.

El auditor desempeña sus labores mediante la aplicación de una serie de conocimientos especializados que vienen a formar el cuerpo técnico de su actividad. El auditor adquiere responsabilidades, no solamente con la persona que directamente contratan sus servicios, sino con un número de personas desconocidas para él que van a utilizar el resultado de su trabajo como base para tomar decisiones.

Normas.

Según describe el Instituto Mexicano de Contadores Públicos (2010), las normas de auditoría son los requisitos mínimos de calidad relativos a la personalidad del auditor, al trabajo que desempeña ya la información que rinde como resultado de este trabajo.

Las normas de auditoría se clasifican en:

a. Normas personales.
b. Normas de ejecución del trabajo.
c. Normas de información.

Normas personales

Son cualidades que el auditor debe tener para ejercer sin dolo una auditoría, basados en un sus conocimientos profesionales así como en un entrenamiento técnico, que le permita ser imparcial a la hora de dar sus sugerencias.

Normas de ejecución del trabajo

Son la planificación de los métodos y procedimientos, tanto como papeles de trabajo a aplicar dentro de la auditoría.

Normas de información

Son el resultado que el auditor debe entregar a los interesados para que se den cuenta de su trabajo, también es conocido como informe o dictamen.

Técnicas.

Se define a las técnicas de auditoría como "los métodos prácticos de investigación y prueba que utiliza el auditor para obtener la evidencia necesaria que fundamente sus

opiniones y conclusiones, su empleo se basa en su criterio o juicio, según las circunstancias".

Al aplicar su conocimiento y experiencia el auditor, podrá conocer los datos de la empresa u organización a ser auditada, que pudieran necesitar una mayor atención.

Las técnicas como los procedimientos están estrechamente relacionados, si las técnicas no son elegidas adecuadamente, la auditoría no alcanzará las normas aceptadas de ejecución, por lo cual las técnicas así como los procedimientos de auditoría tienen una gran importancia para el auditor.

Según el IMCP en su libro Normas y procedimientos de auditoría las técnicas se clasifican generalmente con base en la acción que se va a efectuar, estas acciones pueden ser oculares, verbales, por escrito, por revisión del contenido de documentos y por examen físico.

Siguiendo esta clasificación las técnicas de auditoría se agrupan específicamente en estudio General, análisis, inspección, confirmación, investigación, declaración, certificación, observación y cálculo.

Procedimientos.

Se considera como al conjunto de técnicas de investigación aplicables a un grupo de hechos o circunstancias que nos sirven para fundamentar la opinión del auditor dentro de una auditoría, se les dan el nombre de procedimientos de auditoría en informática.

La combinación de dos o más procedimientos, derivan en programas de auditoría, y al conjunto de programas de auditoría se le denomina plan de auditoría, el cual servirá al auditor para llevar una estrategia y organización de la propia auditoría.

El auditor no puede obtener el conocimiento que necesita para sustentar su opinión en una sola prueba, es necesario examinar los hechos, mediante varias técnicas de aplicación simultánea.

En General los procedimientos de auditoría permiten:

- Obtener conocimientos del control interno.
- Analizar las características del control interno.
- Verificar los resultados de control interno.
- Fundamentar conclusiones de la auditoría.

Por esta razón el auditor deberá aplicar su experiencia y decidir cuál técnica o procedimiento de auditoría serán los más indicados para obtener su opinión.

Análisis de Archivos Logs.

Hoy en día los sistemas de cómputo se encuentran expuestos a distintas amenazas, las vulnerabilidades de los sistemas aumentan, al mismo tiempo que se hacen más complejos, el número de ataques también aumenta, por lo anterior las organizaciones deben reconocer la importancia y utilidad de la información contenida en los Archivos Logs de los sistemas de cómputo así como mostrar algunas herramientas que ayuden a automatizar el proceso de análisis de las mismas.

El crecimiento de Internet enfatiza esta problemática, los sistemas de cómputo generan una gran cantidad de información, conocidas como Archivos Logs, que pueden ser de gran ayuda ante un incidente de seguridad, así como para el auditor.

Los Archivos Logs pueden registrar mucha información acerca de eventos relacionados con el sistema que la genera los cuales pueden ser: Fecha y hora, direcciones IP origen y destino, dirección IP que genera la bitácora, Usuarios y Errores.

La importancia de los Archivos Logs es la de recuperar información ante incidentes de seguridad, detección de comportamiento inusual, información para resolver problemas, evidencia legal, es de gran ayuda en las tareas de cómputo forense.

Las Herramientas de análisis de Archivos Logs más conocidas son las siguientes:

- Para UNIX, Logcheck, SWATCH.
- Para Windows, LogAgent

Los Archivos Logs contienen información crítica es por ello que deben ser analizadas, ya que están teniendo mucha relevancia, como evidencia en aspectos legales.

El uso de herramientas automatizadas es de mucha utilidad para el análisis de Archivos Logs, es importante registrar todas las bitácoras necesarias de todos los sistemas de cómputo para mantener un control de las mismas.

Técnicas de auditoría computarizada

Al llevar a cabo auditorías donde existen sistemas computarizados, el auditor se enfrenta a muchos problemas de muy diversa condición, uno de ellos, es la revisión de los procedimientos administrativos de control interno establecidos en la empresa que es auditada.

La utilización de paquetes de programas generalizados de auditoría ayuda en gran medida a la realización de pruebas de auditoría, a la elaboración de evidencias plasmadas en los papeles de trabajo.

