

2017

AUDITORÍA DE SISTEMAS DE INFORMACIÓN ORGANIZACIONAL

FUNDAMENTOS DE INGENIERÍA ADMINISTRATIVA
MARIELA DENISSE REBOLLO ALTAMIRA

INSTITUTO TECNOLÓGICO DE ORIZABA | MAESTRÍA EN INGENIERÍA ADMINISTRATIVA

TODO BAJO CONTROL

AUDITORÍA

(FCA-UNAM, 2008) explica que el concepto de auditoría se puede entender como el examen de los estados financieros de una entidad, con el objeto de que el responsable emita una opinión sobre la razonabilidad de las cifras que de ellos emanen.

Sin embargo, (García, 2001) nos dice que con frecuencia la palabra auditoria se ha empleado incorrectamente y se le ha considerado como una evaluación cuyo único fin es detectar errores y señalar fallas, debido a eso se ha llegado a usar la frase “tiene auditoria” como sinónimo de que, desde antes de realizarse, ya se encontraron fallas y por lo tanto se está haciendo la auditoria.

Por lo que este autor nos indica que la auditoria no solo se encarga de detectar errores, sino que es el examen crítico que se realiza con objeto de evaluar la eficiencia y eficacia de una sección o de un organismo, y determinar recursos alternativos de acción para mejorar la organización y lograr los objetivos propuestos.

Por otra parte, este autor señala que según el Nuevo Diccionario Español Sopena dice que la auditoria se desarrolla con base en normas, procedimientos y técnicas definidas formalmente por institutos establecidos a nivel nacional e internacional; la palabra auditoria proviene del latín “auditorius”, y que de esta proviene “auditor”, el que tiene la virtud de oír; definiendo justamente que el auditor es el “revisor de cuentas colegiado.

Auditoria es un proceso sistemático, independiente y documentado para obtener registros, declaraciones, de hechos o cualquier otra información pertinente verificable y de utilidad, para ser evaluada a fin de determinar la extensión en que se cumple el conjunto de políticas, procedimiento o requisitos que se tienen como

Hecho por: L.A Mariela Denisse Rebollo Altamira

Asesor: Dr. Fernando Aguirre y Hernández

referencia para comparar las evidencias para comparar las evidencias objetivas aludidas (Galindo, 2013).

(Brito & Solís, 2008) explican que las razones principales para mantener un adecuado Sistema de Control Interno dentro de una organización son las siguientes:

- Mantener un eficiente control administrativo
- Cumplir con las exigencias gubernamentales
- Cumplir con la responsabilidad de presentar información financiera confiable a terceros.

En conclusión, de las anteriores definiciones de auditoría, se puede decir que ésta es una herramienta de control mediante la cual se lleva a cabo una revisión profunda y exhaustiva de todos los procesos, políticas y normas de una empresa para verificar que estos se realicen de acuerdo a lo establecido. Esta se lleva a cabo con la finalidad de detectar oportunamente errores, evaluar la eficiencia y eficacia de la sección auditada dentro de la organización. Con la auditoria se espera que el encargado de realizarla emita recomendaciones para que la organización labore eficientemente y así lograr que sus procedimientos sean totalmente aptos para sus funciones.

CLASIFICACIÓN DE LOS TIPOS DE AUDITORÍA

(Galindo, 2013) explica que la auditoría se clasifica en:

1. AUDITORIA POR LA PROCEDENCIA DEL AUDITOR
 - a. Auditoría externa
 - b. Auditoría interna
2. AUDITORIA POR SU AREA DE APLICACIÓN
 - a. Auditoría financiera
 - b. Auditoría administrativa
 - c. Auditoría gubernamental
 - d. Auditoría informática
3. AUDITORIA INFORMATICA
 - a. Auditoría con la computadora
 - b. Auditoría sin la computadora
 - c. Auditoría a la gestión informática
 - d. Auditoría al sistema de cómputo
 - e. Auditoría alrededor de la computadora
 - f. Auditoría de la seguridad de sistemas computacionales
 - g. Auditoría a los sistemas de redes
 - h. Auditoría integral a los centros de cómputo
 - i. Auditoría ISO-9000 a los sistemas computacionales
 - j. Auditoría outsourcing
 - k. Auditoría ergonómica de sistemas computacionales

SISTEMAS DE INFORMACIÓN

(Rodríguez, 2014) argumenta que los sistemas de información han tenido un profundo desarrollo desde la década de los 50 hasta hoy en día , con el paso del tiempo se han convertido en una valiosa herramienta dentro de las organizaciones, y así mejorar la eficiencia y aumentando la productividad.

