UNIVERSIDAD

GOBERNABILIDAD DE TI UNIDAD 3

Autores: ZULLY CARVAJAL

Fecha: 5 de octubre 2018

Materia: Electiva de Profundización III

Tabla de contenido

Pg.

Introducción 1

Definiciones2

Fundamentos de la Auditoria3

Control Interno de TI5

Riesgos y Controle6

Niveles de riesgo según Pricewaterhouse Coopers 5

Metodologías, técnicas y herramientas de auditoría de TI 4

Metodologías que apoyan el control interno de TI 5

Plan De Contingencias6

El informe de auditoría4

El código de ética5

Esquema del documento de auditoría6

Características del informe de auditoría5

Construcción del informe de auditoría 5

Conclusiones del informe de auditoría 5

Conclusión4

Bibliografía4

INTRODUCCION

Las empresas y los gobiernos dependen hoy en día de las tecnologías de información (TI) para su funcionamiento y desarrollo. Hacen enormes esfuerzos e inversiones en TI con el objetivo de ser más eficientes, más seguras, cumplir con su misión y con los aspectos claves de su planeación estratégica. Infortunadamente muchas de ellas funcionan como silos, aisladas unas de otras, las divisiones no se comunican y los esfuerzos de un área son desconocidos o entorpecidos por otras.

Por ello la relevancia de hacer una conveniente planeación y verificar que se preserve el valor generado por negocio y sus inversiones. Los procesos de auditoría de TI deben realizarse por una persona, empresa u organización, que mantenga una posición independiente de los auditados.

A continuación, se dará una breve definición de auditoria, sus procesos, sus metodologías, técnicas y herramientas, además de la documentación que se debe realizar.

DEFINICIONES

- Auditoria TI:

"*La auditoría es un proceso de apoyo estratégico a la organización a través del cual es posible medir, revisar y evaluar el nivel de cumplimiento y desempeño de eventos, procedimientos, actividades u objetos que se aborden.*

De igual forma, brinda la posibilidad de conocer su estado y avance de acuerdo con lo establecido en sus planes, proporcionando una fotografía de dicho estado, es decir, de su estado actual y real, con base en la evaluación de este estado respecto al esperado o deseado."

(Alarcon, 2014)

- Plan de contingencias:

"*Una estrategia previamente planificada que coordina las actividades para restaurar de manera progresiva y ágil los servicios de TI de una organización, que se han visto detenidos o interrumpidos de forma total o parcial, afectando por ende el funcionamiento de la organización*"

(Alarcon, 2014)

- PriceWaterhouseCoopers

"*Es una de las empresas más grandes del mundo que brinda servicios profesionales de consultoría, auditoría, outsourcing, entre otros*."

(Alarcon, 2014)

FUNDAMENTOS DE LA AUDITORÍA DE TI

Como se muestra en la definición de este documento, la auditoria (TI), es una actividad de control que comprende la evaluación de las Tecnologías de Información (TI), dentro de una organización, está basada en buenas prácticas y normas nacionales e internacionales, que son utilizadas para revisar y calificar el diseño, desempeño y cumplimiento de los controles realizados en el ambiente de TI.

Es el de evaluar e identificar las fallas que hay en el sistema y dar opiniones de como corregirlas y procurar que se cumplan los procesos y se alcancen los objetivos y metas de la organización. Para conseguir que los medios sean eficaces y rentables y con esto poder tener un buen manejo de la información y esta pueda ser solicitada en cualquier momento y esté disponible.

Dentro de la auditoria Ti, existen varias certificaciones para controlar el seguimiento de las acciones, actividades y el progreso de los proyectos a la hora de realizar un proyecto dentro de la empresa respecto a las Ti. Las cuales son:

- *CISA - Certified Information Systems Auditor* (Alarcon, 2014)
- *CISM - Certified Information Security Manager* (Alarcon, 2014)
- *CGEIT - Certified in the Governance of Enterprise IT* (Alarcon, 2014)
- *CRISC - Certified in Risk and Information Systems Control* (Alarcon, 2014)

Estas certificaciones ayudan al auditor, a la hora de implementar proyectos en la empresa. Sin embargo, cualquier empresa necesita la implementación de métodos de auditoría, cuyo principal objetivo es alcanzar la transparencia financiera y económica de la empresa frente a la sociedad.

A continuación, observaremos algunas de las características más usuales de la auditoría: *Base de datos, Calidad, Dirección, Financiera, Gestión, Información, Redes y Seguridad*. (Alarcon, 2014)

Vale la pena mencionar, que sea cual sea el tipo de auditoria que se realice, su principal objetivo siempre será el de revisar y evaluar los hechos, fenómenos y operaciones que realiza una empresa u organización, para que estas se desarrollen de acuerdo a como fueron planeados, que de igual modo se respetan las políticas y lineamientos establecidos y además se cumple con todas obligaciones fiscales y jurídicas en general.