Castello (2008) describe las técnicas computarizadas para realizar pruebas a los controles programados o de aplicación más utilizadas:

a) *Ejecución manual del procesamiento:*

Castello (2008) la define como la re-ejecución del proceso que se quiere controlar en forma manual, a partir de datos reales o ficticios, por medio de una muestra. Luego se comparan manualmente con los que oportunamente generó el computador. Debe existir documentación fuente que provea los datos requeridos para la comparación.

b) *Lotes de prueba (Test Deck)*

Según Castello (2008) consiste en hacer ingresar un conjunto de datos de entrada ficticios al computador, al fin de ser procesados con la copia del mismo programa que se encuentra en operación. El lote de prueba debe incluir todas las posibles situaciones que pudieran ocurrir durante las operaciones reales. Luego, los resultados se compararán con los esperados.

c) *Simulación paralela*

Castello (2008) lo explica como la acción de simular el procesamiento de la aplicación mediante programas especialmente preparados. El auditor elabora sus propios programas y éstos deben procesar los mismos datos que los programas de la aplicación a auditar. Luego ambos resultados son comparados. La simulación necesita disponer de los datos reales de entrada y los archivos usados en su procesamiento. Luego se evaluarán las excepciones obtenidas de la corrida de simulación, entendiéndose por tales, las anomalías detectadas en el proceso de reconciliación. Estas excepciones se tendrán en cuenta a la hora de hacer las recomendaciones.

d) *Procesamiento paralelo (Parallel Test Facility)*

Castello (2008) lo define como la extracción de una muestra representativa de la información residente en los archivos de datos. Todo esto se realiza mediante una copia de los programas. Luego, se reprocesa usando datos de transacciones reales, seleccionadas por el auditor. El reprocesamiento se realiza usando los mismos programas y bases de datos, pero en otro computador.

e) *Pruebas integradas (ITF o minicompañía)*

Para Castello (2008) consiste en la creación de un ente ficticio dentro del sistema de procesamiento en operación. Por ejemplo crear una división, un departamento, una sucursal, una empresa, un empleado, etc. ficticios, insertados como registro dentro de los archivos reales que utilizan las aplicaciones en producción. A este ente ficticio se le aplicarán registros de transacciones de prueba, confeccionados en forma especial por el auditor. Debe destacarse que se utiliza el mismo sistema que está en producción. Es

necesario programar procedimientos especiales para depurar las transacciones ficticias efectuadas por el auditor contra dicha entidad.

f) Pistas de transacciones (Tagging & Tracing)

Castello (2008) la define como la técnica que establece rastros (datos especiales), con la finalidad exclusiva de servir como pista de auditoría, en los registros de movimiento que se generan a partir de las transacciones. Los datos utilizados como pistas de auditoría son grabados como campos ad-hoc en los registros durante el procesamiento de las operaciones que ingresan al sistema. A este se le incorpora un atributo (campo) especial, por ejemplo, el número de legajo del empleado, la fecha y hora de la operación, el número de estación de trabajo, entre otros. Estos datos sirven para identificar quién y cuándo se realizó la operación. La idea es guardar información que permita realizar un seguimiento de las distintas etapas que siguió el procesamiento de una transacción en particular.

g) Comparación de programas

Según Castello (2008) consiste en emplear utilitarios del sistema operativo para comparar dos o más versiones de un mismo programa ejecutable (archivo objeto) de una aplicación. La finalidad es verificar si existen diferencias entre las distintas copias y versiones de los "ejecutables". Si son diferentes se presume que hubo cambios al programa, por ejemplo, desde la última visita del auditor. En estos casos, el auditor puede pedir que se le informe respecto de dichos cambios y se le proporcione la documentación relacionada a la modificación del programa (solicitud de modificación, autorizaciones, especificaciones, pruebas, orden de puesta en operación, etc.).

h) Software de auditoría

Los productos de software para auditoría, actualmente conocidas como herramientas CAATs, son herramientas diseñadas para ayudar a los auditores a acceder e investigar el contenido de las bases de datos de la entidad auditable.

Según Zavaro y Martinez (2012) las Técnicas de Auditoría Asistidas por Computadora (CAATs) son la utilización de determinados paquetes de programas que actúan sobre los datos, llevando a cabo con más frecuencia los trabajos siguientes:

- Selección e impresión de muestras de auditorías sobre bases estadísticas o no estadísticas, a lo que agregamos, sobre la base de los conocimientos adquiridos por los auditores.
- Verificación matemática de sumas, multiplicaciones y otros cálculos en los archivos del sistema auditado.
- Realización de funciones de revisión analítica, al establecer comparaciones, calcular razones, identificar fluctuaciones y llevar a cabo cálculos de regresión múltiple.
- Manipulación de la información al calcular subtotales, sumar y clasificar la información, volver a ordenar en serie la información, etc.
- Examen de registros de acuerdo con los criterios especificados.
- Búsqueda de alguna información en particular, la cual cumpla ciertos criterios, que se encuentra dentro de las bases de datos del sistema que se audita.

Consecuentemente, Zavaro y Martinez (2012) explican porque se hace indispensable el empleo de las CAATs. Esto se debe a que esta herramienta permite al auditor evaluar las múltiples aplicaciones específicas del sistema que emplea la unidad auditada, examinar un diverso número de operaciones específicas del sistema y facilitar la búsqueda de evidencias. También permite reducir al mínimo el riesgo de la auditoría para que los resultados expresen la realidad objetiva de las deficiencias, así como de las violaciones detectadas y elevar notablemente la eficiencia en el trabajo.

Teniendo en cuenta que se hacía imprescindible auditar sistemas informáticos, así como diseñar programas auditores, se deben incorporar especialistas informáticos, formando equipos multidisciplinarios capaces de incursionar en las auditorías informáticas y comerciales, independientemente de las contables, donde los auditores que cumplen la función de jefes de equipo, están en la obligación de documentarse sobre todos los temas auditados.

