Dom. Cien., ISSN: 2477-8818
Vol. 3, núm. mon., agos., 2017, pp. 157-173

Número Publicado el 22 de agosto de 2017

http://dx.doi.org/10.23857/dom.cien.pocaip.2017.3.mono1.ago.157-173
URL:http://dominiodelasciencias.com/ojs/index.php/es/index

Auditoría informática: un enfoque efectivo

Computer audit: an effective approach

Auditoria informática: uma abordagem efetiva

[I] Diego A. Arcentales-Fernández
darcentales2013@gmail.com

[II] Xiomara Caycedo-Casas
xiomaracaycedo@hotmail.com

Recibido: 30 de enero de 2017 *** Corregido:** 25 de abril de 2017 *** Aceptado:** 28 de junio de 2017

[I] Ingeniero en Sistemas, Programa de Revalidación de la Maestría de Gestión Estratégica de Tecnologías de la Información, Facultad de Ingeniería, Universidad de Cuenca, Campus Central, Cuenca, Azuay.

[II] Magister en Gerencia y Liderazgo Educacional, Profesional en Terapia Ocupacional.

Resumen

En un entorno cambiante, el éxito de una organización se ha relacionado estrechamente con su capacidad para gestionar los riesgos. La importancia de las auditorías informáticas radica en que permiten determinar las fortalezas y debilidades del sistema de información de las organizaciones. El objetivo de esta investigación documental es identificar las mejores prácticas en auditorias informáticas. Entre los hallazgos de la investigación se destaca, la importancia de las competencias del auditor; y en cuanto a las mejores prácticas, aunque la mayoría se decanta por el enfoque COBIT, muchos autores recomiendan un sistema integrado que combine muchas estrategias.

Palabras clave: auditoria informática; sistemas de información; TIC.

Abstract

In a changing environment, the success of an organization is closely related to its ability to manage risks. The importance of computer audits is that they determine the strengths and weaknesses of the information system of organizations. The objective of this documentary research is to identify the best practices in computer audits. Among the findings of the research highlights the importance of the auditor's competencies; And in terms of best practices, although the majority opt for the COBIT approach, many authors recommend an integrated system that combines many strategies.

Keywords: IT audit; information systems; ICT.

Resumo

Em um ambiente em mudança, o sucesso de uma organização tem sido intimamente ligado à sua capacidade de gerenciar riscos. A importância das auditorias informáticas é que eles determinam os pontos fortes e fracos do sistema de informação das organizações. O objetivo desta pesquisa documental é identificar as melhores práticas em auditorias de computadores. Entre as descobertas da pesquisa, destacam-se a importância das competências do auditor; E em termos de melhores práticas, embora a maioria opte pela abordagem COBIT, muitos autores recomendam um sistema integrado que combina muitas estratégias.

Palavras chave: auditoria informática; sistemas de informação; TIC.

Introducción

En un entorno cambiante, el éxito de una organización se ha relacionado estrechamente con su capacidad para gestionar los riesgos; a medida que las empresas se vuelven cada vez más dependientes de la información para su ventaja competitiva y la información gana incluso mayor proporción en el valor agregado incorporado en los productos y servicios de las empresas, la capacidad de proteger información valiosa y sensible se ha convertido en una capacidad estratégica para asegurar la sostenibilidad empresarial, y el valor total de una empresa (Hohan, Olaru & Pirnea, 2015). En un contexto global cada vez más competitivo y complejo tecnológicamente, el éxito de las empresas pasa a depender de su capacidad para administrar sus recursos, incluso los de tecnología de la información y comunicación (TIC), de forma efectiva (Tarouco & Graeml, 2001).

Para las organizaciones empresariales, es vital que se evalúen constante y regularmente todos los procesos que en ellas se llevan a cabo, con el fin de verificar su calidad y suficiencia en cuanto a los requerimientos de negocio para la información: control, integridad y confidencialidad (Graterol & Hernández, 2011). A medida que los negocios iban evolucionando, el volumen de información y de las transacciones se incrementaban, por lo que las organizaciones tuvieron la necesidad de recurrir a la automatización de sus sistemas de información, por ejemplo, tuvieron que automatizar los registros contables y varios procesos operativos, los cuales tenían que ser soportados por activos de tecnología como servidores, redes, software y hardware especializado (Espinoza, 2016).

