

Auditoría de Sistema de TI como medio de aseguramiento de control en las empresas del Siglo XXI

IT audit System as a means of control assurance in 21st-century companies

TI auditoria do sistema como um meio de proteger as empresas de controle do século XXI

Omar Téllez Barrientos

Universidad Tecnológica de Tecámac, México

omar_tellez76@hotmail.com

Moramay Ramírez Hernández

Universidad Tecnológica de Tecámac, México

moramayrh@hotmail.com

Angelina Díaz Alva

Universidad Tecnológica de Tecámac, México

angelinadial@yahoo.com.mx

Resumen

En pleno siglo XXI, en la era de internet, las comunicaciones y la digitalización, la auditoría de sistemas de TI se ha convertido en un factor clave para el cumplimiento de los objetivos organizacionales a través de la correcta utilización de los sistemas de información y de los servicios de TI.

Hoy en día los sistemas de información son un común denominador en las empresas pues a través de ellos las diferentes áreas: recursos humanos, finanzas, producción, mercadotecnia, compras y ventas, pueden realizar sus tareas diarias, todo esto gestionado por el área de sistemas e informática.

El éxito de la funcionalidad y operatividad de los sistemas de información depende de que estén alineados con los objetivos del negocio y, sobre todo, de que cubran los procesos adecuados en

su automatización. No existe empresa u organización del siglo XXI que no cuente con sistemas de información que permitan a estas empresas volverse altamente productivas y competitivas. Para que las empresas sean productivas y competitivas desde el escenario informático, aplicar una auditoria de sistemas de TI se convierte en un factor clave. Esto asimismo permite revisar y evaluar que los recursos informáticos con que cuenta la empresa sean utilizados correctamente.

Palabras clave: Sistemas de Información, Sistema ERP y CRM, Plataforma informática, TIC.

Abstract

In the XXI century, in the age of internet, communications and digitization, the audit of IT systems has become a key factor for the fulfillment of the organizational objectives through the correct use of the systems of information and IT services.

Nowadays information systems are a common denominator in the companies because through them the different areas: human resources, finance, production, marketing, purchasing and sales, can perform their daily tasks, all of this is managed by the area of information systems and information technology.

The success of the functionality and operation of information systems depends on that they are aligned with the business objectives and, above all, that cover appropriate automation processes. There is no company or organization of the 21st century that does not have information systems that allow these companies become highly productive and competitive.

So the companies are productive and competitive from the stage computer, apply an audit of systems of TI is converts in a key factor. This also allows you to review and evaluate the resources with which the company has to be used properly.

Key Words: Information System, ERP system, CRM system, computing platform, ICT.

Resumo

No século XXI, na era da Internet, comunicações e digitalização, sistemas de TI de auditoria tornou-se um factor essencial para o cumprimento dos objetivos organizacionais através da utilização adequada dos sistemas de informação e Serviços de TI.

Hoje os sistemas de informação são um denominador comum em empresas, porque através deles as diferentes áreas: recursos humanos, finanças, produção, marketing, compras e vendas,

eles podem executar suas tarefas diárias, tudo o que conseguiu pela área de sistemas e tecnologia da informação.

O sucesso da funcionalidade e da operação de sistemas de informação depende de que estão alinhados com os objetivos de negócios e, acima de tudo, cobrindo os processos de automação apropriadas. Nenhuma empresa ou organização século XXI que não tem sistemas de informação que permitem que essas empresas tornam-se altamente produtivo e competitivo.

Para as empresas para ser produtivo e competitivo do cenário computador, aplique uma auditoria de sistemas de TI torna-se um fator chave. Isso também permite revisar e avaliar os recursos informáticos da empresa são usados corretamente.

Palavras-chave: Sistemas de Informação, ERP e sistema de CRM, plataforma de computação, as TIC.

Fecha recepción: Enero 2016

Fecha aceptación: Junio 2016

Introducción

La tecnología siempre ha sido parte de la vida del hombre. Desde tiempos prehistóricos, el hombre ha usado su inteligencia para crear tecnologías que le permitan contar con herramientas con las cuales pudiera hacer mejor sus labores. La tecnología desde ese momento y a raíz de las necesidades del hombre ha evolucionado constante y aceleradamente, sobre todo ahora cuando muchas acciones humanas se hacen con insumos y productos tecnológicos de carácter computacional.