Control Interno De Ti

"Este va de la mano con el de proceso de auditoría, teniendo en cuenta que contribuyen como mecanismos de control en el seguimiento y evaluación de los procesos, y en la definición de acciones que permitan reducir las fallas, problemas y el incumplimiento de los objetivos estratégicos de la organización." (Alarcon, 2014)

El control interno (TI) se trata de simples reglas a seguir, para documentar la forma en la que se realizan las actividades, como se realizan, como se supervisan, como se organización la empresa para asignar responsabilidades de supervisión y control. Esto permite evitar desviaciones que nos alejen de los objetivos institucionales, agregando valor y eliminando riesgos.

Por otro lado, la auditoría y control interno en sistemas computacionales son dos campos semejantes y tienen objetivos comunes, pero existen diferencias. El control interno analiza los controles día a día, el informe se dirige solo al personal interno y el alcance de sus funciones es solamente sobre el área de informática.

Por el contrario auditoría realiza un análisis de un momento informático determinado, informa a la dirección general de la empresa y cubre todos los componentes de los sistemas de información de la entidad. Se puede hablar también de similitudes en cuanto a conocimientos especializados en tecnología de la informática, verificación del cumplimiento de controles internos, normatividad y procedimientos establecidos por la Gerencia de informática y la Dirección General para los sistemas de información. Indiscutiblemente prestan un servicio de valor agregado al ayudar a la entidad y a sus directivos a cumplir sus obligaciones relativas al control interno mediante el proceso de recolección, agrupación y evaluación de evidencias para determinar de esta forma si el sistema informatizado cumple efectivamente los objetivos de la empresa y utiliza en forma eficiente estos recursos.

Riesgos Y Controles

Cada día son mayores los riesgos de seguridad informática, las aplicaciones institucionales a la medida pueden sufrir vulnerabilidades que cualquiera puede descubrir y atacar; se necesitan con urgencia un Backus online en remoto con infraestructuras seguras, por otro lado las reuniones por fuera, el teletrabajo, una caída de la red significa horas de trabajo perdidas, es decir se hace necesario proteger la red de la empresa.

Para información de amenazas, hay disponibles muchas fuentes, tales como:

- *Probabilidad de que una amenaza llegue a ocurrir por una vulnerabilidad (Piattini y del Peso, 2001).*
- *Un riesgo es la probabilidad de que una amenaza se materialice, utilizando vulnerabilidades existentes en un activo o un grupo de activos, generándole pérdidas o daños (ISO/IEC, 2004)*

(Alarcon, 2014)

Estas fuentes pueden ayudarnos a determinar la probabilidad de que ocurran ciertos eventos, así como la gravedad de los sucesos actuales.

Así mismo, hay otros elementos asociados al riesgo como lo son: Activo, amenaza, impacto, incidente, vulnerabilidad cada uno de estos riesgos ayuda a disminuir la probabilidad de vulnerabilidad y riesgo dentro de una empresa u organización. Controlar implica llevar a cabo acciones para estabilizar una situación o para reducir la posibilidad y la probabilidad de un daño, ya sean Preventivo, Directivos o Correctivos.

Niveles De Riesgo Según Pricewaterhouse Coopers Para Evaluar El Desempeño De Un Sí.

¿Qué es Price Waterhouse Coopers?

Según Wikipedia "*Es la firma de servicios profesionales más grande del mundo prestando servicios de auditoría, consultoría y asesoramiento legal y fiscal a las principales compañías, instituciones y gobiernos a nivel global."* (PwC, 2018)

Esta empresa nos da unos niveles de riesgo a la hora de desempañar una auditoria o sistema de información dentro de una empresa u organización los cuales son:

- Acceso a funciones de procesamiento
- Ingreso de datos
- Ítems rechazados o en suspenso
- Procesamiento
- Estructura organizativa del Dpto. de sistemas

Cada uno de estos niveles sirve de base para generar las acciones preventivas, acciones correctivas y oportunidades de mejora que tengan lugar los riesgos identificados en el SI.

METODOLOGÍAS, TÉCNICAS Y HERRAMIENTAS DE AUDITORÍA DE TI

Se pueden desarrollar una serie de actividades y técnicas que nos pueden ayudar a realizar la auditoria de información: Planificar, ejecución, informar y seguimiento. Para lograr mejores resultados de un proceso de auditoría.

Por otro se hablara un poco del análisis de riesgos, control interno de TI y plan de contingencias que se debe tener en cuenta durante el proceso de auditoría.