Un gran número de organizaciones considera que la información y la tecnología asociada a ella, representan sus activos más importantes; al igual que se exige para los otros activos, los requerimientos de calidad, controles, seguridad e información son indispensables; la comprobación de la aplicación de los mencionados mecanismos es tarea de la auditoria informática (de Pablos et al.,, 2006). Cada vez con más frecuencia, se hace necesario acceder a los datos confidenciales e intercambiarlos entre sistemas informáticos complejos y distribuidos; para proteger la confidencialidad de los datos, se han desarrollado numerosos mecanismos de control de acceso distribuido, los cuales, típicamente, intentan prevenir acciones ilegítimas antes de su ocurrencia, decidiendo sobre la marcha si el acceso debe ser concedido o no (Dekker & Etalle, 2007).

La "Seguridad de la Información", ha cobrado una importancia relevante en gran parte de las organizaciones, tanto públicas como privadas, ya que la información que genera la empresa, se ha

convertido en un bien (Activo Real) en riesgo, que debe ser resguardado y protegido contra posibles daños, perdidas, manipulación, etc., que pueden tener como origen, tanto personal interno, como externo, personas jurídicas y naturales, con los cuales la empresa se desenvuelve de manera cotidiana en sus actividades, procesos, operaciones y transacciones de carácter, jurídico legal, administrativo, contable, financiero u otro (Dávalos, 2013).

La importancia de las auditorías informáticas radican en que permiten determinar las fortalezas y debilidades en la gestión de proyectos, el nivel de funcionalidad de los sistemas de información automatizados, la adecuación de la configuración de la plataforma informática, el nivel de calidad de los servicios prestados por la unidad encargada y la situación de los contratos con proveedores de productos y servicios, entre otros aspectos, todo ello en el ámbito del uso y aplicación de las TIC´s en la organización (Hernández, 2010).

En este documento se revisa la literatura de auditoría informática, con el propósito de identificar buenas prácticas para la gestión de las mismas.

Materiales y métodos

Este estudio representa una revisión de la literatura sobre enfoques de auditorías de sistemas de gestión de tecnologías de información, cuyo objetivo es identificar las mejores prácticas en la gestión. Se hizo una búsqueda en bases de datos como ScieceDirect y Google Scholar, entre otras. Además, se examinaron los portales académicos más importantes sobre gestión de auditoría informática de TI en educación superior.

Se utilizaron los siguientes criterios para el proceso de revisión: la búsqueda se realizó en agosto de 2017; publicaciones escrita en español o inglés, y disponible en texto completo; palabras clave "Auditoría Informática", "Computer audit", con la combinación del tema y el título. Se encontraron otros artículos sobre este tema, pero no fueron considerados, ya que sólo se tenía acceso al resumen.

Resultados y discusión

La tecnología de la información (TI) se ha convertido en un elemento esencial para apoyar el crecimiento y la sostenibilidad de todo tipo de organizaciones; para controlar este conjunto heterogéneo de tecnologías, es necesaria su gestión eficaz utilizando estructuras, procesos y

mecanismos relacionales; cada uno de estos mecanismos tiene una función y cuando se implementa, debe impactar positivamente a la organización (Scalabrin & Dinis, 2016).

Así como la tecnología ha ido evolucionando, los fraudes y delitos informáticos han ido a la par, a tal punto que en la actualidad un delincuente informático puede sustraer recursos económicos de una organización desde la comodidad de su hogar, sin dejar rastro alguno, o estructurar grandes delitos desde el interior de la organización; esta situación sumados a los grandes desfalcos financieros ocurridos a nivel mundial, incluyendo delitos informáticos, han obligado al auditor un cambio de enfoque y la necesidad de que el auditor cuente con nuevas habilidades y conocimientos, sobre todo el área de tecnología (Espinoza, 2016).

El desarrollo vertiginoso en las redes informáticas trajo consigo un aumento considerable en la velocidad de procesamiento y en la transmisión de información del negocio, pero con riesgos cada vez mayores en lo referente a seguridad de los datos transportados por estos medios; en este sentido, en la actualidad, la convergencia de las tecnologías de la información han ocasionado una tecnodependencia que impide una separación certera entre la seguridad propia de las aplicaciones (seguridad informática) con la seguridad de la información como tal (Díaz, 2012).

La gestión de la seguridad de la información es un factor importante para proteger los activos de información de una organización; el auge del comercio electrónico a través de los proveedores de servicios y directamente con los clientes, la pérdida de barreras organizacionales y exposiciones de seguridad de alto perfil tales como riegos físicos (Robos, daños por siniestros, destrucción de equipamiento, etc.) y lógicos (Virus, acceso clandestino de redes, Violación de contraseñas, etc), han elevado el perfil de riesgo de la información, y la necesidad de administrar la Seguridad de la Información; por esta razón, han cobrado relevancia las Auditorias sobre la Seguridad de la Información, ya que las mismas permiten obtener una ventaja competitiva y satisfacer los requerimientos básicos del negocio (Dávalos, 2013).

