NUEVA PERSPECTIVA DE LA AUDITORIA EN TI

- Ángel Lewis Terrero (2016-3553)
- Carlos Ozuna (2016-3633)
- Josue Cayetano (2016-3938)
- Neftalí Lugo Terrero (2016-3825)
- Edison Mancebo (2015-3212)
- Yojansel Cuevas (2016-4391)

GRUPO #2

2. Nueva perspectiva de la auditoria en TI.

El desarrollo de la Informática, y la existencia de un elevado grado de aplicaciones de procesamiento de datos orientados a la gestión, así como su vertiginoso y constante crecimiento, unido a la necesidad de dotar a las organizaciones de un instrumento de control que promueva una beneficiosa expectativa a un costo razonable y eleve constantemente el Control Interno, constituyen la base sobre la que se sustenta el principio de practicar auditorías con el uso de herramientas informáticas y a los sistemas informáticos.

2.1. Fases de la auditoría.

Fase 1: Programación general de las auditorías

Esta fase incluye un análisis integral de todos los componentes internos y externos de la Entidad, con el fin de determinar los procesos que cuentan con mayor relevancia para cumplir con la misión y objetivos estratégicos y los que presentan un alto nivel de riesgo.

Fase 2: Planeación de la Auditoría por procesos

El plan de auditoría es un enunciado, lógicamente ordenado y clasificado, de los procedimientos de auditoría que han de emplearse, el alcance que se les ha de dar y la forma en que se han de aplicar.

Las Normas Internacionales para el Ejercicio Profesional de la Auditoría Interna establecen que los auditores internos deben elaborar un plan para cada trabajo que incluya su alcance, objetivos, tiempo y asignación de recursos

Fase 3: Ejecución de la auditoría por procesos

Se desarrolla el plan de auditoria previamente aprobado, se ejecutan las actividades definidas para obtener y analizar toda la información del proceso que se audita y contar con evidencia suficiente, competente y relevante para emitir conclusiones

Fase 4: Comunicación de resultados de la auditoría

En esta fase se presentan los resultados de la auditoría y se suscriben los planes de acción o mejoramiento.

Fase 5: Seguimiento al cumplimiento de los planes de mejoramiento

Consiste en validar la ejecución de las acciones propuestas en los planes de mejoramiento en las fechas establecidas y valorar su efectividad.

2.2 Planificación de la auditoria en informática

Una persona que quiere auditar, para realizar una buena planificación debe de cumplir una serie de pasos previos que nos permite cumplir con los objetivos de las auditorías planificadas. En ello nos permite saber algunas características de algún negocio o trabajo, por ejemplo, recursos, procedimientos y acciones que se necesitan para realizar el trabajo.

Podemos decir que la planificación es uno de los pasos más importantes ya que realizándolo de una manera inadecuada se obtiene una serie de problemas que nos impediría cumplir con el objetivo, es decir, no conoceríamos el entorno de la empresa en el que se ha de realizar la auditoría, así como los controles asociados y controles de riesgo.

En la planificación debe ser documentada e incluiría:

- El establecimiento de los objetivos y el alcance del trabajo.
- La determinación de los recursos necesarios para realizar la auditoría.
- La realización de una forma más apropiada. Esto quiere decir una evaluación o inspección física que nos permite identificar de las áreas el cual requiere hacer auditoría.
- Obtener la aprobación del plan de trabajo de la auditoria.
- Entre otras cosas.

El caso de la auditoria informática podríamos decir que debemos de realizar una evaluación de los recursos IT y saber cómo son los procesos de datos de cada sistema.

Cuando queremos lograr una planificación adecuada lo primero que debemos de obtener es la información general de la empresa y las funciones tecnológicas o función de informática de acuerdo a las evaluaciones.

El proceso de planeación comprende el establecer:

- Metas.
- Informes de actividades.
- Programa de trabajo de auditoría.
- Planes de contratación personal y presupuesto financiero.

2.3 Revisión preliminar

En esta fase el auditor debe de armarse de un conocimiento amplio del área que va a auditar, los objetivos que debe cumplir, tiempos (una empresa no pude dejar sus equipos y personal que lo opera sin trabajar porque esto le genera pérdidas sustanciosas), herramientas y conocimientos previos, así como de crear su equipo de auditores expertos en la materia con el fin de evitar tiempos muertos a la hora de iniciar la auditoria

La revisión preliminar significa la recolección de evidencias por medio de entrevistas con el personal de la instalación, la observación de las actividades en la instalación y la revisión de la documentación preliminar.

El primero paso en el desarrollo de la auditoria, después de la planeación, es la revisión preliminar del área de informática. el objetivo de la revisión preliminar es el de obtener la información necesaria para que el auditor pueda tomar la decisión de cómo proceder en la auditoria.