Hoy en día no existen empresas públicas o privadas que no realicen sus actividades mediante el uso de un computador. La revolución tecnológica ha sugerido la necesidad de asegurarse de que dichos sistemas de información sean lo más precisos y confiables sobre todo en procesamientos de información financiera. Uno de los principales desafíos de la auditoria moderna es el de evaluar y controlar de forma adecuada y eficiente la gestión empresarial utilizando las herramientas informáticas.

(Brito & Solís, 2008; Rodríguez, 2014) argumentan que un sistema de información (SI) puede definirse como el conjunto de elementos o componentes entre sí en el que se puede ingresar, almacenar, presentar la información para la oportuna y eficiente toma de decisiones. Al hablar de sistemas de información no precisamente se refiere a computadoras ni informática.

Existen cuatro grupos de SI de acuerdo a los niveles jerárquicos de la organización:

1. Sistemas de nivel operativo: directamente relacionados con los procesos operacionales y transaccionales de una organización. Dentro de este nivel se encuentran los sistemas de procesamiento de transacciones. Se caracterizan por ser de uso fácil, realizan procesos transaccionales sencillos, las consultas y reportes son limitados en su estructura y sus usuarios son los empleados y jefes del nivel primario de la organización.
2. Sistemas de nivel de conocimiento: se relacionan con el nivel secundario de la organización, el propósito de estos sistemas consiste en ayudar a

Hecho por: L.A Mariela Denisse Rebollo Altamira

Asesor: Dr. Fernando Aguirre y Hernández

desarrollar, procesar, ordenar e interrelacionar el flujo de información y nuevos conocimientos de la organización.

3. **Sistemas de nivel administrativo:** se enfocan hacia actividades de monitoreo, dirección, control y toma de decisiones de los jefes de nivel medio, aquí se encuentran los sistemas de apoyo a decisiones tales como los sistemas de análisis de costos, análisis de producción, análisis de ventas, rentabilidad, se caracterizan por presentar información periódica para análisis y por lo general relacionan variables de carácter interno y externo para producir resultados que ayuden a la gerencia a tomar decisiones eficaces y oportunas.
4. **Sistemas de nivel estratégico:** apoyan en la toma de decisiones del nivel estratégico a largo plazo, considerando las políticas y metas propuestas relacionando con el ambiente externo de la organización de tal forma que se pueden tomar decisiones que mejoren la competitividad. Son fáciles de usar, flexibles y no requieren que el usuario posea complejos conocimientos de informática para poder hacer uso de ellos. Su característica principal es el análisis de datos provenientes de los otros sistemas (transaccionales y administrativos) mediante el modelado de tablas o cubos de información, en el cual, se obtienen cuadros y resúmenes de información fáciles de usar.

Las organizaciones dependen de sistemas de información, de tal forma que las estrategias y la planificación organizacional estarán dadas en función de la capacidad de crecimiento, flexibilidad y capacidad de sus SI.

La incorporación de tecnología de información dentro de los procesos productivos de una organización puede convertirse en una ventaja competitiva, permiten ser más eficientes y darles la capacidad de desarrollar productos y servicios a menor calidad.

AUDITORÍA INFORMÁTICA

(Rodríguez, 2014) nos explica que la gestión del conocimiento no es algo nuevo, son muchas las empresas que en los últimos años han buscado implementar programas con el fin de conseguir tal objetivo, las empresas han optado por tecnologías de la información y las diferentes soluciones que brinda el software han estado dando de qué hablar.

Sin embargo, la mayoría de estos programas se han enfocado en la implantación de intranets que intentan facilitar la comunicación entre las personas y documentar todos los procesos de la organización. Además de poner a disposición de dos empleados las estadísticas e indicadores de la evaluación.

Es evidente que el conocimiento es muy difícil de gestionarse, pero la información con la que se cuenta si puede ser gestionada. Por tal motivo la información tiene un papel relevante y la hace una estrategia base de gestión de conocimiento.

La adecuada gestión de la información es un elemento indispensable. Las empresas han incorporado tecnologías de información como parte de su eje de sistemas de información, hasta el grado de compáralo con un sistema informático de la empresa, sin embargo, pocas veces ha sido llevada a cabo en forma correcta.

La Auditoría de la Información o Informática es un proceso que ayuda a detectar, controlar y evaluar la información existente en una organización y los flujos de esta, el uso que hacen de la información y la adecuación a las necesidades dl personal. De esta manera se resolverá la incertidumbre de con lo que cuenta la organización y donde está establecida, esto ayudará a:

- Duplicidades: se refiere a las unidades de una misma organización que algunas veces se mantiene la misma información de forma independiente.