Las TIC hoy en día están en todas partes, dicho de otra forma, las tecnologías de la información y comunicación son una herramienta que las personas y empresas de este siglo utilizan diariamente para revisar su correo electrónico, hablar por teléfono, monitorear las redes sociales, chatear con amigos, etcétera.

Los sistemas de información ayudan a cumplir los objetivos organizacionales, pero sobre todo las tecnologías de información ya que son clave para la funcionalidad. También implementar los sistemas ERP, CRM, SIA, entre otros, permite que las diferentes áreas de la empresa realicen sus actividades y obtengan de manera precisa los resultados esperados.

Figura 1. Elementos que forman parte de las TIC.



Marco Teórico

Sistemas de Información

Un Sistema de Información es el conjunto de elementos debidamente organizados de hardware y software, orientados al procesamiento y almacenamiento de grandes cantidades de información, para el cumplimiento de los objetivos organizacionales de las empresas.

Sistemas ERP

Un Sistema ERP es un sistema computacional que te permite gestionar y controlar de cierta manera los recursos, los procesos y las operaciones de una empresa o negocio. Estos sistemas funcionan a través de módulos y su idea principal es gestionar la cadena de producción de la empresa. Sus siglas significan planeación de recursos empresariales.

Sistemas CRM

Un Sistema CRM es un sistema computacional que permite gestionar las relaciones con los clientes de manera organizada; asimismo es una estrategia orientada a fidelizar y satisfacer al cliente, por lo que a veces se denomina gestión del servicio al cliente. Este sistema también motiva al área de mercadotecnia.

Auditoría de Sistemas de Tecnologías de Información

Dicha auditoría es el conjunto de técnicas y procedimientos que permiten revisar y evaluar los sistemas de información y los servicios de TI de las empresas, basados en la normatividad informática y los estándares de la organización.

Auditoría

Es el proceso de revisión y evaluación “inspección o verificación”, de una actividad o proceso que se realiza en la empresa.

Procesos

Un proceso es una secuencia de pasos dispuesta con un tipo de lógica que se enfoca en lograr algún resultado específico. Los procesos son mecanismos de comportamiento que diseña el personal, para mejorar la productividad de algo, establecer un orden o eliminar algún tipo de problema.

Plataforma Informática

Una plataforma informática está compuesta por 3 elementos importantes: plataforma de hardware (tarjeta madre, microprocesador, memoria RAM, ranuras de expansión, fuente de alimentación), sistema operativo (programa principal de un equipo de cómputo, gestor de los recursos de hardware y software), y software de aplicación (conjunto de aplicaciones que permiten realizar una tarea específica en el equipo de cómputo).

Usuarios

Un usuario es el individuo que trabaja o utiliza un objeto o dispositivo que usa algún servicio en particular. El concepto de usuario informático es la persona que utiliza una computadora, sistema operativo, software de aplicación y que tiene diferentes permisos para entrar a un sistema en línea o de manera local realizar las actividades encomendadas.

Control Interno

Se puede definir como “cualquier actividad o acción realizada manual y/o automáticamente para prevenir, corregir errores o irregularidades que pueden afectar el funcionamiento de un sistema para conseguir sus objetivos”.

Los controles cuando se diseñan, desarrollan e implementan han de ser por lo menos completos, simples, fiables, revisables, adecuados y rentables. Los controles internos utilizados en el entorno informático continúan evolucionando a medida que los sistemas de información se vuelven complejos. Los progresos que se producen en la tecnología de soportes físicos y de software han modificado de manera significativa los procedimientos que se empleaban tradicionalmente para controlar los procesos de aplicaciones y para gestionar los sistemas de información.

