METODOLOGÍA DE TRABAJO DE LA AUDITORÍA INFORMÁTICA

MG. ING. Bruno Roberti (2021)

Tabla de Contenidos

Introducción

En la medida que el grado de informatización en los sistemas de información se ha incrementado en forma constante durante los últimos años, ha sido necesario adecuar las técnicas de auditoria para poder contener de mejor manera los nuevos desafíos que plantean estos cambios, dando pie a la creación de una nueva rama de la auditoría, la Auditoría Informática. Pero estos cambios no solo impactaron en esta nueva rama, sino también en las demás ramas de la auditoría ya que los sistemas están integrados de forma profunda dentro de la gestión de las organizaciones.

Si tomamos la definición de auditoría como "La inspección y verificación formal para comprobar la adhesión a un stándard o conjunto de reglas, la precisión de los registros, o si la eficiencia y eficacia de los objetivos se está alcanzando" (ISACA) podemos vislumbrar como los avances tecnológicos, los cuales han generado una serie de cambios muy importantes dentro de las organizaciones, plantean dificultades en diversas áreas de la práctica de la auditoría que exceden el ámbito de la auditoría en informática, por ejemplo la gran cantidad de registros a revisar, la implementación de controles y cálculos en forma automática y el alto grado de interrelación entre distintas aplicaciones informáticas por mencionar algunos.

El objetivo inicial que perseguía la Auditoría Informática era evaluar el diseño y efectividad del sistema de control interno asociado a los sistemas de información que posee una organización. Actualmente este concepto ha evolucionado incluyendo la evaluación de la eficiencia y eficacia del sistema de información en su totalidad. Esto se realiza principalmente, pero no exclusivamente, a través de 3 grandes funciones:

- El análisis de la eficiencia y eficacia de los Sistemas de Información
- La verificación de la consistencia y cumplimiento de la Normativa general en ese ámbito
- La revisión de la eficaz gestión de los Recursos Informáticos.

Tipos y Enfoques de Auditoria Informática

Para el presente documento no se tomará el enfoque de la división entre auditoria interna y externa, el cual si bien presenta aristas muy interesantes que se prestan para el debate como es la objetividad, el nivel de profundidad alcanzado o las diferencias en el seguimiento, no aporta al objetivo bajo análisis el cual es las herramientas de soporte a la auditoria informática.

El enfoque en el cual basaremos nuestro análisis son los controles, tomados desde la óptica del ámbito sobre donde se aplican los mismos. Con este criterio podemos proponer la división entre:

- Controles Aplicativos
- Controles Generales de TI

Controles Aplicativos

Estos controles se aplican a nivel de procesos, definidos para actividades específicas las cuales pueden estar automatizadas o integradas con los sistemas aplicativos. Una clasificación general de los diferentes tipos de controles a implementar podría incluir:

- Controles Manuales sobre las aplicaciones
- Controles Programados en las aplicaciones
- Controles Lógicos de acceso a los sistemas aplicativos

Sin embargo una enumeración más rigurosa de las distintas categorías de controles a implementar sobre una aplicación es de muy difícil realización, ya que son muchos los objetivos que persiguen y las mismas varían también de acuerdo a la naturaleza del sistema de información al cual brindan soporte. Otro enfoque para definir las categorías en las cuales se van a ajustar los diferentes controles aplicativos es a través de la definición de los Objetivos de Control que se busca evaluar al momento de realizar una Auditoría Informática sobre una aplicación.

Tomando las definiciones de COBIT y combinándolas con los objetivos ampliados de la definición de Auditoría Informática podemos definir los siguientes Objetivos de Control de una aplicación:

- Eficiencia de la Aplicación
- Eficacia de la Aplicación
- Preparación y Autorización de Información de Origen.
- Recolección e Ingreso de Información de Origen
- Chequeos de Exactitud, Integridad y Autenticidad
- Integridad y Validez del Procesamiento
- Revisión de Salidas, Reconciliación y Manejo de Errores
- Autenticación e Integridad de Transacciones

Controles Generales de TI

Estos controles se definen sobre las actividades de servicio de TI, están presentes sobre el ambiente que rodea a los sistemas de información.