De esta forma los auditores adquieren más conocimientos de los diferentes temas, pudiendo incluso, sin ser especialistas de las restantes materias realizar análisis de esos temas. Aunque en ocasiones es necesario que el auditor se asesore con expertos, tales como, ingenieros industriales, abogados, especialistas de recursos humanos o de normalización del trabajo para obtener evidencia que le permita reunir elementos de juicio suficientes.

2. Descripción de las contingencias en un ambiente informático, medidas de resguardo y seguridad.

Según San Román (2012) Los sistemas de información, incluidos los contables, contienen datos privados y confidenciales que pueden quedar comprometidos si no se protegen. El uso no autorizado de la información de un sistema puede llegar a ser catastrófico, resultando en un riesgo de pérdida de esta, errores en la introducción de datos o mal uso de la información confidencial. La seguridad de los sistemas de información es una prioridad en la mayoría de las organizaciones.

La Ley Sarbanes-Oxley (2002) procura hacer más comparable el reporte de estados financieros de las organizaciones. El escándalo de Enron y la manipulación de la información reportada por parte de los altos ejecutivos financieros provocó que el Congreso Norteamericano endureciera su postura hacia las organizaciones que cotizan en Bolsa, buscando que todo aquel que tiene interés en la organización (empleados, ejecutivos, proveedores o accionistas llamados de manera genérica stakeholder) tenga un aseguramiento de que la gestión es honesta, transparente y que siempre hay un responsable por lo que se hace en todos los niveles.

Así pues, la Sección 404 de la Ley Sarbanes-Oxley hizo obligatorio para la Dirección incorporar controles internos sobre el reporteo financiero, que incluye los sistemas contables que generan los números que darán a esos reportes.

El tema de cumplimiento de Sarbanes-Oxley o de legislaciones específicas de las diferentes industrias (como PCI, SAS70, Basilea II, COSO, entre otras) hace cada vez más importante que todos los miembros de la organización, tecnócratas o no, se involucren en manejar funcionalidades enfocadas en seguridad para recursos tecnológicos.

AMENAZAS

Continuando con la opinión de San Román (2012) las amenazas que puede enfrentar un sistema contable varían desde transacciones fantasmas hasta que alguien robe, de manera física, una cinta magnética con información financiera. Adicionalmente, algunos otros riesgos a los que está expuesto son:

- Robo de identidad y datos de sus empleados o proveedores, que es una particularidad criminal que constituye una de las mayores actividades fraudulentas en las organizaciones.
- Pagos a proveedores inexistentes, que es uno de los recursos más recurridos en la actividad ilícita.
- Robo o eliminación intencional de información, donde participan empleados resentidos con la compañía, espías industriales o criminales informáticos.
- Daños a medios de respaldo, que son el seguro de vida de las organizaciones en caso de cualquier situación de contingencia.
- Robo de servidores, computadoras personales o equipos portátiles como: tabletas, teléfonos inteligentes, etcétera.

MEDIDAS DE SEGURIDAD

Los controles de seguridad pueden prevenir la materialización de uno de estos riesgos o detectar un problema cuando este ya se dio. Una vez que se identifican los riesgos para proteger los sistemas. Para San Román (2012) se pueden aplicar las siguientes medidas como:

- Cambiar con frecuencia las contraseñas de acceso a los sistemas, con el fin de que tengan un aceptable nivel de complejidad (combinando mayúsculas, minúsculas, números y caracteres especiales).
- "Encriptar" o cifrar la información, con el fin de que si esta es interceptada por alguien más en su transmisión entre emisor y receptor, tenga un alto nivel de complejidad para descifrarla.
- Revisar y auditar con periodicidad los reportes contables u otro relativo al negocio, lo cual permite detectar con oportunidad si existe alguna desviación de los parámetros esperados en la operación.
- Tomar previsiones para que la información de respaldo se resguarde en sitios alternos, con el fin de maximizar las posibilidades de recuperación. Esto involucra la información en medios magnéticos y la que existe en medios físicos; asimismo, la digitalización de facturas facilita que los requerimientos de espacio sean cada vez menores.
- Mantener buenos hábitos como usuario en los sistemas. Por lo general, tenemos la idea de que corresponde al Departamento de Sistemas velar por el buen funcionamiento de los recursos de información, pero las buenas prácticas comienzan con el mismo usuario: cuidando sus contraseñas, instalando solo las aplicaciones

autorizadas, no abriendo archivos de dudosa procedencia y resguardando el acceso físico a los sistemas.

San Román (2012) concluye que dentro del gobierno corporativo de las organizaciones, el cual busca que las decisiones dentro de la organización estén alineadas con los objetivos del negocio, existe, a su vez, el subconjunto del gobierno de tecnología de la información, de manera que las decisiones de TI (entre ellas las de seguridad informática) también lo estén. La información es propiedad de la organización que la genera y utiliza para fines del negocio.

De acuerdo con lo visto en el punto anterior, todos los miembros de la organización tienen responsabilidad sobre el manejo consciente de los recursos de información, desde lo que se abre en el correo hasta lo que se navega en Internet, pasando por lo que instalamos o conectamos en nuestras máquinas. El Contador Público es uno de los principales artífices de la dinámica del negocio por la criticidad de la información que maneja, y adoptar una postura de compromiso con la seguridad de la organización puede elevar el nivel de blindaje de los recursos de información.

La IRAM-ISO IEC 17799/27001 establece que la seguridad de la información se logra implementando un adecuado conjunto de controles que incluye políticas, procesos, procedimientos, estructuras organizacionales y funciones de software y hardware. Se necesitan establecer, implementar, monitorear, revisar y mejorar estos controles cuando sea necesario para asegurar que se cumplan los objetivos de seguridad y comerciales específicos. Esto se debiera realizar en conjunción con otros procesos de gestión del negocio.