2.4 Revisión Detallada

Los objetivos de la fase detallada son los de obtener la información necesaria para que el auditor tenga un profundo entendimiento de los controles usados dentro del área de informática.

El auditor debe decidir si debe continuar elaborando pruebas de consentimiento, con la esperanza de obtener mayor confianza por medio del sistema de control interno, o proceder directamente a la revisión con los usuarios (pruebas compensatorias), o a las pruebas sustantivas.

En las fases de evaluación detallada es importante para el auditor identificar las causas de las pérdidas existentes dentro de la instalación y los controles para reducir las pérdidas existentes dentro de la instalación y los controles para reducir las pérdidas y los efectos causados por éstas. Los métodos de obtención de información al momento de la evaluación detallada son los mismos usados en la investigación preliminar, y lo único que difiere es la profundidad con que se obtiene la información y se evalúa.

Como en el caso de la investigación preliminar, se tienen diferentes formas de lograr los objetivos desde el punto de vista del auditor interno o externo. El auditor interno debe considerar las causas de las pérdidas que afectan la eficiencia y eficacia. Este debe evaluar si los controles escogidos son óptimos.

Si el auditor interno considera que los controles internos del sistema no son satisfactorios, en lugar de proceder directamente a revisar, a probar los controles alternos o a realizar pruebas sustantivas y procedimientos, debe señalar las recomendaciones para mejorar los controles de los sistemas.

2.5 Examen y Evaluación de la Información

Los auditores internos deberán obtener, analizar, interpretar y documentar la información para apoyar los resultados de la auditoría.

El proceso de examen y evaluación de la información es el siguiente:

- Se debe obtener la información de todos los asuntos relacionados con los objetivos y alcances de la auditoría.
- La información deberá ser suficiente, competente, relevante y útil para que proporcione bases sólidas en relación con los hallazgos y recomendaciones de la auditoría.
- Los procedimientos de auditoría, incluyendo el empleo de las técnicas de pruebas selectivas y el muestreo estadístico, deberán ser elegidos con anterioridad, cuando esto sea posible, y ampliarse o modificarse cuando las circunstancias lo requieran.
- El proceso de recabar, analizar, interpretar y documentar la información deberá supervisarse para proporcionar una seguridad razonable de que la objetividad del auditor se mantuvo y que las metas de auditoría se cumplieron.
- Los documentos de trabajo de la auditoría deberán ser preparados por los auditores y revisados por la gerencia de auditoría.

Los auditores deberán reportar los resultados del trabajo de auditoría. El auditor deberá discutir las conclusiones y recomendaciones en los niveles apropiados de la administración antes de emitir su informe final.

Los informes pueden incluir recomendaciones para mejoras potenciales y reconocer el trabajo satisfactorio y las medidas correctivas.

2.6 Pruebas de consentimiento

El objetivo de la fase de prueba de consentimiento es el de determinar si los controles internos operan como fueron diseñados para operar. El auditor debe determinar si los controles declarados en realidad existen y si realmente trabajan confiable.

Además de las técnicas manuales de recolección de evidencias, muy frecuente al auditor debe recurrir a técnicas de recolección de información asistidas por computadora, para determinar la

existencia y confiabilidad de los controles. Por ejemplo, para evaluar la existencia y confiabilidad de los controles de un sistema de red, se requerirá al entrar a la red y evaluar directamente al sistema.

2.7 Pruebas de controles del usuario

En algunos casos el auditor puede decidir el no confiar en los controles internos dentro de las instalaciones informáticas, porque el usuario ejerce controles que compensan cualquier debilidad dentro de los controles internos de la informática. Estas pruebas que compensan las deficiencias de los controles internos se pueden realizar mediante cuestionarios, entrevistas, vistas y evaluaciones hechas directamente con los usuarios.

2.8 Pruebas Sustantivas

Son realizadas para obtener evidencia de auditoría, con respecto a si las aseveraciones de los estados financieros carecen de errores significativos. Dentro de ellas se aplican las pruebas sustantivas de detalle y procedimientos analíticos sustantivos.

Este tipo de estas pruebas es conseguir suficientes pruebas que puedan permitir al auditor poder emitir su propio juicio sobre cuando pueden ocurrir desventajas o pérdidas materiales en medio del proceso de la información.

- **¿Como se realiza la prueba?**

El auditor externo informa los resultados en forma de una opinión sobre cuando puede existir un proceso erróneo o que pueda haber falta de información.

En la auditoria podemos identificar ocho diferentes pruebas sustantivas:

1. Pruebas para identificar errores en el procesamiento o de falta de seguridad o confidencialidad.
2. Prueba para asegurar la calidad de los datos.
3. Pruebas para identificar la inconsistencia de datos.

4. Prueba para comparar con los datos o contadores físicos.
5. Confirmación de datos con fuentes externas.
6. Pruebas para confirmar la adecuada comunicación.
7. Prueba para determinar falta de seguridad.
8. Pruebas para determinar problemas de legalidad.