La auditoría es un componente del sistema de control interno de las organizaciones, el cual tiene como misión fundamental asesorar a la alta dirección en la definición, desarrollo, implantación y mantenimiento de los sistemas de control: legal, financiero, informático y de gestión para asegurar los resultados esperados de las operaciones conforme a los objetivos preestablecidos (Pinilla, 1994). La auditoría, una disciplina, asociada tradicionalmente con aspectos financieros y actualmente anclada

en los aspectos estratégicos de la vida organizacional, convertida en una herramienta gerencial indispensable para el logro eficaz y eficiente de los objetivos organizacionales, pero que requiere ser más pertinente, desde una perspectiva tecnológica, si se tiene en cuenta que las TIC, han evolucionado en las organizaciones, al dejar de ser, simplemente estructuras de apoyo, a ser parte del negocio (Valencia & Tamayo, 2012).

En general, la auditoría es una práctica de trascendental importancia social y económica, permite entablar relaciones de diversa índole entre los agentes económicos, debido a la confianza que se deposita en el trabajo de los auditores cuando ellos extienden su garantía personal o fe pública, respecto del trabajo de investigación denominado auditoría; la auditoría ha sido tomada y apropiada por diferentes profesiones técnicas y científicas ampliando su campo de acción, se puede considerar que cualquier asunto de interés es posible de auditar, razón por la que existe un sinnúmero de diferentes auditorías y de distintos profesionales que la realizan (Montilla & Herrera, 2006).

Por su parte, la auditoría informática o de tecnología de información, se originó en los Estados Unidos en los años sesenta; a principios de los años sesenta, IBM publicó "auditoría electrónica de procesamiento de datos" y "Las normas de auditoría y métodos de organización con procesamiento electrónico de datos", que regula nuevas reglas de auditoría interna y métodos organizativos en el entorno de procesamiento electrónico de datos; en 1968, el Instituto de Contadores Públicos de los Estados Unidos publicó "Auditoría contable e informática", que había realizado requisitos técnicos para la auditoría de TI; en 1969, se creó la Asociación Internacional de Auditoría y Control de Sistemas de Información (ISACA), la única organización internacional en el campo de auditoría de TI hasta el momento (Zhi & Zhou, 2013).

Una auditoría informática es "la revisión, verificación y evaluación con un conjunto de métodos, técnicas y herramientas de los sistemas de información de una organización, de forma continua y a petición de su Dirección y con el fin de mejorar su rentabilidad, seguridad y eficacia (de Pablos et al., 2006). Hay especialistas que opinan que la auditoría de gestión financiera con el uso de recursos informáticos, se denomina Auditoría Informática; sin embargo otros opinan que este término debe ser exclusivo de las auditorías que se hacen a la función informática (Alfonso, Blanco & Loy, 2012).

La auditoría informática comprende el diagnóstico y evaluación del entorno informático (hardware, software, bases de datos, redes, instalaciones, etc.) sobre la base de estándares internacionalmente

aceptados y de modelos de referencia que hacen énfasis en la mejor forma de gestionarlo; se trata de un proceso empresarial, en el cual intervienen de manera conjunta los responsables del área de informática, administradores, contadores, auditores generales y coordinadores del resto de procesos ejecutados en la organización; su participación puede concretarse en las diferentes etapas de la auditoría informática: planificación, ejecución (levantamiento de información), análisis de resultados, hallazgos o evidencias útiles en la elaboración del informe final. (Hernández, 2010)

El propósito a alcanzar por una organización al realizar una auditoría informática de cualquier parte de sus sistemas de información es asegurar que sus objetivos estratégicos son los mismos que los de la propia organización y que los sistemas prestan el apoyo adecuado a la consecución de estos objetivos, tanto en el presente como en su evolución futura (de Pablos et al., 2006). La Auditoría Informática permite a la Entidad Pública buscar los medios para alcanzar los estándares internacionales en el uso adecuado de las tecnologías de información, con miras a una certificación de calidad; pone al descubierto si los esfuerzos de la Entidad están correctamente orientados a controlar los riesgos de mayor impacto y a redireccionar aquellos esfuerzos orientados a áreas que no representan riesgos (Ramírez & Álvarez, 2003).