Hecho por: L.A Mariela Denisse Rebollo Altamira

Asesor: Dr. Fernando Aguirre y Hernández

- Carencias: en ocasiones si no se comparte la información se detectan vacíos que son perjudiciales al correcto funcionamiento de determinadas unidades de negocio dentro de la entidad.
- Inconsistencias: mantener la misma información de modo independiente puede dar lugar a informaciones dispares.

La auditoría también permite diagnosticar que uso se hace de la información y en definitiva la importancia que se le otorgue. Esto dará la posibilidad de conocer quien la usa en cada caso y para qué fin, así se podrá identificar puntos críticos de la cadena de valor donde el uso de esta información es esencial.

Por otro lado, (Brito & Solís, 2008) argumentan que el control interno informático es un subsistema dentro del sistema de control interno de la organización y comprende todos los procesos administrativos y sistematizados dentro de una organización, cuyo objetivo es garantizar el control y seguridad de los recursos informáticos para una eficiente, efectiva y económica gestión operacional.

Los objetivos del control interno informático, podría dividirse en generales y específicos.

Entre los objetivos generales tenemos:

- El cumplimiento de las políticas y procedimientos establecidos por la alta gerencia y demás normativas legales relacionadas con el uso de la tecnología.
- Servir como apoyo a la alta gerencia para el control de los recursos informáticos y como pistas de auditoría para la función de auditoría interna o los auditores externos.
- Garantizar una adecuada gestión de la función PED, la calidad del servicio informático y la satisfacción de los usuarios.

Mientras que entre los objetivos específicos tenemos:

- El cumplimiento de la planeación informática de la organización.

Hecho por: L.A Mariela Denisse Rebollo Altamira

Asesor: Dr. Fernando Aguirre y Hernández

- Mantener el control de los cambios realizados a los Sistemas de información.
- Asegurar el acceso a la información solo a personal autorizado.
- Asegurar la calidad de desarrollo y mantenimiento de los sistemas de información.
- Proteger los sistemas contra ataques informáticos provenientes desde el internet (hackers) y minimizar el riesgo de infección por virus.
- Mantener en orden las licencias y contratos por el uso de sistemas y aplicativos.

Existen diversas metodologías para la implementación de controles informáticos, basadas en diferentes estándares a nivel internacional, se las puede clasificar en dos grandes grupos: cuantitativas y cualitativas.

1. Metodologías cuantitativas: se basan en el uso de modelos matemáticos para el análisis de riesgos, en el que se asigna a cada riesgo una probabilidad de ocurrencia. Luego utilizando simulaciones sofisticadas se puede establecer el grado de riesgo al que está expuesta la organización y los controles a implementarse para la disminución de riesgo.
2. Metodologías cualitativas: se basan en la experiencia y capacidad del profesional a cargo de la implementación de los controles informáticos. Ésta utiliza métodos estadísticos no sofisticados para identificar las posibles amenazas dentro de la organización para luego seleccionar los mecanismos de respuestas a tales amenazas.

En conclusión, la auditoría informática es la revisión sistematizada de los sistemas computacionales, hardware, software e información de una organización, así como del entorno: área de trabajo, redes y telecomunicaciones, con el propósito de salvaguardar la integridad de los datos. El auditor encargado de realizar este tipo de auditoría debe ser un experto en el área de sistemas computacionales el cual evalúa y comprueba los controles y procedimientos informáticos más complejos, desarrollando y aplicando técnicas de auditoría para verificar la eficacia, utilidad, fiabilidad y seguridad de los equipos e información.

FASES DE LA AUDITORÍA DE LA INFORMACIÓN

(Serrano & Zapata, 2003) nos describen las fases de la auditoría de la información de la siguiente manera:

1. Planificación: en esta etapa se definen los objetivos, el punto de partida y hasta donde se desea llegar, las tareas que se realizan en esta etapa contemplan la de identificar las personas clave, la magnitud del proyecto y la localización de recursos, se desarrolla el plan de acción para la implementación, un plan estratégico y un plan de negocio.
2. Colección de datos: en esta etapa se prepara la información que se va a recibir, se desarrollan bases de datos, entrevistas, etc.
3. Evaluación de datos: se localizan vacíos y duplicados, servirá para interpretar el flujo de información, evalúa los problemas, formula recomendaciones y se desarrolla un plan de acción para el cambio. Una vez que se pasó la etapa anterior se deben comunicar las recomendaciones para atender las irregularidades detectadas y explicar el trabajo realizado, así el entorno organizacional y corporativo tendrá información de los resultados.
4. Implantar las recomendaciones: se debe desarrollar un programa de implementación, se deben incorporar los cambios en los planes formales y desarrollar la estrategia de post implementación. Una vez que se realizaron los cambios se debe ser consciente de la necesidad de un seguimiento continuo, medir y valorar los cambios y planificar un ciclo de auditoría de información cíclica.