- Cumplimiento de Políticas y Procedimientos
- Desarrollo, Adquisición y Mantenimiento de Aplicaciones Informáticas
- Monitoreo de las Operaciones
- Organización y Planificación de TI
- Administración de la Seguridad de la Información
- Otros

Relación entre Controles de Aplicación y Generales de IT

La efectividad de los Controles de Aplicación depende del grado de confiabilidad del ambiente donde se realizan las actividades de IT. Debido a que los Controles Generales de IT están embebidos en el ambiente de procesamiento de las aplicaciones, fallos o rupturas en estos tienen un impacto significativo en la efectividad de los Controles de Aplicación. Es importante comprender como afectan los Controles Generales de IT aplicados a través de las actividades de diseño, implementación, operación y mantenimiento de los controles de actividad.

Tipos de Auditoría Informática

Basándonos en los enfoques descriptos en los párrafos anteriores y analizando los aspectos más relevantes a controlar dentro de los Sistemas de Información que posee la organización, podemos presentar un listado, no exhaustivo, de las diferentes tipos de auditorías informáticas que podemos emprender dentro de una organización:

- Auditoría sobre los elementos que componen la Organización Informática y su definición dentro de la organización
- Auditoría sobre la elaboración, aprobación, implementación, actualización y seguimiento del Plan Estratégico de TI
- Auditoría sobre la Arquitectura de la Información, analizando la disponibilidad, oportunidad, integridad y exactitud de los datos
- Auditoría de la creación, documentación, comunicación y actualización de Políticas y Procedimientos sobre las actividades relacionadas con TI
- Auditoria sobre el cumplimiento de la Regulaciones Externas a la organización
- Auditorías sobre las actividades relacionadas con la Administración de Proyectos
- Auditorías sobre las actividades asociadas al Desarrollo, Adquisición y Mantenimiento de Software de Aplicación
- Auditorías sobre las actividades asociadas a la Adquisición y Mantenimiento de la Infraestructura Tecnológica
- Auditoría sobre la elaboración, aprobación, implementación, actualización y cumplimiento de la Política de Seguridad de la Información.
- Auditoría sobre contratación de servicios de Procesamiento y/o Soporte brindados por Terceros
- Auditoría sobre el monitoreo de los Procesos
- Auditoría sobre las Aplicaciones Informáticas

Metodología de Trabajo de la Auditoria Informática

La auditoría informática se realiza dentro del marco de trabajo similar al resto de los tipos de auditorías, con algunas diferencias propias de la actividad que se reflejan sobre todo en la volatilidad de algunos elementos dentro del ámbito de la informática. Dentro de este marco de trabajo es conveniente presentar las fases sobre las que se desenvuelve la actividad de auditoria:

Planeamiento

Si bien existen tres niveles de planificación para la auditoría: estratégica, anual, e individual para cada auditoría; en el presente trabajo nos vamos a concentrar en la etapa de planificación individual de la auditoria. Esta última etapa a su vez puede dividirse en un planeamiento general y uno específico de la auditoria a realizar.

Durante la etapa del planeamiento General se definirá el enfoque de la auditoría, procediéndose a relevar aspectos del sistema de control interno, de los riesgos de auditoría y de la importancia relativa (significatividad) del sector o dependencia a auditar.

El planeamiento Específico es donde se seleccionan los procedimientos, se estiman los recursos humanos y el tiempo requerido necesarios para la ejecución de la auditoría. Por procedimientos se refiere a la confección o selección de aquellos procedimientos de control y sustantivos de auditoría que se aplicarán durante la ejecución del proyecto.