Sistemas de gestión de tecnología de la información

Un conjunto bien definido de políticas y procedimientos de seguridad puede prevenir pérdidas y ahorrar recursos para la organización, de ahí que la Auditoria de Seguridad de la Información cobra importancia como medio de detección de desviaciones de las políticas y procedimientos implantados por medio de herramientas de aplicación aceptadas a nivel mundial (Estándares, prácticas, etc.) y permiten la retroalimentación para las correcciones o cambios oportunos con el fin de lograr mejorar la Seguridad de la Información y salvaguardar la misma (Dávalos, 2013).

Como lo plantea Díaz (2012), las ventajas en lo organizacional de aspirar a una certificación o de alinear sus procesos hacia estándares certificados confluyen principalmente en las siguientes: 1) se puede aprovechar una curva de aprendizaje adquirida por experiencias exitosas y también por los errores anteriores en la implementación de los requerimientos de la norma; 2) la organización se pone a tono con prácticas certificadas, lo que en sí mismo ya es una garantía razonable de que, a raíz de una buena implementación, mejorarán los procesos involucrados; 3) implementar la mejor forma de realizar los procesos implica ahorros considerables a las compañías en cuanto a tiempo, recursos

empleados, cumplimiento del marco legal aplicable si se adapta la norma certificable a la realidad normativa del entorno del negocio; todo esto repercute directamente en una disminución de costes y por ende en el mejoramiento de la eficiencia; 4) el alineamiento de los procesos con la norma certificable genera mejoras en la eficacia de la organización, dada su capacidad de efectuar solo aquellas tareas que contribuyen al logro de los objetivos del negocio.

Los enfoques de gestión del ciclo de vida de los servicios de infraestructura de tecnologías de la información y comunicación han presentado las mejores prácticas de prestación de servicios y la literatura debate cómo se pueden racionalizar las fases de desarrollo y explotación de servicios y qué objetivos deben perseguir los profesionales del servicio en cada fase (Hosono & Shimomura, 2017).

La Auditoria de Sistemas de Información ha pasado a tener un rol fundamental para ayudar a garantizar los atributos básicos que debe tener la información como la efectividad, la eficiencia, la confiabilidad, la integridad, la disponibilidad, el cumplimiento y la confiabilidad. (Valdéz, 2009).

La situación actual en el mundo de las normas y estándares que más o menos influyen en las TIC, puede describirse como un gran número de documentos y métodos que son muy diferentes pero tratan de administrar lo mismo en diferentes forma y enfoques (Maryska, Doucek & Nedomova, 2015).

Entre los sistemas de gestión de tecnología de información más conocidos se incluyen COSO [Committee of Sponsoring Organizations of the Treadway Commission Internal Control-Integrated Framework, EEUU 1992)], COBIT [Control Objectives for Information Related Technology], ITIL (Information Technologies Infrastructure Library), IT4IT (Information Technologies for Information Technologies), ISO 27001 y la declaración de la Norma de Auditoría No. 70 (Hosono & Shimomura, 2017; Haufe, Colomo, Dzombeta, Brandis & Stantchev, 2016; Fazlida & Said, 2015; Franco & Guerrero, 2013), los cuales son marcos de gestión del ciclo de vida de los servicios TIC, aunque sus resultados surgen de una diferencia de Ángulos de gestión (Hosono & Shimomura, 2017); como lo señalan Maryska, Doucek & Nedomova (2015), lo importante en este contexto es que la gestión de la informática empresarial está muy influenciada no sólo por los estándares antes mencionados directamente creados para, o al menos remotamente conectados con la tecnología de la información, sino también por muchas otras normas que aparentemente no tienen nada en común.

Zhi & Zhou (2013), clasifican las auditorías en tres grupos, basadas en la preparación del conocimiento relacionado, con la consideración de las reglas de auditoría de tecnología de la información, tales como COBIT, ISO17799 / 27001 ISO13335 ISO20000 ITIL SSE-CMM PCAOB2 normas de auditoría Basilea II BCM COSO / ERM y Etc., adoptando métodos de prueba de auditoría de TI, titulación a cargo y después de la auditoría a través del sistema de información.