AUDITORÍA INFORMÁTICA EN LAS ORGANIZACIONES

(Galindo, 2013) argumenta que el control interno informático y su auditoría permiten gestionar y rentabilizar los sistemas de información de la forma más eficiente, optimizando, en suma, resultados.

El autor nos menciona que en la actualidad existen tres tipos de metodologías de Auditoría Informática:

1. R.O.A. (RISK ORIENTED APPROACH) diseñada por Arthur Andersen.
2. CHECKLIST o cuestionarios.
3. AUDITORIA DE PRODUCTOS (por ejemplo, Red Local Windows NT; sistemas de Gestión de base de Datos DB2; Paquete de seguridad RAFC, etc.).

Las tres metodologías están basadas en la minimización de los riesgos, que se conseguiría en función de que existan los controles y de que estos funcionen. En consecuencia, el auditor deberá revisar estos controles y su funcionamiento.

De estas tres metodologías, la más adecuada a la Auditoría de las PyMes es la de CHECKLIST. En conclusión, es necesario que para se alcancen resultados homogéneos es importante que el personal más experto en el tema de auditoría adecue o tome en cuenta los puntos de la auditoría para así lograr el resultado homogéneo esperado.

METODOLOGÍA CHECKLIST

(Galindo, 2013) explica que el checklist o lista de verificación es uno de los métodos de recopilación y evaluación de auditoría más sencillos, más cómodos y más fáciles de utilizar, debido a la simplificación de su elaboración, la comodidad de su aplicación y por la facilidad para encontrar desviaciones, lo cual hace una de las herramientas más confiables y utilizables para cualquier revisión de sistemas computacionales; así mismo se aplica tanto para el área de sistemas, para la gestión administrativa o para cualquier otra función informática.

Esta herramienta consiste en la elaboración de una lista ordenada, en la cual se anotan todos los aspectos que se tiene que revisar del funcionamiento de un sistema, de sus componentes, del desarrollo de una actividad, del cumplimiento de una operación o de cualquier otro aspecto relacionado con la evaluación con el área de sistemas; esta lista se complementa con una o varias columnas en las que se califica el cumplimiento del aspecto evaluado. Por lo general se palomea el cumplimiento, se tacha el incumplimiento o se deja en blanco. Con esto se identifica a simple vista el cumplimiento o incumplimiento del aspecto evaluado.

La lista de verificación (checklist) puede ser diseñada en dos columnas: el concepto y el cumplimiento o incumplimiento, o en varias columnas: una para el concepto y las otras para elegir una calificación representada en cada columna según el grado de cumplimiento del concepto.

El checklist es una técnica muy utilizada en el campo de la auditoría informática. No es más que una lista de comprobación o cuestionario, que sigue unas pautas determinadas dependiendo de qué estemos evaluando o qué objetivos queramos alcanzar.

Hecho por: L.A Mariela Denisse Rebollo Altamira

Asesor: Dr. Fernando Aguirre y Hernández

El auditor crea un checklist para evaluar un sistema informático (ya sea de una empresa, de un comercio, de un particular...) y sacar conclusiones, guiándose por las respuestas que el cliente ha dado a través del cuestionario o checklist.

Principalmente existen dos tipos de checklists, dependiendo del tipo de respuesta que haya que dar a las preguntas que se plantean.

1. Checklist de Rango: En las respuestas el cliente tendrá que introducir un número dentro de un rango dado, como, por ejemplo, a la pregunta de que si está satisfecho con el trabajo de los empleados de la empresa deberá responder con una puntuación que estará entre un mínimo y un máximo. El rango de respuesta podrá variar, dependiendo del auditor o de la pregunta que se formule (En nuestra herramienta, 0 si no está nada de satisfecho y 5 el máximo).
2. Checklist binario: Este tipo es de respuestas verdadero y falso (1 y 0 respectivamente). Solamente se podrá contestar con esos dos valores independientemente de cual sea la pregunta (Auditoria informática, 2007).