La norma se basa en que las organizaciones y sus sistemas y redes de información enfrentan amenazas de seguridad de un amplio rango de fuentes. En estas se incluyen fraude por computadora, espionaje, sabotaje, vandalismo, fuego o inundación. Las causas de daño como código malicioso, pirateo computarizado o negación de ataques de servicio se hacen cada vez más comunes, más ambiciosas y cada vez más sofisticadas.

Es esencial que una organización identifique sus requerimientos de seguridad. La IRAM-ISO IEC 17799 establece como necesario tres fuentes principales de requerimientos de seguridad:

1- Una fuente se deriva de evaluar los riesgos para la organización, tomando en cuenta la estrategia general y los objetivos de la organización. A través de la evaluación del riesgo, se identifican las amenazas para los activos, se evalúa la vulnerabilidad y la probabilidad de ocurrencia y se calcula el impacto potencial.
2- Otra fuente son los requerimientos legales, reguladores, estatutarios y contractuales que tienen que satisfacer una organización, sus socios comerciales, contratistas y proveedores de servicio; y su ambiente socio-cultural.
3- Como última fuente el conjunto particular de principios, objetivos y requerimientos comerciales para el procesamiento de la información que una organización ha desarrollado para sostener sus operaciones.

La IRAM-ISO IEC 17799 propone controles para los siguientes aspectos relacionados a la seguridad de la información:

a) Documento de la política de seguridad de la información. Este debiera ser aprobado por la gerencia, y publicado y comunicado a todos los empleados y las partes externas relevantes.

b) Asignación de responsabilidades de la seguridad de la información. Debieran estar claramente definidas.

c) Conocimiento, educación y capacitación en seguridad de la información. Todos los empleados de la organización y, cuando sea relevante, los contratistas y terceras personas debieran recibir una adecuada capacitación en seguridad y actualizaciones regulares sobre las políticas y procedimientos organizacionales conforme sea relevante para su función laboral.

d) Procesamiento correcto en las aplicaciones. Prevenir errores, pérdida, modificación no autorizada o mal uso de la información en las aplicaciones

e) Gestión de la vulnerabilidad técnica. Reducir los riesgos resultantes de la explotación de las vulnerabilidades técnicas. Estas consideraciones debieran incluir a los sistemas de operación, y cualquier otra aplicación en uso.

f) Gestión de la continuidad comercial. Se debiera desarrollar y mantener un proceso gerencial para la continuidad del negocio en toda la organización para tratar los requerimientos de seguridad de la información necesarios para la continuidad comercial de la organización.

g) Gestión de los incidentes y mejoras de la seguridad de la información. Se debieran establecer las responsabilidades y los procedimientos de la gerencia para asegurar una respuesta rápida, efectiva y metódica ante los incidentes de la seguridad de la información.

La IRAM-ISO IEC 17799 también agrega como Factores críticos para la implementación exitosa de la seguridad de la información, dentro de una organización:

a) política de seguridad, objetivos y actividades que reflejen los objetivos de la empresa.

b) una estrategia de implementación de seguridad que sea consecuente con la cultura organizacional.

c) apoyo y compromiso manifiestos por parte de la gerencia.

d) un claro entendimiento de los requerimientos de seguridad, la evaluación de riesgos y la administración de los mismos.

e) comunicación eficaz de los temas de seguridad a todos los gerentes y empleados.

f) distribución de guías sobre políticas y estándares de seguridad de la información a todos los empleados y contratistas.

g) instrucción y entrenamiento adecuados.

h) un sistema integral y equilibrado de medición que se utilice para evaluar el desempeño de la gestión de la seguridad de la información y para brindar sugerencias tendientes a mejorarlo.

Rocha Vargas (2015) explica la ISO/IEC 27001 como un estándar para la seguridad de la información el cual especifica los requerimientos necesarios para establecer, implantar, mantener y mejorar un SGCI o ISMS. Este último es la abreviatura de Sistema de Gestión de la Seguridad de la Información. El término es utilizado principalmente en la nombrada ISO. Es esa parte del sistema gerencial general, basada en un enfoque de riesgo de negocio, para: Establecer, Implementar, Operar, Monitorear, Revisar, Mantener y Mejorar la Seguridad de la Información.

La Norma, en su Anexo A, enumera en forma de resumen los objetivos de control y controles que desarrolla la ISO 27002 (nueva numeración de ISO 17799), para que sean seleccionados por las organizaciones en el desarrollo de sus SGSI. A pesar de no ser obligatoria la implementación de todos los controles enumerados en dicho anexo, la

organización deberá argumentar sólidamente la no aplicabilidad de los controles no implementados.

Rocha Vargas (2015) aclara que el objetivo de un SGCI es generar un proceso que permita preservar la: Integridad, Disponibilidad y Confidencialidad de la información, Con el fin de asegurar la "continuidad del negocio". Gestionando y minimizando los riesgos a los que se encuentran expuestos los activos de la Organización. Entre estos se incluyen registros, instrucciones, checklist, formularios, procedimientos, manual de seguridad y políticas.

El cumplimiento de la legalidad, la adaptación dinámica y puntual a las condiciones variables del entorno, la protección adecuada de los objetivos de negocio para asegurar el máximo beneficio o el aprovechamiento de nuevas oportunidades de negocio, son algunos de los aspectos fundamentales en los que un SGSI es una herramienta de gran utilidad y de importante ayuda para la gestión de las organizaciones.

El nivel de seguridad alcanzado por medios técnicos es limitado e insuficiente por sí mismo. En la gestión efectiva de la seguridad debe tomar parte activa toda la organización, con la gerencia al frente, tomando en consideración también a clientes y proveedores de bienes y servicios.

El modelo de gestión de la seguridad debe contemplar unos procedimientos adecuados y la planificación e implantación de controles de seguridad basados en una evaluación de riesgos y en una medición de la eficacia de los mismos.