Los Objetivos de control para la tecnología relacionada con la información (CobiT, Control Objectives for Information Related Technology), son un marco de gobernanza de las TIC y un conjunto de herramientas de apoyo, que permite a los administradores superar la brecha entre los requisitos de control, las cuestiones técnicas y los riesgos empresariales. COBIT permite un claro desarrollo de políticas y buenas prácticas para el control de las TIC en todas las organizaciones. COBIT hace hincapié en el cumplimiento normativo, ayuda a las organizaciones a aumentar el valor obtenido de las TIC, facilita la alineación y simplifica la implementación del marco de gobierno y control de las TIC de las empresas. COBIT se refiere a la organización, aunque no da mucho pensamiento a las acciones individuales en las organizaciones (Hosono & Shimomura, 2017).

La norma COBIT surge como una alternativa factible para ser utilizada como una guía de acción al momento de garantizar la calidad de los procesos relacionados con el monitoreo, control, calidad y seguridad de los datos correspondientes a transacciones contables; COBIT es la fusión entre prácticas de informática (ITIL, ISO/IEC 17799) y prácticas de control (COSO), las cuales plantean tres tipos de requerimientos de negocio para la información: requerimientos de calidad (calidad, costo y entrega de servicio), requerimientos fiduciarios (efectividad y eficiencia de operaciones, confiabilidad de la información y cumplimiento de las leyes y regulaciones), y por ´ultimo, requerimientos de Seguridad (confidencialidad, integridad y disponibilidad). Todo lo anterior bajo la auditoria o revisión de cuatro dominios de control, como lo son: planificación y organización, adquisición e implementación, entrega/soporte y monitoreo. Siendo una norma flexible para la auditoría de control, sus dominios pueden ser evaluados de manera aislada dependiendo de las necesidades de la gerencia (Graterol & Hernández, 2011).

En cuanto a las prácticas de control COSO, algunos autores, destacan que aunque el marco COSO, se ha utilizado ampliamente como una guía para evaluar el control interno, su carácter general no aborda la complejidad y los riesgos especiales inherentes a la tecnología de la información; incluso la versión

revisada de COSO 2013, ha sido criticada por no tratar específicamente la tecnología de la información.

Con respecto a la ISO 27.001, algunos autores la enumeran como el principal marco de seguridad de la información para atender el objetivo de seguridad de la información en el marco de la categoría ITG. Esta norma, anteriormente conocida como BS 7799, proporciona un conjunto formal de especificaciones para que las organizaciones manejen el riesgo de seguridad de la información y busquen la certificación para su Sistema de Gestión de la Seguridad de la Información (ISMS). La ISO 27001 podría sugerir controles de seguridad adecuados que puedan preservar con éxito la confidencialidad, integridad y disponibilidad de la información comercial y así poder integrar la seguridad de la información en las actividades y funciones diarias de una organización.

ITIL (Information Technologies Infrastructure Library) es una serie de documentos, que se utilizan para ayudar a la implementación de un marco de ciclo de vida para la gestión de servicios de tecnología de la información. Este marco personalizable define cómo se aplica la gestión de servicios dentro de una organización, y se alinea con la norma internacional, ISO 20000. ITIL se organiza en una serie de cinco elementos: estrategia de servicio, diseño de servicio, transición de servicio, operación de servicio y mejora continua del servicio, los describen un sistema de retroalimentación de bucle cerrado, que proporciona retroalimentación en todas las etapas del ciclo de vida. Los lineamientos de ITIL para cada elemento proporcionan mejores prácticas y disciplinas detrás de ellos para proporcionar servicios TIC de manera efectiva; ITIL no proporciona tareas o procedimientos concretos, y se confieren a la discreción de la interpretación del practicante individual (Hosono & Shimomura, 2017).

IT4IT (IT for IT), comprende una arquitectura de referencia y un modelo operativo basado en la cadena de valor para gestionar el negocio de la tecnología de la información. La introducción de un marco de esta cadena de valor a los proveedores de TIC ayudará a identificar las actividades que son especialmente importantes para el avance de la estrategia y el logro de metas. La cadena de valor se agrupa en dos categorías principales de actividades: 1) actividades primarias, que se refieren a la producción o entrega de bienes / servicios, y 2) actividades de apoyo, que facilitan la eficiencia y la eficacia de las actividades primarias. El estándar IT4IT divide la cadena de valor en cuatro flujos de valor para ayudar a adoptar la arquitectura de referencia IT4IT. Cada flujo de valor representa un área

clave de valor que las TIC proporcionan el ciclo de vida integral de los servicios. Los cuatro flujos de valor primarios son (1) estrategia para cartera, (2) requisito para implementar, (3) solicitud para cumplir y (4) detectar para corregir. Los flujos de valor primario para la cadena de valor de las TIC generalmente se alinean con lo que las TIC tradicionalmente llaman plan, construcción, entrega y ejecución. Cuando se utiliza con un modelo basado en la cadena de valor de las TIC, se transforma en plan, fuente, oferta y gestión. Estos flujos de valor tienen un papel vital en ayudar a ejecutar de manera integral todo el ciclo de vida del servicio. De esta manera, IT4IT examina las actividades a través del ciclo de vida (Hosono & Shimomura, 2017).

