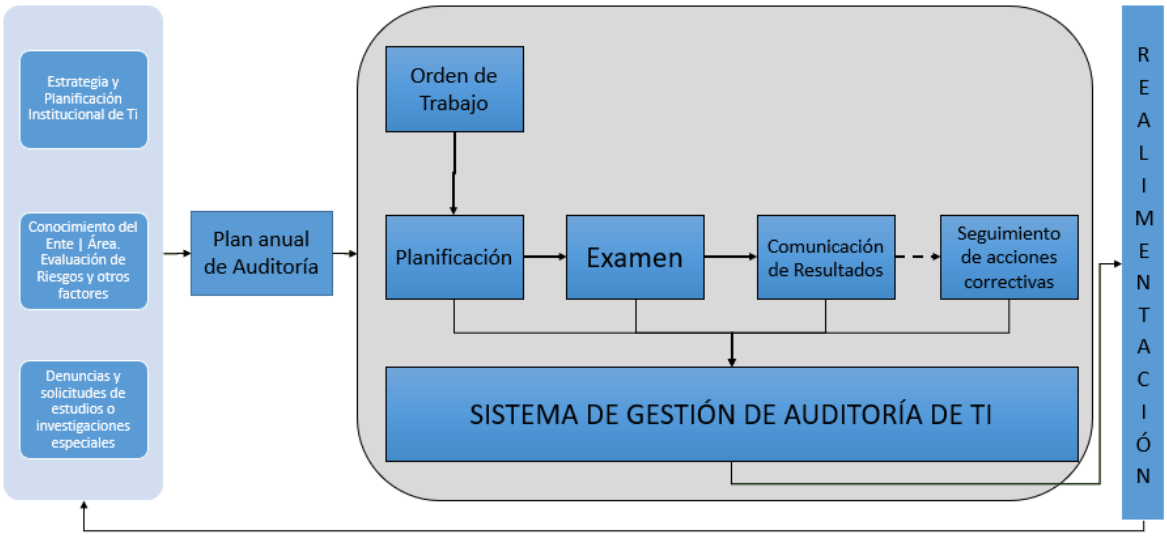
AUDITORÍA INFORMÁTICA

Definición

La Auditoría de TI es el PROCESO mediante el cual se evalúa el cumplimiento de los criterios de gestión y control de los recursos tecnológicos de información de una empresa o entidad, con el propósito de concluir sobre el grado de economía y eficiencia en la adquisición y uso y sobre la eficacia para producir información pertinente al negocio, íntegra, correcta, confiable, confidencial y oportuna para la toma de decisiones de la organización, bajo criterios de ética, legalidad y cuidado por el ambiente. Como resultado de este proceso se espera coadyuvar con los miembros de la organización para un desempeño efectivo de sus responsabilidades.

Sistema de Gestión de Auditoría



¿Por qué realizarla?

La auditoría informática es un campo nuevo dentro de los procesos de auditoría. La tecnología ha traído consigo cambios dentro de los procesos de las organizaciones. Es por ello por lo que es necesario que las Tecnologías de Información sean objeto de evaluación por parte de la Auditoría, con el fin de verificar el grado de razonabilidad del control interno.

La tecnología informática (hardware, software, redes, bases de datos, etc.) es una herramienta estratégica que brinda rentabilidad y ventajas competitivas a los negocios frente a otros negocios similares en el mercado, pero puede originar costos y desventajas si no es bien administrada por el personal encargado.

La solución clara es entonces realizar evaluaciones oportunas y completas de la función informática, a cargo de personal calificado, consultores externos, auditores en informática o evaluaciones periódicas realizadas por el mismo personal de informática.

También es un conjunto de tareas realizadas por un especialista para la evaluación o revisión de políticas y procedimientos relacionados con las diferentes áreas de una empresa:

- Administrativas
- Financieras
- Operativas
- Informática

- Crédito
- Fiscales

Campos de acción

El campo de acción de la auditoria informática es:

- La evaluación administrativa del área de informática. esto comprende la evaluación de:
    - Los objetivos del departamento, dirección o gerencia.
    - Metas, planes, políticas y procedimientos de procesos electrónicos estándares.
    - Organización del área y su estructura orgánica.
    - Funciones y niveles de autoridad y responsabilidad del área de procesos electrónicos.
    - Integración de los recursos materiales y técnicos.
    - Dirección.
    - Costos y controles presupuestales.
    - Controles administrativos del área de procesos electrónicos.
- La evaluación de los sistemas y procedimientos, y de la eficiencia que se tiene en el uso de la información, lo cual comprende:
    - Evaluación del análisis de los sistemas y sus diferentes etapas.
    - Evaluación del diseño lógico del sistema.
    - Evaluación del desarrollo físico del sistema.