Ejecución

El objetivo de esta fase está orientado a la obtención de evidencias y a la formulación de observaciones con sus respectivas recomendaciones, soluciones y alternativas sobre las áreas y los procesos auditados, aprobados en el plan de auditoría y bajo la metodología del programa de la auditoria. Esto se logra mediante la ejecución de pruebas bajo la aplicación de diversas técnicas y herramientas. Todas las herramientas utilizadas deben permitir la obtención de evidencias suficientes, competentes y pertinentes que demuestren la relevancia de los criterios identificados en la fase

anterior. Los procedimientos de auditoría pueden dividirse según la evidencia que se obtiene, en procedimientos de cumplimiento y sustantivos. En la práctica puede resultar difícil realizar esta distinción ya que muchos cumplen un doble propósito.

- Procedimientos de cumplimiento: Proporcionan evidencia de que los controles claves existen y son aplicados en forma efectiva.
- Procedimientos sustantivos: Proporcionan evidencia directa sobre la validez de las transacciones y los datos que proporciona el sistema de información - registros contables, estados financieros y presupuestarios.

A continuación se presenta un detalle de los procedimientos y técnicas que pueden utilizarse durante la ejecución de una auditoría:

- Relevamiento: Representa el conjunto de actividades encaradas para documentar la forma como se lleva a cabo un procedimiento.
- Revisión: Consiste en el análisis de las características que debe cumplir una actividad, informe, documento, etc. Sirve para seleccionar operaciones que serán verificadas en el curso de la auditoría.
- Confrontación: Consiste en el cotejo de información contenida en registros contra el soporte documental de las transacciones registradas.
- Rastreo: Es utilizado para seguir el proceso de una operación de manera progresiva o regresiva, reconstruyendo el flujo de actividades y controles, a través de la documentación respectiva.
- Observación: Consiste en la verificación ocular de operaciones y procedimientos durante la ejecución de las actividades de la entidad. Se la considera complemento del relevamiento.
- Comparación: Consiste en establecer las diferencias entre las operaciones realizadas y los criterios, normas, procedimientos y prácticas que se utilizan habitualmente.
- Indagación: Consiste en la obtención de manifestaciones mediante entrevistas a funcionarios y empleados o personas relacionadas con las operaciones.

- Encuesta: Se formaliza mediante la utilización de cuestionarios escritos sobre actividades u operaciones objeto de análisis.
- Cálculo: Se trata de la verificación aritmética de comprobantes, documentos, etc., para evaluar su corrección y exactitud.
- Comprobación: Determina la verosimilitud de los actos y la legalidad de las operaciones, autorizaciones, etc. mediante el examen de la documentación respectiva.
- Inspección: Es el examen físico y ocular de ciertos activos tangibles como ser bienes de consumo o de uso, insumos, obras, valores, etc., para comprobar su real existencia y autenticidad.
- Análisis: Es la separación de una operación, procedimiento o actividad en sus elementos componentes, para establecer su conformidad con criterios de orden normativo y técnico.
- Circularización: Procura obtener información directa y por escrito de un sujeto externo a la entidad (persona u organización), que se encuentra en situación de conocer la naturaleza y condiciones de la operación consultada, y de informar válidamente sobre ella.
- Conciliación: Es el examen de la información emanada de diferentes fuentes, con relación a la misma materia, a efectos de verificar su concordancia y determinar de esa manera la validez y veracidad de los registros e informes que se está examinando.
- Determinación de Razonabilidad: Se lleva a cabo a través de la utilización de indicadores o tendencias sobre la evolución de determina-dos comportamientos.

Adicionalmente, se pueden aplicar otros métodos que complementan a los procedimientos y técnicas citados y que constituirán elementos auxiliares para la selección y utilización de los mismos.

Si bien suele confundirse como parte de la etapa de la comunicación del Informe, es en el final de la etapa de ejecución donde se realiza la oportuna comunicación de las observaciones al personal del Auditado involucrado en las mismas, a fin de que presenten sus aclaraciones o comentarios en forma documentada, para su evaluación y consideración en el informe correspondiente. Tan pronto como sea

elaborada una observación de auditoría, el auditor debe comunicarla con el objeto de obtener puntos de vista respecto a las observaciones presentadas y facilitar la oportuna adopción de acciones correctivas.