La norma internacional ISO / IEC para la gobernanza de la tecnología de la información, representa una herramienta eficaz de gestión de la informática empresarial a nivel estratégico; para hacerla utilizable para la gestión informática corporativa en su conjunto, es útil integrar sus procesos con los de gestión táctica y operativa; en general, ISO / IEC 38500 puede considerarse una muy buena base para la gestión estratégica de la informática corporativa, pero debe incluir indicadores específicos para: Interconectar el logro de los objetivos estratégicos de la organización y los servicios específicos de la informática corporativa, Evaluar la eficacia de los servicios TIC proporcionados (monitoreando tanto el costo como los ingresos de los servicios TIC), y Preparar un sistema eficaz de recopilación de datos para evaluar los servicios informáticos corporativos (Maryska, Doucek & Nedomova, 2015).

El estándar de referencia para la seguridad de la información - ISO / IEC 27001: 2013 (ISO, 2013), utiliza el enfoque PDCA establecido para impulsar la mejora continua; en este enfoque, la auditoría es la herramienta de gestión que proporciona a los interesados una confianza razonable en el logro de los objetivos de la organización; el enfoque moderno de la auditoría va más allá de la identificación de no conformidades con los requisitos y los hallazgos de auditoría son, junto con el monitoreo de procesos y métricas de desempeño, uno de los principales impulsores de la mejora continua de un sistema de gestión de la seguridad de la información (Graterol & Hernández, 2011).

La gestión de la seguridad de la información es un factor cada vez más determinante en la competitividad de las organizaciones; la gestión del riesgo y el aseguramiento de la información se apoyan en la aplicación de normas internacionales como el estándar ISO/IEC 27002.

Procedimiento para las auditorias de sistemas de tecnologías de información

En toda auditoría que se lleve a cabo en una empresa con el fin de determinar la razonabilidad de datos, funciones, operaciones, actividades, informes y reportes, la mayor parte del trabajo consiste en la recopilación de evidencia que sirva para sustentar las conclusiones, opiniones y recomendaciones; independientemente del tipo de auditoría que se esté realizando, sea financiera, operacional, administrativa, de seguimiento o de tecnología de información, siempre lo primero que debe hacer es saber a ciencia cierta, cuál es la evidencia que debe recopilar, en qué medio reside y cuáles son las posibilidades y medios para obtenerla; mientras no conozca estos aspectos de ninguna manera podrá saber qué es lo que necesita hacer y cómo lograr su objetivo (Espinoza, 2012).

Basado en su experiencia, Zhi & Zhou (2013), plantean que los procedimientos de auditoría informática incluyen la preparación previa, la auditoría in situ, la comunicación y el intercambio de opiniones, entre otras fases. Específicamente, plantean los tres pasos siguientes: 1) El auditor y el auditado, comparten el contenido de la auditoría, que incluye una lista previa de la información requerida por las partes, y requiere más o menos la mitad de un día a un día; 2) la auditoría in situ, donde se inspecciona el proyecto, y 3) Informe de auditoría, donde se emiten los resultados.

Al desempeñar su trabajo, el auditor se encuentra con diferentes sistemas de administración de la información implementados las organizaciones, sobre todo automatizados, como los registros contables, sistemas de personal, gestión de inventarios, transferencias bancarias electrónicas, registros biométricos, y la aparición de activos de tecnología que soportan estos sistemas como ser los servidores, redes, centrales de comunicación, son solo algunos ejemplos (Espinoza, 2016).

Actualmente, una de las debilidades de los auditores que no tienen formación en ingeniería de sistemas y que seguramente de muchas otras profesiones que realizan las labores de fiscalización control y supervisión, es la carencia de entendimiento de las tecnologías de la información dentro de las organizaciones a nivel de control y riesgos (Espinoza, 2016).

Las normas internacionales de auditoría establecen que el auditor debe contar con conocimientos suficientes, dentro lo que comprende el enfoque moderno de auditoría basada en riesgos, estos conocimientos se refieren a habilidades y competencias para el examen de los controles de aplicación que están directamente relacionados a los procesos del negocio, pero también llegar a comprender los

controles generales de las tecnologías de la información, ya que a través de la comprensión e identificación de los probables riesgos y de los controles clave, puede planificar, dirigir, supervisar y revisar el proceso (Espinoza, 2016).