- Facilidades para la elaboración de los sistemas.
- Control de proyectos.
- Control de sistemas y programación.
- Instructivos y documentación.
- Formas de implantación.
- Seguridad física y lógica de los sistemas.
- Confidencialidad de los sistemas.
- Controles de mantenimiento y forma de respaldo de los sistemas.
- Utilización de los sistemas.
- Prevención de factores que puedan causar contingencias; seguros y recuperación en caso de desastre.
- Productividad.
- Derechos de autor y secretos industriales.

- La evaluación del procesamiento de datos, de los sistemas y de los equipos de cómputo (software, hardware, redes, bases de datos, comunicaciones), la cual comprende:
  - Controles de los datos fuente y manejo de cifras de control.
  - Control de operación.
  - Control de salida.
  - Control de asignación de trabajo.
  - Control de medios de almacenamiento masivo.
  - Control de otros elementos de cómputo.

    - Control de medios de comunicación.
    - Orden en el centro de cómputo.
- La seguridad y confidencialidad de la información, que comprende:
    - Seguridad física y lógica.
    - Confidencialidad.
    - Respaldos.
    - Seguridad del personal.
    - Seguros.
    - Seguridad en la utilización de los equipos.
    - Plan de contingencia y procedimiento de respaldo para casos de desastre.
    - Restauración de equipos y de sistemas.

Los principales objetivos de la auditoria informática son los siguientes:

- Salvaguardar los activos. Se refiere a la protección del hardware, software y recursos humanos.
- Integridad de datos. Los datos deben mantener consistencia y no duplicarse.
- Efectividad de sistemas. Los sistemas deben cumplir con los objetivos de la organización.
- Eficiencia de sistemas. Que se cumplan los objetivos con los menores recursos.
- Seguridad y confidencialidad.

Para que sea eficiente la auditoria informática, ésta se debe realizar también durante el proceso de diseño del sistema. Los diseñadores de sistemas tienen la difícil tarea de asegurarse que interpretan las necesidades de los usuarios, que diseñan los controles requeridos por los auditores y que aceptan y entienden los diseños propuestos.

La interrelación que debe existir entre la auditoria informática y los diferentes tipos de auditoria es la siguiente: el núcleo o centro de la informática son los programas, los cuales pueden ser auditados por medio de la auditoria de programas. Estos programas se usan en las computadoras de acuerdo con la organización del centro de cómputo (personal).

La auditoría en informática debe evaluar todo (informática, organización del centro de cómputo, computadoras, comunicación y programas), con auxilio de los principios de la auditoria administrativa, auditoria interna, auditoría contable/financiera y, a su vez, puede proporcionar información a esos tipos de auditoria. Las computadoras deben ser una herramienta para la realización de cualquiera de las auditorias.

La adecuada salvaguarda de los activos, la integridad de los datos y la eficiencia de los sistemas solamente se pueden lograr si la administración de la organización desarrolla un adecuado sistema de control interno.

El tipo y características del control interno dependerán de una serie de factores, por ejemplo, si se trata de un medio ambiente de minicomputadoras o macrocomputadoras, si están conectadas en serie o

trabajan en forma individual, si se tiene Internet y Extranet. Sin embargo, la división de responsabilidades y la delegación de autoridad es cada vez más difícil debido a que muchos usuarios comparten recursos, lo que dificulta el proceso de control interno.

La evaluación que se debe desarrollar para la realización de la auditoria en informática debe ser hecha por personas con un alto grado de conocimiento en informática y con mucha experiencia en el área.

La información proporcionada debe ser confiable, oportuna, verídica, y debe manejarse en forma segura y con la suficiente confidencialidad, pero debe estar contenida dentro de parámetros legales y éticos.