En conclusión, el checklist o lista de verificación es una herramienta diseñada para la recolección de información, la cual ayuda al auditor para simplificar a facilidad de encontrar desviaciones en la revisión del área de sistemas computacionales. Este tipo de método consiste en la elaboración de una lista ordenada de todos los aspectos que se tienen que revisar del funcionamiento de un sistema tales como son: la revisión de sus componentes, el desarrollo de una actividad, del cumplimiento de una operación o de cualquier otro aspecto relacionado con la evaluación del área de sistemas.

Una lista de verificación puede ser diseñada en dos tipos de formato, el primero es el de dos columnas o también denominada checklist binario y el segundo el diseñado en varias columnas conocido también como checklist de rango, los cuales tienen la finalidad de recolectar información.

EJEMPLOS DE METODOLOGÍA CHECKLIST

Verificar el funcionamiento y cumplimiento adecuado de la red de cómputo, así como la inclusión de sus componentes, su aplicación y uso.	
Descripción del concepto	Cumple
La instalación de la red es flexible y adaptable a las necesidades de la empresa.	
La lista de componentes de la red contiene todo el hardware requerido para su funcionamiento adecuado.	
La lista de componentes de la red contienen todo el software requerido para su funcionamiento adecuado.	
La red de cómputo es aprovechada al máximo en la empresa.	
La configuración de recursos de la red es la mejor para el uso correcto de los sistemas computacionales de la empresa.	
Existen niveles y seguridad en la red.	

Figura: Ejemplo de Chequeo de dos columnas.

Fuente:(Galindo, 2013)

Verificar la seguridad en el centro de cómputo y calificar cada concepto según su grado de cumplimiento.				
Descripción del concepto	100% Excelente	80% Cumple	60% Mínimo	40% Deficiente
1.- Evaluación en la seguridad en el acceso al sistema				
Evaluar los atributos de acceso al sistema				
Evaluar los niveles de acceso al sistema				
Evaluar la administración de contraseñas del sistema				
2.- Evaluación en la seguridad en el acceso al área física				
Evaluar el acceso del personal al centro de				

Hecho por: L.A Mariela Denisse Rebollo Altamira

Asesor: Dr. Fernando Aguirre y Hernández

cómputo				
Evaluar el acceso de los usuarios y terceros al centro de cómputo				
Evaluar la administración de la bitácora de acceso físico al área de sistemas.				

Figura: Ejemplo de Chequeo de varias columnas.

Fuente:(Galindo, 2013)

AGRADECIMIENTOS Y TEMA DE TESIS

Agradezco a Dios por todas sus bendiciones, igualmente por la oportunidad de trabajar en el proceso de mejorarme a mí misma. Agradezco a mis padres por apoyarme en todo momento en esta nueva aventura, al Consejo Nacional de Ciencia y Tecnología por su apoyo en mis estudios de posgrado, al Instituto Tecnológico de Orizaba, a la Maestría de Ingeniería Administrativa, así como a la materia de Fundamentos de Ingeniería Administrativa, por proporcionarme las bases necesarias para ser mejor como profesionista y ser humano.

Tema: Implementación de Auditorías en Sistemas de Información Organizacionales como herramienta para incrementar la competitividad de la organización.

Objetivo: Implementar auditorías en sistemas de información organizacional para incrementar la efectividad, competitividad y productividad de la organización.

REFERENCIAS CONSULTADAS

Brito, J., & Solís, G. (2008). Análisis y Aprovechamiento de los Sistemas de Información para una eficiente auditoría control de gestión. Recuperado a partir de

<https://www.dspace.espol.edu.ec/bitstream/123456789/1901/1/3786.pdf>

FCA-UNAM. (2008, agosto). Auditoría en Informática. Recuperado a partir de

http://fcasua.contad.unam.mx/apuntes/interiores/docs/98/8/audi_infor.pdf

Galindo, M. A. (2013). *La auditoría informática en las PyMES*. Recuperado a partir de

<http://cdigital.uv.mx/handle/123456789/34459>

García, J. A. E. (2001). *Auditoría en informática*. McGraw-Hill.

Rodríguez, N. (2014). Auditoría de los Sistemas de Información Organizacional. Recuperado a partir de

<http://www.auditorescontadoresbolivia.org/archivos/3.auditoriadelossistemasdeinformacionorganizacionalimportancia.pdf>

Serrano, S., & Zapata, M. (2003). Auditoría de la información, punto de partida de la gestión del conocimiento. *El Profesional de La Información*, 12(4), 290–297.