2.9 Evaluación de los sistemas de acuerdo al riesgo

Una de las formas de evaluar la importancia que puede tener para la organización de un determinado sistema, es considerar el riesgo que implica el que no sea utilizado adecuadamente, la pérdida de la información o bien el que sea usado por personal ajeno a la organización.

Algunos sistemas de aplicaciones son de más alto riesgo que otros debido a que:

• Son susceptibles a diferentes tipos de pérdida económica. Ejemplo: Fraudes y desfalcos entre los cuales están los sistemas financieros.

• Las fallas pueden impactar grandemente a la organización. Ejemplo: Una falla en el procesamiento de la nómina puede tener como consecuencia una huelga.

• Potencialmente, alto riesgo debido a daños en la competencia. Algunos sistemas le dan a la organización un nivel competitivo muy alto dentro del mercado. Ejemplo: Sistemas de planeación estratégica. Patentes. Derechos de autor, los cuales son las mayores fuentes de recursos de la organización. Otros a través de los cuales su pérdida puede destruir la imagen de la organización.

• Sistemas de alto costo. Sistemas que son muy costosos de desarrollar, los cuales son frecuentemente sistemas complejos que pueden presentar muchos problemas de control.

2.10 Investigación Preliminar

Se deberá observar el estado general del área, su situación dentro de la organización, si existe la información solicitada, si es o no necesaria y la fecha de su última actualización.

Se debe hacer la investigación preliminar solicitando y revisando la información de cada una de las áreas basándose en los siguientes puntos:

ADMINISTRACIÓN

Se recopila la información para obtener una visión general del departamento por medio de observaciones, entrevistas preliminares y solicitud de documentos para poder definir el objetivo y alcances del departamento.

Para analizar y dimensionar la estructura por auditar se debe solicitar a nivel del área de informática

Objetivos a corto y largo plazo.

Recursos materiales y técnicos

Solicitar documentos sobre los equipos, número de ellos, localización y características.

Estudios de viabilidad.

Número de equipos, localización y las características (de los equipos instalados y por instalar y programados)

Fechas de instalación de los equipos y planes de instalación.

Contratos vigentes de compra, renta y servicio de mantenimiento.

Contratos de seguros.

Convenios que se tienen con otras instalaciones.

Configuración de los equipos y capacidades actuales y máximas.

Planes de expansión.

Ubicación general de los equipos.

Políticas de operación.

Políticas de uso de los equipos.

SISTEMAS

Descripción general de los sistemas instalados y de los que estén por instalarse que contengan volúmenes de información.

Manual de formas.

Manual de procedimientos de los sistemas.

Descripción genérica.

Diagramas de entrada, archivos, salida.

Salidas.

Fecha de instalación de los sistemas.

Proyecto de instalación de nuevos sistemas.

En el momento de hacer la planeación de la auditoria o bien su realización, debemos evaluar que pueden presentarse las siguientes situaciones.

Se solicita la información y se ve que:

No tiene y se necesita.

No se tiene y no se necesita.

Se tiene la información, pero:

No se usa.

Es incompleta.

No esta actualizada.

No es la adecuada.

Se usa, está actualizada, es la adecuada y está completa.

En el caso de No se tiene y no se necesita, se debe evaluar la causa por la que no es necesaria. En el caso de No se tiene pero es necesaria, se debe recomendar que se elabore de acuerdo con las necesidades y con el uso que se le va a dar. En el caso de que se tenga la información pero no se utilice, se debe analizar por que no se usa. En caso de que se tenga la información, se debe analizar si se usa, si está actualizada, si es la adecuada y si está completa.

El éxito del análisis crítico depende de las consideraciones siguientes:

Estudiar hechos y no opiniones (no se toman en cuenta los rumores ni la información sin fundamento)

Investigar las causas, no los efectos.

Atender razones, no excusas.

No confiar en la memoria, preguntar constantemente.

Criticar objetivamente y a fondo todos los informes y los datos recabados.

2.11 Personal participante

Una de las partes más importantes en la planeación de la auditoria en informática es el personal que deberá participar, ya que se debe contar con un equipo seleccionado y con ciertas características que puedan ayudar a llevar la auditoria de manera correcta y en el tiempo estimado.

Para complementar el grupo, como colaboradores directos en la realización de la auditoria, se deben tener personas con las siguientes características:

- □ Técnico en informática.
- □ Conocimientos de Admón., contaduría y finanzas.
- □ Experiencia en el área de informática.
- □ Experiencia en operación y análisis de sistemas.
- □ Conocimientos y experiencias en psicología industrial.
- □ Conocimientos de los sistemas operativos, bases de datos, redes y comunicaciones, dependiendo del área y características a auditar.
- □ Conocimientos de los sistemas más importantes.