Perfil requerido

Especialización en función de la importancia económica que tienen distintos componentes financieros dentro del entorno empresarial

Debe conocer técnicas de administración de empresas y de cambio, ya que las recomendaciones y soluciones que aporte deben estar alineadas a los objetivos de la empresa y a los recursos que se poseen

El auditor debe tener un enfoque de calidad total, lo cual hará que sus conclusiones y trabajo sean reconocidos como un elemento valioso dentro de la empresa

Principios Éticos del Auditor

- Principio de calidad
- Principio de capacidad
- Principio de comportamiento profesional
- Principio de confianza
- Principio de criterio propio
- Principio de legalidad
- Principio de secreto profesional
- Principio de veracidad
- Principio de información suficiente
- Principio de cautela

Certificaciones (CISA)

¿Qué es un CISA? CISA, por sus siglas en inglés, significa *Certified Information System Auditor*, o en su traducción: Auditor Certificado en Sistemas de Información.

Esta certificación dada por la organización internacional ISACA (Information Systems Audit and Control Association, o, Asociación de Auditoría y Control de Sistemas de Información) que apoya y patrocina el desarrollo de

metodologías y certificaciones para la realización de actividades de auditoría y control de sistemas de información.

La certificación CISA es reconocida a nivel mundial que reconocer aptitudes y conocimientos de un profesional en las tareas de:

- Auditoría en Sistemas de Información.
- Gobierno y mantenimiento de tecnología de información.
- Adquisición, desarrollo e implementación de sistemas de información.
- Operaciones, mantenimiento y soporte de sistemas de información.
- Protección de activos de información.

La certificación demuestra la experiencia, habilidades y conocimientos en auditoría, capaz de evaluar las vulnerabilidades, informes de cumplimiento y establecer controles dentro de una empresa.

Beneficios

- Conocimiento y experiencia
- Nivel de conocimientos necesarios para afrontar los retos dinámicos de una empresa moderna.
- Reconocimiento mundial como profesional de auditoría de sistemas de información.
- Combinación de la teoría, el trabajo y la experiencia educativa que proporciona credibilidad en el mercado.

- Ayuda a lograr un alto nivel profesional a través de ISACA para la educación continua y la conducta ética.

Cómo lograr la certificación

- Aprobar el examen CISA. Dicho examen puede realizarse por cualquier persona interesada en las áreas de auditoría en sistemas de información, control y seguridad
- Enviar la aplicación a la certificación CISA Los candidatos que aprueban el examen de certificación CISA deben demostrar los requisitos de experiencia laboral. Un mínimo de 5 años de experiencia profesional en auditoría en sistemas de información, control o seguridad (como se describe en las áreas de práctica CISA)
- Apegarse al código de ética profesional Las personas que aplican a la certificación CISA deben apegarse al código de ética profesional y conducta
- Apegarse al programa de educación continua profesional (CPE) Para seguir siendo un CISA un individuo debe estar de acuerdo en cumplir con el programa de educación continua profesional. Mantener un mínimo de 20 horas CPE anuales y un mínimo de 120 horas CPE durante un periodo de 3 años

- Cumplir con los estándares en auditoría en Sistemas de Información los candidatos a la certificación CISA, debe apegarse a los estándares adoptados por ISACA en auditoría en Sistemas de Información

Conceptos relevantes

Riesgos

Según la RAE, un riesgo es “Contingencia o proximidad de un daño.”, es decir, riesgo es la vulnerabilidad ante un potencial perjuicio o daño para las unidades, personas, organizaciones o entidades. Cuanto mayor es la vulnerabilidad mayor es el riesgo, pero cuanto más factible es el perjuicio o daño, mayor es el peligro.

Riesgo de auditoría

Un riesgo de auditoría es aquel que existe en todo momento por lo cual se genera la posibilidad de que un auditor emita una información errada por el hecho de no haber detectado errores o faltas significativas que podría modificar por completo la opinión dada en un informe.

La posibilidad de existencia de errores puede presentarse en distintos niveles, por lo tanto, se debe analizar de la forma más apropiada para observar la implicación de cada nivel sobre las auditorias que vayan a ser realizadas.

Riesgo inherente

Este tipo de riesgo tiene ver exclusivamente con la actividad económica o negocio de la empresa, independientemente de los sistemas de control interno que allí se estén aplicando.

Si se trata de una auditoría financiera es la susceptibilidad de los estados financieros a la existencia de errores significativos; este tipo de riesgo está fuera del control de un auditor por lo que difícilmente se puede determinar o tomar decisiones para desaparecer el riesgo ya que es algo innato de la actividad realizada por la empresa.