Al finalizar la fase de ejecución se deberá prestar especial atención que los archivos de papeles de trabajo de la auditoría estén completos. Los papeles de trabajo son los documentos elaborados por el auditor en los que registra el trabajo realizado como consecuencia de los procedimientos aplicados y sirve de soporte al informe de auditoría. Constituyen la evidencia que fundamenta las, observaciones, conclusiones y recomendaciones de auditoría.

Informe

El Informe Final de Auditoría es el medio por el cual se exponen las observaciones, conclusiones y recomendaciones por escrito y que es remitido a distintos funcionarios según corresponda.

El mismo debe contener juicios fundamentados en las evidencias obtenidas a lo largo del examen con el objeto de brindar suficiente información acerca de los desvíos o deficiencias más importantes, así como recomen-dar mejoras en la conducción de las actividades y ejecución de las operaciones. Los objetivos del informe para cada auditoria deben estar definidos apropiadamente en la fase de planeamiento y su estructura general debiera responder a criterios uniformes.

Debe emitirse un informe de auditoría "preliminar" para ser examinado con la Unidad o Dependencia auditada, antes de elevar el informe "final". Durante el tratamiento del informe "preliminar", el auditado tiene la posibilidad de efectuar descargos a las observaciones formuladas, los que serán incluidos en el informe "final" en la medida que se los considere técnicamente pertinentes.

Seguimiento

Si bien el auditor no es el responsable de tomar las acciones para mejorar los controles y/o superar los incumplimientos normativos, su actuación debe propender a la modificación de conductas y al apoyo de la mejora de la gestión. Esto debe verificarse a través del seguimiento

efectivo que lleve a cabo, de las falencias expuestas en los informes anteriormente emitidos. El seguimiento periódico le permitirá al auditor asegurarse respecto de la adopción de medidas adecuadas con relación a los hechos verificados, y si resultan fuente de información para la realización de nuevas auditorías. Al vigilar el cumplimiento de las medidas correctivas, se podrá evaluar no sólo lo acertado del asesoramiento, sino también si los resultados obtenidos de tales soluciones se corresponden con las expectativas.

Resumiendo las fases presentadas y técnicas presentadas en este apartado podemos decir que el método de trabajo del auditor pasa por las siguientes etapas:

1. Definición de Alcance y Objetivos de la Auditoría Informática.
2. Estudio inicial del entorno auditable, tareas preliminares.
3. Determinación de los recursos necesarios para realizar la auditoría.
4. Elaboración de los Programas de Trabajo.
5. Actividades propiamente dichas de la auditoría, tareas de campo.
6. Confección y redacción del Informe Preliminar.
7. Remisión al auditado para que emita su opinión.
8. Confección del Informe Final.

Un último elemento dentro de la metodología presentada es el denominado Riesgo de Auditoría, el cual surge de las eventualidades por las cuales el auditor no pueda detectar error o falsedad en la información que examina o irregularidades en el proceder de los operadores. El riesgo de auditoría tiene tres componentes:

- Riesgo inherente.
- Riesgo de control.
- Riesgo de detección.

Las dos primeras categorías de riesgo se encuentran fuera de control por parte del auditor y son propias de los sistemas y actividades del organismo en cambio, el riesgo de detección está directamente relacionado con las tareas del auditor.

Bibliografía

- "Manual de Control Interno Gubernamental", Sindicatura General de la Nación, 2010
- "Auditing General and Application Controls", S. Anantha Sayana, 2002, ISACA Journal Volume 5
- "Normas de Auditoría Interna Gubernamental", Res 152/2002, Sindicatura General de la Nación
- "Normas de Control Interno para Tecnología de la Información para el Sector Público Nacional", Res 48/2005, Sindicatura General de la Nación
- "Information Technology Assurance Framework" (ITAF), 3ra edición, 2014, ISACA.