Cuando hablamos de metodologías de auditoría de SI, se debe tener en cuenta, el análisis de riesgos ya que es considerado uno de los pasos más importantes, para la identificación de los posibles problemas que podrían surgir en la organización, puesto que servirá como herramienta de decisión para hacer frente a dichos riesgos. La evaluación y análisis de riesgos, son utilizados actualmente por muchas empresas para evitar perdida de información o cualquier otro elemento valioso para esta.

Los métodos de identificación del riesgo pueden incluir: identificar situaciones, evaluar probabilidad de ocurrencia, gestionar el riesgo y comunicar la información. (Alarcon, 2014)

De esta manera obtendremos un conocimiento global de los riesgos, de sus causas, sus consecuencias, sus probabilidades, sus incertidumbres, etc. Este proceso suele necesitar un enfoque, para dar la mejor información posible a quien tiene que tomar decisiones, y pueda hacerlo manejando los datos más fiables.

Metodologías que apoyan el control interno de TI

El control interno es un proceso llevado a cabo por la dirección y el resto del personal de una empresa u organización, diseñado con el objeto de proporcionar un grado de seguridad.

Para explicar lo anterior, podemos analizar en forma breve la definición de control interno:

"El informe de auditoría aporta información a todos los interesados de la organización y cuando se requiere a entidades externas, como es el caso de procesos de certificación en normas de calidad, seguridad, riesgos, etcétera." (Alarcon, 2014)

El auditor, como parte de su trabajo de revisión de las cuentas anuales, tiene que conocer, entender y analizar los procedimientos de control interno de la empresa. Para ello tiene que mantener entrevistas con los responsables de gerencia y de la dirección. También es necesario reunirse con los responsables de los distintos departamentos de la sociedad y confrontar la información obtenida.

Plan De Contingencias

La información es uno de los principales activos que la empresa debe prevenir mediante el desarrollo de un plan de contingencia, que permita el adecuado funcionamiento del negocio frente a un cese prolongado del servicio informático.

El objetivo del plan no es evitar los riesgos, sino minimizar el impacto que las incidencias podrían producir en la organización. La alta dirección debe tomar conciencia que el desarrollo y la implantación de planes de contingencia comprende toda la organización, pues se trata de una situación de negocios y no puramente informática.

El diseñar e implementar un plan de contingencia para recuperación de desastres no es una tarea fácil; puede implicar esfuerzos y gastos considerables, sobre todo si se está partiendo de cero.

Principales actividades requeridas para la planificación e implementación de una capacidad de recuperación de desastres:

- *Identificación de riesgos*
- *Evaluación de riesgos*
- *Asignación de prioridades a las aplicaciones*
- *Establecimiento de los requerimientos de recuperación*
- *Elaboración de la documentación*
- *Verificación e implementación del plan*
- *Distribución y mantenimiento del plan*
- *Identificación de Riesgos*

(Informática Actualizada | Todo sobre sistemas y auditoría informática, 2012)

Todo proceso de auditoría requiere la aplicación de técnicas que le permitan de manera práctica obtener los insumos (información, evidencia, hallazgos), para llevar a cabo el análisis de la situación de estudio, la evaluación y la comprobación de funciones o procesos, a través de los cuales pueda emitir un informe de auditoría con base en su opinión profesional.

EL INFORME DE AUDITORÍA

El informe de auditoría es un informe realizado por un auditor, donde se expresa una opinión sobre los hallazgos detectados y es el soporte documental para sustentar el dictamen emitido en una empresa. En la guía nos dan una breve definición de que es el informe de auditoría, la cual se mostrara a continuación:

"*A raíz de las diferentes necesidades de administración y seguimiento a los procesos de TI, las cuales motivan a las organizaciones a acudir e implementar procesos de auditoría, se centra la atención en sus resultados, que se documentan y se hacen visibles a través del informe de auditoría, siendo este un producto que requiere contar con actividades estructuradas y responsables para su elaboración*." (Alarcon, 2014)

La Auditoría Interna es aquella que se practica en una empresa y es la encargada de la valoración de sus actividades. Constituye por ende una actividad vital, ya que por medio de esta se puede reducir pérdidas, su producto se ve revelado a través de los informes y recomendaciones.