El Sistema de Gestión de la Seguridad de la Información (SGSI) ayuda a establecer estas políticas y procedimientos en relación a los objetivos de negocio de la organización, con objeto de mantener un nivel de exposición siempre menor al nivel de riesgo que la propia organización ha decidido asumir.

Rocha Vargas. (2015) también explica que la ISO/IEC 27001 incorpora el modelo de mejora continua o ciclo de Demmings PDCA:

- *Plan. Establecer el SGSI, Política y Análisis de Riesgos.*

Se buscan las actividades susceptibles de mejora y se establecen los objetivos a alcanzar. Para buscar posibles mejoras se pueden realizar grupos de trabajo, escuchar las opiniones de los trabajadores, buscar nuevas tecnologías mejores a las que se están usando ahora, etc.

- *Do. Implementar y operar controles.*

Se realizan los cambios para implantar la mejora propuesta. Generalmente conviene hacer una prueba piloto para probar el funcionamiento antes de realizar los cambios a gran escala.

- *Check. Monitorear y evaluar.*

Una vez implantada la mejora, se deja un periodo de prueba para verificar su correcto funcionamiento. Si la mejora no cumple las expectativas iniciales habrá que modificarla para ajustarla a los objetivos esperados.

• *Act. Mantener y mejorar.*

Por último, una vez finalizado el periodo de prueba se deben estudiar los resultados y compararlos con el funcionamiento de las actividades antes de haber sido implantada la mejora. Si los resultados son satisfactorios se implantará la mejora de forma definitiva, y si no lo son habrá que decidir si realizar cambios para ajustar los resultados o si desecharla. Una vez terminado el último paso, se debe volver al primer paso periódicamente para estudiar nuevas mejoras a implantar.

En resumen, aplicando la mejora continua y siguiendo el análisis de Rocha Vargas (2015), pasaría lo siguiente:

1º) Se analizan posibles mejoras, ya sea porque se han detectado problemas, porque los trabajadores han propuesto formas distintas de realizar alguna tarea, porque en el mercado han salido máquinas más eficientes que permiten ahorrar costes, etc.

2º) Se estudian las posibles mejoras y su impacto. Se eligen las que mejor van a funcionar y se decide implantarlas en una prueba piloto a pequeña escala.

3º) Una realizada la prueba piloto, se verifica que los cambios funcionan correctamente y dan el resultado deseado. Si los cambios realizados no satisfacen las expectativas se modifican para que funcionen conforme a lo esperado.

4º) Por último, si los resultados son satisfactorios se implantan a gran escala en la línea de producción de la fábrica. Una vez finalizadas e implantadas las mejoras, las actividades en la fábrica de piezas de aluminio funcionarán más eficientemente. No obstante, periódicamente habrá que volver a buscar posibles nuevas mejoras y volver a aplicar el círculo de Demming de nuevo.

PLAN DE CONTINGENCIA

Para concluir hasta lo aquí analizado en cuanto a medidas de seguridad y resguardo en un ambiente informático Castello (2008) incluye a lo que se llama plan de contingencia, el cual contiene las acciones planificadas para recuperar y/o restaurar el servicio de procesamiento de datos ante la ocurrencia de un evento grave que no pudo ser evitado. Cuando las medidas de seguridad fallan o su efecto no es el esperado, actúan los Planes de Contingencia.

Esta medida de resguardo debe incluir: manuales de instrucciones, juegos de copias de seguridad especiales con todos los archivos (de datos, programas y procedimientos) y bases de datos del sistema, capacitación especial para el personal responsable (simulaciones), selección y priorización de los servicios básicos a mantener (servicios de emergencia o de supervivencia), entre otros.

En ocasiones, las grandes compañías cuentan con empleados con responsabilidades tales como "Planificador de contingencias" o " Planificador para la continuidad de la actividad" asignados a la tarea de estudiar y planificar la reanudación de las actividades de la compañía tras una catástrofe. Su trabajo no está enfocado exclusivamente a recuperar sistemas informáticos, pero ellos, ciertamente, deben saber bastante sobre ellos. Cabe destacar que como todas las cosas que necesitan disciplina y práctica, restablecer un servicio informático después de un desastre requiere de práctica y análisis para tener aptitudes y poder realizarlo con un alto nivel de eficacia.

3. Análisis sobre la Metodología de revisión y evaluación de un sistema de Control interno.

Según Muñoz Razzo (2002) el establecimiento del control interno en las empresas tiene como finalidad ayudarles en la evaluación de la eficacia y eficiencia de su gestión administrativa, resaltando su trascendencia a través de la adopción de los objetivos que se pretenden satisfacer con dicho control. Estos son:

- Establecer la seguridad y protección de los activos de la empresa.
- Promover la confiabilidad, oportunidad y veracidad de los registros contables, así como de la emisión de la información financiera de la empresa.
- Incrementar la eficiencia y eficacia en el desarrollo de las operaciones y actividades de la empresa.
- Establecer y hacer cumplir las normas, políticas y procedimientos que regulan las actividades de la empresa.
- Implementar los métodos, técnicas y procedimientos que permitan desarrollar adecuadamente las actividades, tareas y funciones de la empresa.

También Muñoz Razzo (2002) destaca la influencia que tiene el control interno en la gestión administrativa de las empresas, así como su importancia en la protección de los bienes y en el buen desarrollo de las actividades y operaciones de las mismas. Siguiendo este análisis propone los siguientes puntos como objetivos específicos del control interno informático:

- Establecer como prioridad la seguridad y protección de la información, del sistema computacional y de los recursos informáticos de la empresa.

• Promover la confiabilidad, oportunidad y veracidad de la captación de datos, su procesamiento en el sistema y la emisión de informes en la empresa.