En este sentido, Espinoza (2016) agrega que, ante diversos fraudes de toda índole ocurridos a través del uso de la tecnología cada vez más sofisticada, se ha convertido en un gran reto para el auditor en el campo el cual se desempeña, exigiéndole a contar con mayores habilidades y competencias en este campo, para dar un valor agregado a las organizaciones inclusive en tiempo real y minimizando el riesgo de auditoría.

Franco & Guerrero (2013), plantearon una metodología que permite asumir práctica y eficientemente la verificación de controles de seguridad informática soportada desde un sistema que orienta el proceso de auditorías de seguridad; este sistema involucra en su estructura y funcionamiento las siguientes fases metodológicas: Creación, Activación, Ponderación, Argumentación, Valoración, Cierre, Reclamación y Finalización. Basado en la ISO 27.002, los autores señalan que el sistema puede evolucionar, en futuras versiones, con la adaptación de otros modelos o estándares de evaluación diferentes a ISO 27002, tales como OSSTMM y COBIT.

Como lo señalan Graterol & Hernández (2011), la madurez en el desempeño puede utilizarse como punto de referencia para la comparación y como una herramienta para comprender las mejores prácticas en gestión de auditorías informáticas y lograr el cumplimiento de un conjunto de requisitos.

La estrategia utilizada para la implementación de las mejores prácticas de control, es un proceso de benchmarking, que toma en cuenta las mejores recomendaciones internacionales de instituciones que orientan las auditorías informáticas a nivel mundial, las normas contenidas en el COBIT, las utilizadas por empresas de prestigio internacional, las normas internacionales de auditoría, entre otros; los que permiten obtener altos niveles de seguridad, fiabilidad y conformidad en la gestión de la tecnología de la información (Ramírez & Álvarez, 2003).

Por otro lado, se nota una escasa participación de la comunidad académica en la investigación relacionada con el uso de la tecnología en los procesos de auditoría, sustentado fundamentalmente en que la mayoría de estudios que se han llevado a cabo son desarrollados por firmas de auditoría o agrupaciones profesionales. Es importante tener en cuenta que para obtener apropiada evidencia de

auditoría, se debe acudir a técnicas acordes a la realidad de la organización, y la realidad no es análoga, es digital, por lo tanto el auditor debe utilizar las diferentes técnicas y herramientas de auditoría asistidas por computador como soporte de su labor profesional, y ponerse a tono con la realidad organizacional (Valencia & Tamayo, 2012). El profesional, en su papel de auditor, de igual manera tendrá que cambiar y desarrollar nuevas técnicas de auditoría a medida que progresa la tecnología (Valdéz, 2009).

Conclusiones

Lo más importante que debe considerar un auditor es conocer con propiedad, cual es la evidencia que debe recopilar; si no se prepara antes del proceso de auditoría, todo el proceso puede estar cuestionado por las partes involucradas. Un adecuado indicador de madurez en el desempeño puede utilizarse como referencia para la comparación y como una herramienta para comprender las mejores prácticas en gestión de auditorías informáticas. La Auditoría Informática permite a las organizaciones, alcanzar los estándares internacionales en el uso adecuado de las tecnologías de información, con miras a una certificación de calidad; así mismo, da cuenta del uso adecuado de los controles de de riesgos de mayor impacto.

Finalmente, la elección del marco adecuado es vital para asegurar que los profesionales hagan referencia al mejor marco para una gestión eficaz de la seguridad de la información. Algunos autores argumentan que COBIT podría ayudar a la alta gerencia a tener una excelente capacidad de gestión de la seguridad de la información con una alineación con los objetivos estratégicos generales del negocio; otros agregan que COBIT es útil para ayudar a la organización en términos de cumplimiento con la regulación y seguridad de la seguridad de la información. Sin embargo, la mayoría termina señalando que la combinación de los Estándares de Auditoría (ISA, SOX) y los Estatutos de la Organización de Seguridad de la Información (COSO, COBIT, ISO27001 / BS7799), sería el mejor enfoque para ayudar a los auditores en la búsqueda de la excelencia en la gestión de auditorías informáticas.

Referencias bibliográficas

Alfonso, Y.; Blanco, B. & Loy, L. (2012). Auditoría con Informática a Sistemas Contables. Revista de Arquitectura e Ingeniería, 6(2), 1-14.