El Código De Ética

El propósito del Código de Ética del Instituto es promover una cultura ética en la profesión de auditoría interna. Es necesario contar con un código de ética para la profesión de auditoría interna, ya que ésta se basa en la confianza que se imparte a su protección justo sobre la gestión de riesgos, control y dirección. Existen varios principios que se debe tener en cuenta como auditores:

- *Beneficio del auditado*
- *Calidad*
- *Capacidad*
- *Cautela*
- *Comportamiento profesional*
- *Concentración en el trabajo*
- *Confianza*
- *Criterio propio*
- *Discreción*
- *Economía*
- *Formación continuada*
- *Fortalecimiento y respeto de la profesión*
- *Independencia*

- *Información suficiente*
- *Integridad moral*
- *Legalidad*
- *Libre competencia*
- *No discriminación*
- *No injerencia*
- *Precisión*
- *Responsabilidad*
- *Secreto profesional*
- *Servicio público*
- *Veracidad*

(Alarcon, 2014)

El código de ética deberá ser aplicado por todo aquel que desarrolle el rol de auditor, ya que es la carta de presentación e inspiración para que su ejercicio, con el único objetivo de proteger y mejorar el funcionamiento de la Entidad.

Esquema Del Documento De Auditoría

Al presentar un informe de auditoría, este debe mostrar aspectos que reflejen un resultado de excelencia y que tanto para el auditor como para la entidad auditada represente un proceso exitoso.

Características Del Informe De Auditoría

"*El informe de auditoría debe contar con las características de ser objetivo, claro, oportuno, constructivo y concreto*".

- *El informe es claro cuando quien lo recibe puede comprenderlo y acceder a información de apoyo para ampliar lo allí descrito.*
- *El informe es concreto cuando hace énfasis en los hechos, hallazgos y evidencias sin entrar en detalles innecesarios.*
- *El informe es constructivo cuando a través de su contenido la organización y los auditados pueden ver las oportunidades de mejora y se evidencia claramente el camino por seguir.*
- *El informe es oportuno cuando se entrega en el tiempo establecido y permite la toma de acciones inmediatas.*
- *Aunque expresa opiniones técnicas de acuerdo con la planificación y la ejecución de la auditoría realizada, es importante que lo señalado pueda ser interpretado por personas que no manejan el lenguaje técnico, con el fin que no se presenten confusiones.*

(Alarcon, 2014)

El auditor mantiene una actitud de independencia mental e imparcialidad respecto a su labor y debe ostentar un grado de profesionalismo muy alto donde su diligencia es factor clave de éxito, debe ser reconocida su integridad e idoneidad, la rectitud ética y profesional.

Construcción Del Informe De Auditoría

"El informe de auditoría debe ser construido teniendo en cuenta que va dirigido al nivel estratégico y directivo de la organización. Su contenido dará cuenta si el(los) auditor(es) cuenta(n) o no con una visión general de la organización en su análisis del área auditada, como también si cuenta(n) con la experiencia y la capacitación para llevar a cabo este proceso." (Alarcon, 2014)

Por lo tanto la auditoría de una organización debe ser una sola, presentada en un único informe que abrevie el trabajo de todos los enfoques de la auditoría, más allá de lo que se conoce actualmente como una auditoría general.

Conclusiones Del Informe De Auditoría

Los informes concluyentes de los auditores dependen de sus capacidades para analizar las situaciones de debilidad o fortaleza de los diferentes medios. El trabajo del auditor consiste en lograr obtener toda la información necesaria para emitir un juicio global imparcial, siempre amparando las evidencias.

El auditor debe estar capacitado para comprender los mecanismos que se desarrollan en un proceso electrónico. También debe estar preparado para enfrentar sistemas computarizados en los cuales se encuentra la información necesaria para auditar.

CONCLUSION

Toda empresa, pública o privada, que posean Sistemas de Información medianamente complejos, deben de someterse a un control estricto de evaluación de eficacia y eficiencia.

Hoy en día, la mayoría de las empresas tienen toda su información estructurada en Sistemas Informáticos, de aquí, la vital importancia que los sistemas de información funcionen correctamente. Una empresa puede contar con personal altamente capacitado, pero si tiene un sistema informático propenso a errores, lento, frágil e inestable; la empresa nunca saldrá a adelante.

La auditoría de Sistemas debe hacerse por profesionales expertos, una auditoria mal hecha puede acarrear consecuencias drásticas para la empresa auditada, principalmente económicas.

Bibliografía

Alarcon, C. A. (2014). *Gobernabilidad Ti- Unidad 3*. Bucaramanga: CreativeCommons.

Informática Actualizada | Todo sobre sistemas y auditoría informática. (2012). Obtenido de http://informaticaactualizada.blogspot.com/2010/06/plan-de-contingencias.html

Malica, C. D. (2012). *EL SISTEMA DE CONTROL INTERNO Y SU IMPORTANCIA EN LA AUDITORÍA*. Obtenido de http://www.facpce.org.ar:8080/iponline/el-sistema-de-control-interno-y-su-importancia-en-la-auditoria/

PwC. (16 de junio de 2018). *Wikipedia*. Obtenido de https://es.wikipedia.org/wiki/PwC