• Implementar los métodos, técnicas y procedimientos necesarios para coadyuvar al eficiente desarrollo de las funciones, actividades y tareas de los servicios computacionales, para satisfacer los requerimientos de sistemas en la empresa.

• Instaurar y hacer cumplir las normas, políticas y procedimientos que regulen las actividades de sistematización de la empresa.

• Establecer las acciones necesarias para el adecuado diseño e implementación de sistemas computarizados, a fin de que permitan proporcionar eficientemente los servicios de procesamiento de información en la empresa.

Tomando como punto de partida dichos objetivos, a continuación, se describe lo propuesto por Muñoz Razzo (2002) sobre los aspectos fundamentales del control interno aplicados a los sistemas de información computarizada:

• Controles internos sobre la organización del área de Sistemas.

• Controles internos sobre el análisis, desarrollo e implementación de sistemas.

• Controles internos sobre la operación del sistema.

• Controles internos sobre los procedimientos de entrada de datos, el procesamiento de información y la emisión de resultados.

• Controles internos sobre la seguridad del área de sistemas.

Como parte del presente estudio, a continuación se detallarán cada uno de los elementos propuestos:

Controles internos sobre la organización del área de Sistemas.

Según Castello (2008) esto implica Implica evaluar la organización interna del área de Sistemas y su dependencia dentro de la estructura general de la empresa. Para analizar la estructura orgánica del área de Sistemas se deberá solicitar toda la información y documentación referida a la organización interna de la misma. Estas son el Organigrama, objetivos y políticas del área fijados por la Dirección de la empresa, regulaciones externas y normas internas, manuales de procedimientos, instructivos de trabajo y guías de actividad, Manuales de descripción de puestos y funciones.

Bajo ese análisis se deberá verificar que ningún puesto tenga más de dos líneas de dependencia jerárquica, que no haya un exceso de descentralización de funciones, que las jerarquías sean adecuadas a las responsabilidades, etc. El tramo de control no debe ser exagerado, ni demasiado numerosos los niveles jerárquicos. También deben ser analizadas y evaluadas las funciones, procurando agrupar aquéllas compatibles o similares relacionadas entre sí debe evitar asignar la misma función a dos o más personas. También procurar localizar las actividades cerca o dentro de la función mejor preparada para realizarla

A continuación, Castello (2008) describe modelos típicos de estructuras organizacionales utilizados para establecer las dependencias funcionales del área Sistemas:

1) Un Primer Modelo el cual el área Sistemas depende de la dirección, departamento o gerencia. Normalmente depende de Administración y Finanzas.

Esto se debe a que inicialmente el Centro de Cómputos se crea para procesar los sistemas de tipo contable, financiero o administrativo. Esta situación se da con más frecuencia en estructuras pequeñas, o bien en aquellas que se inician en el uso de recursos informáticos.

2) Un segundo modelo en el cual el área es dependiente de los niveles superiores de la organización. En estos casos depende directamente de la Gerencia General, o bien, asume la forma de un staff de Asesoría al máximo nivel. Esto permitirá mejorar la comunicación directa con los departamentos usuarios y la asignación de prioridades, de acuerdo con las necesidades generales de la organización.
3) Un tercer modelo con Múltiples áreas de Sistemas en la empresa. Esta situación se produce en estructuras organizacionales muy grandes, en la que hay equipamiento informático independiente y distribuido en diferentes lugares (gerencias, divisiones, sucursales). Los departamentos de Sistemas, distribuidos por toda la organización, son controlados en cuanto a sus funcionamientos, equipamiento, presupuesto y recursos humanos en forma centralizada por la Dirección de Informática.
4) Como último modelo la Tercerización (outsourcing) de la prestación de servicios informáticos. Esta estructura puede darse a través de la creación de una compañía independiente, de propiedad de la empresa, que brinde servicios de computación a la organización o, directamente, contratando con terceros dichos servicios.

Controles internos sobre el análisis, desarrollo e implementación de sistemas.

Siguiendo con Castello (2008) este aspecto tiene por objetivo evaluar el desempeño del sector Análisis y Programación o Desarrollo y Mantenimiento de Sistemas de una empresa. Este sector es el que se ocupa de construir, implementar y mantener las aplicaciones de la organización. Es decir, es el encargado de llevar adelante los proyectos de desarrollo de nuevos sistemas de información y de mantener aquéllos que están en producción. En general, las organizaciones optan por la adquisición de paquetes de gestión estándar (ERP, CRM, SCM) o delegan en terceros el desarrollo y mantenimiento de los sistemas propios (outsourcing de desarrollo).

La actividad más significativa del área de Desarrollo se produce en los proyectos de nuevas aplicaciones, donde son los responsables primarios del éxito o fracaso de este tipo de emprendimientos. Estos proyectos son sumamente complejos, ya que involucran una mezcla de aspectos humanos y tecnológicos, incluso cambios en la cultura organizacional, alquimia que es muy difícil de lograr, tornándose muy difícil controlar el desempeño de esta función. En cambio, en las tareas de mantenimiento de las aplicaciones en producción están más acotadas las funciones y responsabilidades del sector y se pueden administrar más fácilmente. En ambos casos, el énfasis de un trabajo de auditoría debe recaer tanto sobre los costos visibles como sobre los costos ocultos que implica la actividad.

En este tipo de trabajos, el auditor debe identificar la metodología de desarrollo utilizada por el sector y el grado de respeto (uso) por parte de los programadores. Uno de los problemas más frecuentes, es que no están generalmente establecidas las pautas

de trabajo del sector. Por consiguiente, es difícil controlar su desempeño ya que no se puede auditar tareas que no están pautadas, cuantificadas y establecidas.

Controles internos sobre la operación del sistema.