Dávalos, A. (2013). Auditoria de seguridad de información. Fides Et Ratio, 6(6), 19-30.

Dekker, M. & Etalle, S. (2007). Audit-Based Access Control for Electronic Health Records. Electronic Notes in Theoretical Computer Science, 168, 221-236. DOI: http://dx.doi.org/10.1016/j.entcs.2006.08.028

Díaz, R. (2012). Marco de referencia para auditorías integrales de sistemas en las mipymes colombianas. Gestión & Sociedad, 5(1), 15-29.

Espinoza, S. (2012). Las pistas de auditoría. Ciencias Económicas, 30(1), 467-482.

Espinoza, W. (2016). La tecnología de la información como herramienta construccionista para el auditor financiero hibrido. Fides Et Ratio, 11, 17-35.

Fazlida, M. & Said, J. (2015). Information Security: Risk, Governance and Implementation Setback. Procedia Economics and Finance, 28, 243-248. DOI: http://dx.doi.org/10.1016/S2212-5671(15)01106-5

Franco & Guerrero, (2013). Sistema de Administración de Controles de Seguridad Informática basado en ISO/IEC 27002. Eleventh LACCEI Latin American and Caribbean Conference for Engineering and Technology (LACCEI'2013) "Innovation in Engineering, Technology and Education for Competitiveness and Prosperity" August 14 - 16, 2013 Cancun, Mexico.

Governance Institute (2000). Audit Guidelines COBIT. 3era. Edición. USA. Disponible en: http://www.isaca.org (Consulta: Agosto 2017).

Graterol, C. & Hernández, A. (2011). Aplicación de la norma COBIT en el monitoreo de transferencias electrónicas de datos contable-financieros. Publicaciones en Ciencias y Tecnología, 5(1), 27-42.

Haufe, K.; Colomo, R.; Dzombeta, S.; Brandis, K. & Stantchev, W. (2016). Security Management Standards: A Mapping. Procedia Computer Science, 100, 755-761. DOI: http://dx.doi.org/10.1016/j.procs.2016.09.221

Hernández, A. (2010). Auditoría Informática y Gestión de Tecnologías De Información y Comunicación (TICs). Compendium, 13(25), 3-4.

Hohan, A.; Olaru, M. & Pirnea, I. (2015). Procedia Economics and Finance, 32, 352-359. DOI: http://dx.doi.org/10.1016/S2212-5671(15)01404-5

Hosono, S. & Shimomura, Y. (2017). Bridging On-site Practices and Design Principles for Service Development. Procedia CIRP, 60, 422-427. DOI: http://dx.doi.org/10.1016/j.procir.2017.02.018

ISO (2013). ISO/IEC 27001:2013 - Information technology -- Security techniques -- Information security management systems - Requirements. Ginebra: International Standardisation Organisation.

Maryska, M.; Doucek, P. & Nedomova, L. (2015). Corporate Informatics and Strategic Management. Procedia Economics and Finance, 26, 651-656. DOI: http://dx.doi.org/10.1016/S2212-5671(15)00806-0

Montilla, O. & Herrera, L. (2006). El deber ser de la auditoría. Estudios gerenciales, 98, 83-110.

Pablos, de, C.; López, J.; Martín, S.; Medina, S.; Montero, A. & Najera, J. (2006). Dirección y gestión de los sistemas de información en la empresa: una visión integradora, 2da edición. Madrid: ESIC.

Pinilla, J. (1994). Las normas de auditoría informática. INNOVAR, 4, 31-34. DOI: http://dx.doi.org/10.15446/innovar

Ramírez, G. & Álvarez, E. (2003). Auditoría a la Gestión de las Tecnologías y Sistemas de Información. Industrial Data, 6(1), 99-102.

Scalabrin, I. & Dinis, R. (2016). IT Governance mechanisms in higher education. Procedia Computer Science, 100, 941-946. DOI: https://doi.org/10.1016/j.procs.2016.09.253

Tarouco, H.H. & Graeml, A.R. (2011). Governança de tecnologia da informação: um panorama da adoção de modelos de melhores práticas por empresas brasileiras usuárias. Revista de Administração, 46(1), 7-18. DOI: https://doi.org/10.5700/rausp0994

Valdéz, E. (2009). Tendencias de la auditoria informática. Ingenium, 4(8), 69-98. DOI: https://doi.org/10.21774/ing.v4i8.132

Valencia, F. & Tamayo, J. (2012). Evidencia digital y técnicas y herramientas de auditoría asistidas por computador. Ventana informática, 26, 93-110.