Entre los factores que llevan a la existencia de este tipo de riesgos esta la naturaleza de las actividades económicas, como también la naturaleza de volumen tanto de transacciones como de productos y/o servicios, además tiene relevancia la parte gerencial y la calidad de recurso humano con que cuenta la entidad.

Riesgo de control

Aquí influye de manera muy importante los sistemas de control interno que estén implementados en la empresa y que en circunstancias lleguen a ser insuficientes o inadecuados para la aplicación y detección oportuna de irregularidades. Es por esto la necesidad y relevancia que una administración tenga en constante revisión, verificación y ajustes los procesos de control interno.

Cuando existen bajos niveles de riesgos de control es porque se están efectuando o están implementados excelentes procedimientos para el buen desarrollo de los procesos de la organización.

Entre los factores relevantes que determina este tipo de riesgo son los sistemas de información, contabilidad y control.

Prueba de cumplimiento

Es el examen de la evidencia disponible de que una o más técnicas de control interno están operando durante el periodo de auditoría.

El auditor deberá obtener evidencia de auditoría mediante pruebas de cumplimiento de:

- Existencia: el control existe
- Efectividad: el control está funcionando con eficiencia
- Continuidad: el control ha estado funcionando durante todo el periodo.

El objetivo de las pruebas de cumplimiento es quedar satisfecho de que una técnica de control estuvo operando efectivamente durante todo el periodo de auditoría.

Prueba sustantiva.

Consisten en comprobaciones diseñadas para obtener evidencia de la validez y propiedad de las transacciones y saldos que van formando los estados financieros de una organización; incluyen comprobaciones de detalles, como las aplicaciones de muestreo o pruebas selectivas, y procedimientos analíticos, diseñados para detectar errores e irregularidades en la información financiera y sus acumulaciones, dichas pruebas son básicas para determinar la opinión final a los estados financieros. Es decir, que se tiene como pruebas sustantivas, los procedimientos de auditoría dirigidos o examinados a obtener evidencia de validez y corrección del manejo contable de las transacciones y los estados financieros y detección de errores o irregularidades en ellos.

Instrumental básico

Programas de auditoría

Un programa de auditoría, también llamado plan de auditoría, es un plan de acción que documenta qué procedimientos seguirá un auditor para validar que una organización cumple con las regulaciones de cumplimiento.

El objetivo de un programa de auditoría es crear un marco que sea lo suficientemente detallado como para que cualquier auditor externo entienda qué exámenes oficiales se han completado, a qué conclusiones se ha llegado y cuál es el razonamiento detrás de cada conclusión. El marco debe explicar

los objetivos de la auditoría, su alcance y su línea de tiempo. El programa de auditoría también debe describir cómo los documentos de trabajo –la evidencia documentada de la auditoría– serán recopilados, revisados e informados.

Papeles de trabajo

Los papeles de trabajo son el conjunto de documentos que contienen la información obtenida por el auditor en su revisión, así como los resultados de los procedimientos y pruebas de auditoría aplicados; con ellos se sustentan las observaciones, recomendaciones, opiniones y conclusiones contenidas en el informe correspondiente.

Evidencia

En la NIA 500, se define el concepto de Evidencia:

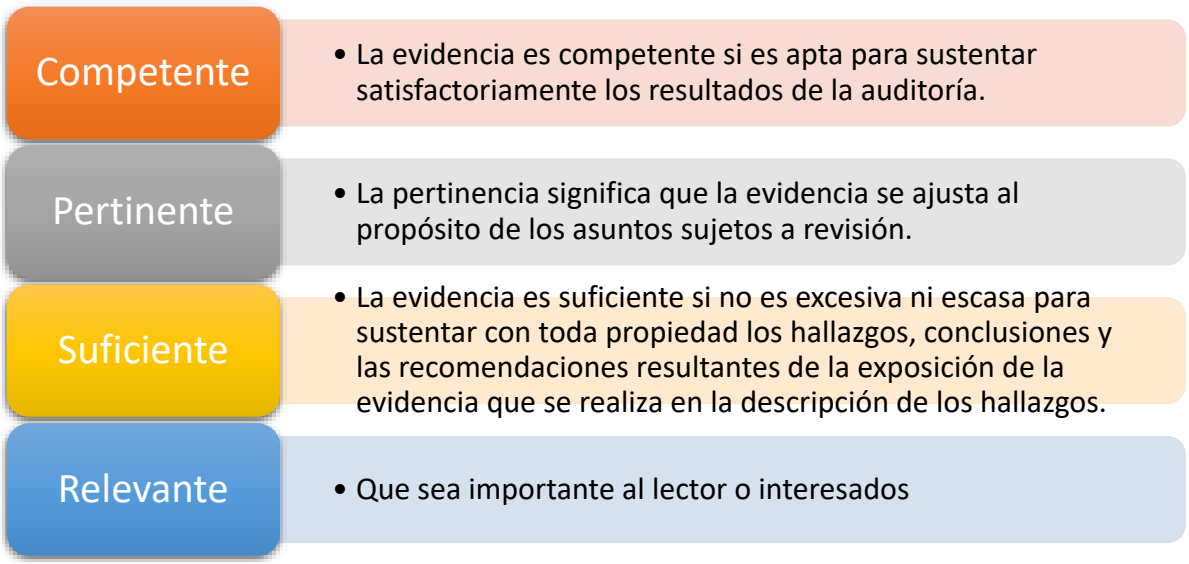
Información utilizada por el auditor para alcanzar las conclusiones en las que basa su opinión. La evidencia de auditoría incluye tanto la información contenida en los registros contables de los que se obtienen los estados financieros, como otra información.