Siguiendo el análisis de Muñoz Razzo (2002) es de suma importancia contar con un elemento de control interno que evalúe la adecuada operación de los sistemas. En este caso será la adopción de un elemento que se encargue de vigilar y verificar la eficiencia y eficacia en la operación de dichos sistemas. Para garantizar una mayor eficiencia y eficacia por este elemento del control interno se propone la aplicación de los siguientes subelementos:

• *Prevenir y corregir errores de operación*

Implementar mecanismos de control que permitan verificar la exactitud, suficiencia y calidad de los datos que serán procesados, vigilando el adecuado cumplimiento de la captura, procesamiento y emisión de resultados.

• *Prevenir y evitar la manipulación fraudulenta de la información*

Estudiar la importancia de prevenir y evitar la manipulación fraudulenta y dolosa de los programas propiedad de la institución y la información que se procesa a través de los equipos de cómputo. Con lo anterior se evitará un mal uso de la información por parte del personal y usuarios del área de sistemas de la empresa.

• *Implementar y mantener la seguridad en la operación*

Estas medidas van desde el control de acceso al sistema para personal, usuarios y personas con derecho, hasta la protección de las bases de datos, de los sistemas institucionales y de los procedimientos para la manipulación de los resultados de dichos procesos, pasando por los respaldos periódicos de los programas y de la información procesada, así como los demás aspectos de seguridad que repercuten en la operación del centro de cómputo.

• *Mantener la confiabilidad, oportunidad, veracidad y suficiencia en el procesamiento de la información de la institución*

Estos son los elementos básicos que se utilizan para establecer un control interno adecuado en un centro de información. Esto obedece a que con su adopción y uso permanente, como norma de trabajo, contribuyen a la cabal comprensión del objetivo fundamental del área de sistemas para la empresa, en cuanto a la captura y procesamiento de datos, emisión de resultados y custodia de la información.

Controles internos sobre los procedimientos de entrada de datos, el procesamiento de información y la emisión de resultados.

Continuando con el análisis de Muñoz Razzo (2002) un sistema de información es un procedimiento simple de entrada, proceso y salida, en donde un dato de entrada se transforma en información útil de salida mediante algún procesamiento interior, entenderemos también que el control interno informático es útil para verificar que este procedimiento se lleve a cabo correctamente. Estas fases son las que dan vigencia a

cualquier sistema. Utilizando como referencia lo anterior, a continuación analizaremos los siguientes subelementos del control interno:

• *Verificar la existencia y funcionamiento de los procedimientos de captura de datos*

Asegura que la entrada de datos será acorde con las necesidades de captura del propio sistema. Para lograr la eficiencia y eficacia que se pretenden al establecer este elemento en la captura de datos, es necesario tener bien establecidos aquellos métodos, procedimientos y actividades que regularán la entrada de datos al sistema, así como las normas, políticas y lineamientos que ayudarán a capturar mejor dichos datos. Con esto se garantiza que el procesamiento de información y la emisión de resultados sean adecuados.

También es necesario comprobar que éstos sean introducidos con la oportunidad que demanda el sistema; esto se verifica con los siguientes procedimientos:

-El establecimiento y cumplimiento de los procedimientos adaptados para satisfacer las necesidades de captura de información de la empresa.

-La adopción de actividades específicas que ayuden a la rápida captura de datos.

- El seguimiento de los métodos y técnicas uniformes que garanticen que la entrada de datos al sistema se realice siguiendo los mismos procedimientos.

• *Comprobar que todos los datos sean debidamente procesados*

Además de verificar que los datos sean capturados y procesados de manera oportuna, confiable y eficiente, igual que en la emisión de los resultados, también es indispensable que con el control interno informático se tenga la confianza de que todos los datos ingresados al sistema sean procesados de igual manera sin que sufran ninguna alteración, ya sea accidental, involuntaria o dolosa, durante su procesamiento.

Cumpliendo con esto se garantiza la uniformidad de los resultados y, consecuentemente, se obtiene una mejor explotación de los mismos.

• *Verificar la confiabilidad, veracidad y exactitud del procesamiento de datos*

Establecer los procedimientos adecuados que ayuden a satisfacer los requerimientos de captura y procesamiento de información en el área de sistemas. También se deben adoptar acciones concretas que ayuden a capturar y a procesar los datos de manera eficiente. Para ello se tienen que establecer métodos, técnicas y procedimientos que sean aplicados de manera uniforme en todas las etapas que intervienen en el procesamiento de información; con esto se pueden garantizar mejores resultados en la verificación de la uniformidad que requiere este subelemento del control interno informático.

• *Comprobar la suficiencia de la emisión de información*

Esta información debe ser adecuada a los requerimientos de la empresa para ofrecer sólo la información requerida, sin dar ni más ni menos datos que los necesarios. A esto se le llama proporcionar la información suficiente. Esto se logra mediante un análisis adecuado de sus necesidades y con el diseño correcto de los sistemas que proporcionarán esa información. Evidentemente, dicha suficiencia sólo se logrará mediante un buen análisis y diseño de sistemas.

Controles internos sobre la seguridad del área de sistemas.

Para el mejor entendimiento de la importancia de este elemento y de su aplicación correcta, remitirse a lo analizado sobre MEDIDAS DE SEGURIDAD de la Metodología segunda de este Trabajo de Tesis Final.

De todo lo analizado se describieron los conceptos y características fundamentales del control interno en los sistemas computacionales y se identificaron sus principales aplicaciones en la auditoría de sistemas. Lo visto ayuda a entender cómo se pueden satisfacer, con eficiencia y eficacia, las necesidades de evaluación, razonabilidad y oportunidad en la protección y seguridad de los bienes, de la información y del personal del área de sistemas de una institución. También para definir el desarrollo de las actividades, operaciones y resultados obtenidos en el procesamiento de la información de las áreas de sistemas de una organización. Todo ello con el propósito de comprender la importancia del control informático en las áreas de sistemas de las empresas, así como su uso en cada uno de los tipos de auditorías de sistemas para identificar los aspectos fundamentales de aplicación en la auditoría de sistemas de información.

CONCLUSIÓN

De lo analizado para la realización de un trabajo de Auditoría de Sistemas de Información hay que tener en cuenta como ejes principales las falencias que se presentan de control en cuanto la gestión informática. Esto se hace visible principalmente debido a la falta de un Plan Estratégico, la inexistencia de una Política de Seguridad Informática y en la carencia de un Plan de Contingencias que asegure la continuidad empresarial.

En el mismo orden, es importante tener en cuenta sobre la definición de una única área responsable de las actividades relacionadas con la Tecnología de Información, como así también, las normas y procedimiento formalizados para las distintas actividades del área.

Por otro parte, tener en cuenta la existencia de aplicaciones desarrolladas que no se utilizan por áreas usuarias o se aplican de manera deficiente. Ambas situaciones denotan falencias metodológicas así como una deficiente administración de los recursos utilizados.

Por consiguiente, el auditor debe tomar de base la eficiencia de los controles organizativos y de gestión de Tecnología de la Información existentes en el ente auditable. A partir de eso, en base a sus conocimientos, experiencias e intuición seleccionará las técnicas que considera más adecuadas para probar el funcionamiento y la calidad de los controles que audita.

En ese sentido, en base a los resultados obtenidos, el auditor debe recomendar al ente o área auditada desarrollar un plan de acción que contemple la superación de los distintos posibles hallazgos, designando en todos los casos, los responsables, tareas, plazos y recursos necesarios para su regularización.

Es de imperiosa necesidad que el auditor abarque los principales aspectos de auditoria de sistemas de información computarizada revisados y analizados en este trabajo de Tesis. Éstos son de gran relevancia y, en base a los mismos, el auditor diseña y desarrolla pruebas de control y procedimientos sustantivos, el plan de auditoría, su dirección y ejecución. Siendo esta la base sólida para la confección y emisión de la opinión de su trabajo como profesional.

1. –Bibliografía

- Acha Iturmendi, J. J. (1996). *Auditoría informática en la empresa*. Ed. Paraninfo. Madrid.
- Barreira Sans, J. (1980). *La auditoría interna*. Revista Española de Financiación y Contabilidad. Vol. 9, Nº 31, 141-150.
- Buchanan S. y Gibb F. (2008). *The Information Audit Methodology Selection*. International of Information Management.Vol. 28. I. 1. 3-11.
- Castello, R. J. (2008). *Auditoría de sistemas y tecnologías de información*. (3ª ed. ACFCE). Córdoba, Argentina.
- Derrien, Y. (1994), *Técnicas de Auditoría Informática.* Marcombo, España.
- Dagoberto Pinilla F. (1994). *Las normas de Auditoría Informática*. Innovar: revista Nº 4, 31-34.
- Gibb F. y Buchanan S. (2008). *The Information Audit theory versus practice*. International of Information Management.Vol. 28. I. 3. 150-160.
- Guiral Contrera, A. y Angulo, J. A. (2005). *Informe de auditoría y comportamiento de los analistas de riesgos*. Revista Española de Financiación y Contabilidad. Vol. 34, Nº 125, 501-536.
- Echenique García, J. A. (1995), *Auditoría en Informática*. Edit. Mc Graw Hill, México.
- Federación Argentina de Consejos Profesionales de Ciencias Económicas. (2004). *Informe Nº 5*. Argentina: Manual de Auditoría.
- Ferreyros Morón, J. A. (1995), *Informática Contable y Auditoría de Sistemas*. Edit. La Senda. Perú.

- Gil Peuchan, I. (1999), *Sistemas y Tecnologías de la Información para la Gestión*. Edit. McGraw Hill. Madrid, España.
- Instituto IRAM (2013). *NORMA IRAM-ISO IEC 17799 y 27001/27002*. Buenos Aires.
- Instituto Mexicano de Contadores Públicos (2010). Normas y procedimientos de auditoría. México D.F.
- Kyriazoglou, J. (2013). *Controles estratégicos y operacionales de la TI*. ISACA Journal. Vol. 2. 1-2.
- Lambarri V, A. (1988). *Utilizando el computador para realizar la auditoría*. I Congreso Iberoamericano de Informática y Auditoría. San Juan de Puerto Rico, Madrid.
- Ley 25326 (2000). *HABEAS DATA*. Argentina: Protección de datos personales.
- Ley Sarbanes Oxley (2002). Estados Unidos.
- Muñoz Razo, C. (2002). *Auditoría en sistemas computacionales*. Ed. Pearson. México.
- Mille, A. (1989). *La monética y sus leyes*. Revista Presencia NCR Nº 10, 35. Buenos Aires.
- Pérez Gómez, J. M. (1988). *La auditoría de los sistemas de información*. I Congreso Iberoamericano de Informática y Auditoría. San Juan de Puerto Rico, Madrid.
- Rocha Vargas, M. (2015). *Seguridad Informática (SGSI).* Córdoba, Argentina.
- San Román, E. (2012). *Seguridad Informática*. Revista Contaduría Pública IMCP Nº 5, 34. México.
- Solís A, y Montes, G. (2002). *Reingeniería de la Auditoría Informática*. Trillas. México.

- Sindicatura General de la Nación (2005). *RES 107/98 Y 4805/05*. Argentina: Normas generales de control interno.
- Zavaro, L. y Martínez C. (2012). *Auditoría informática, las técnicas de auditoría asistidas por computadora (CAAT)*. México.