Para que esta información sea valiosa, se requiere que la evidencia sea competente, es decir con calidad en relación a su relevancia y confiabilidad y suficiente en términos de cantidad, al tener en cuenta los factores como: posibilidad de información errónea, importancia y costo de la evidencia.

- Relevante - Cuando ayuda al auditor a llegar a una conclusión respecto a los objetivos específicos de auditoría.

- Autentica - Cuando es verdadera en todas sus características.
- Verificable - Es el requisito de la evidencia que permite que dos o más auditores lleguen por separado a las mismas conclusiones, en iguales circunstancias.
- Neutral - Es requisito que esté libre de prejuicios. Si el asunto bajo estudio es neutral, no debe haber sido diseñado para apoyar intereses especiales.

Características de la evidencia:



Técnicas de obtención de evidencia

Informes

Es el resultado del trabajo realizado por el auditor, donde se exponen los hallazgos, recomendaciones sobre los hallazgos para reducir o eliminar dichas situaciones y también están las conclusiones del auditor respecto al trabajo realizado. Por lo general, se incluye un resumen ejecutivo del informe.

Estructura de un informe de auditoría

- Información introductoria
    - Antecedentes
    - Objetivos de la Auditoría
    - Alcance de la Auditoría

    - Base legal, Objetivos y estructura orgánica de la entidad
    - Principales funcionarios
- Control Interno
- Observaciones de Auditoría
- Conclusiones
- Recomendaciones
- Firmas responsables (únicamente borrador)

Indización

La indización es el hecho de asignar índices o claves de identificación las cuales permitirán localizar y conocer el lugar exacto donde se encuentra el expediente, este procedimiento representa grandes ventajas para el auditor tales como simplificar: la localización de algún asunto en específico dentro de los papeles de trabajo.

REFERENCIAS

Auditool. (18 de noviembre de 2014). *¿Qué es el riesgo, riesgo inherente y riesgo residual?* Obtenido de Auditool: https://www.auditool.org/blog/control-interno/3073-que-es-el-riesgo-riesgo-inherente-y-riesgo-residual

Auditool. (5 de julio de 2016). *La Evidencia de Auditoría*. Obtenido de Auditool: https://www.auditool.org/blog/auditoria-externa/772-la-evidencia-de-auditoria

Colegio de Contadores Públicos de Costa Rica. (11 de diciembre de 2014). *CIRCULAR No. 03-2014.* Obtenido de Colegio de Contadores Públicos de Costa Rica: https://ccpa.or.cr/wp-content/themes/maximus/pdf/normativa-vigente/circulares-vigentes/Circular03-2014.pdf

Conceptos de auditoria y auditoria informática. (s.f.). Obtenido de Auditoria en Informatica: https://sites.google.com/site/auditoriaeninformaticacun/home

ISACA. (s.f.). *Certificaciones*. Obtenido de ISACA Capítulo Costa Rica: https://www.isacacr.org/certificaciones.html

Quintero Arias, A. (08 de agosto de 2015). *FUNCIONES Y PERFIL DE UN AUDITOR DE SISTEMAS*. Obtenido de Auditoría Informática:

https://chaui201521701020289.wordpress.com/2015/11/08/funciones-y-perfil-de-un-auditor-de-sistemas/