Control Interno Informático

Una de las actividades más importantes del área de sistemas e informática en una organización del siglo XXI, es el control interno informático. Dicha actividad se ejecuta en el control de los sistemas de información y servicios de TI, ya que es la encargada de monitorear su eficiencia y eficacia. Se basa en los siguientes objetivos:

- Establecer la seguridad y la protección de los activos de la empresa.
- Promover la confidencialidad, oportunidad y veracidad de los registros contables y de la emisión de la información financiera de la empresa.
- Incrementar la eficiencia y eficacia en el desarrollo de las operaciones y actividades de la empresa.
- Establecer y hacer cumplir las normas, políticas y procedimientos que regulan las actividades de la empresa.
- Implementar los métodos, técnicas y procedimientos que permitan desarrollar adecuadamente las actividades, tareas y funciones de la empresa.

Figura 2. Funciones del control interno informático



Objetivos de la Auditoría de Sistemas de TI

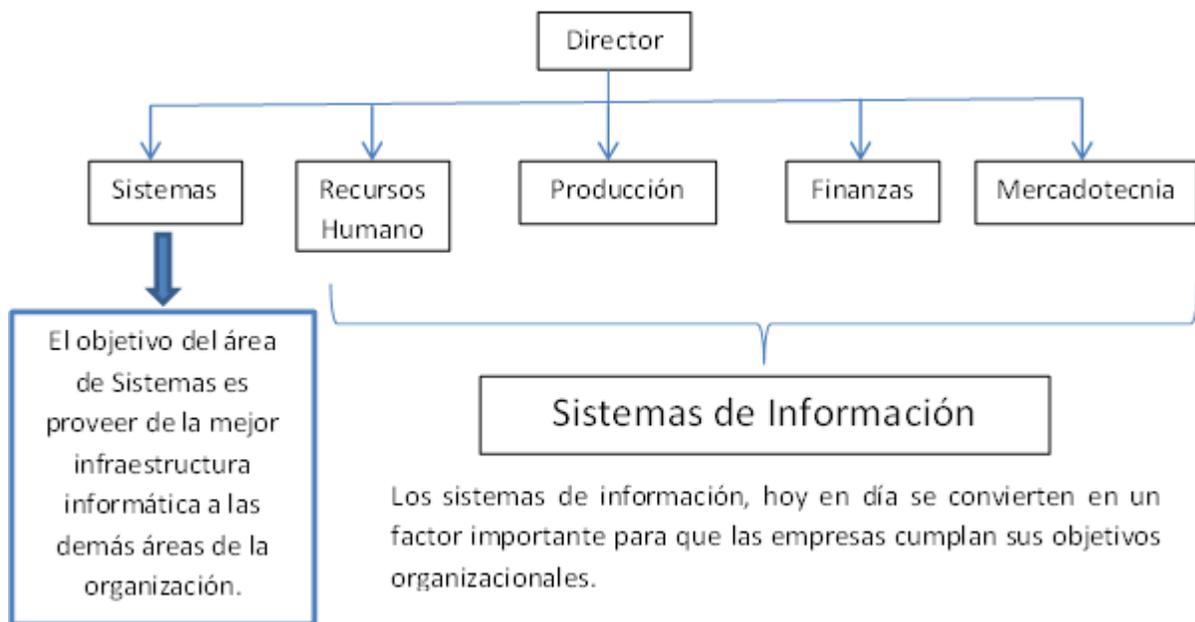
- Incrementar la satisfacción de los usuarios de los sistemas de información.
- Asegurar una mayor integridad, disponibilidad y confidencialidad de la información, mediante controles adecuados y recomendaciones de seguridad.
- Minimizar la existencia de riesgos informáticos en el uso de las tecnologías de información.
- Conocer la situación actual del área de informática y las actividades y los esfuerzos necesarios para lograr los objetivos organizacionales.
- Ubicar la auditoría de TI dentro de los objetivos y metas de la organización, desde el punto de vista estratégico.
- Identificar los elementos teóricos que intervienen en la disciplina de auditoría y su relación con la Auditoría de Sistemas de Tecnologías de Información.
- Identificar los Modelos de Referencia, las Metodologías y las Herramientas que apoyan la actividad de Auditoría de Sistemas de TI.

Método

La información que trata una organización es un recurso crítico que debería ser protegido, ya que es la base de la mayoría de las decisiones que se toman.

Para tener una seguridad razonable sobre si la información es exacta y completa, está disponible cuando se necesita y es confidencial, es necesario implementar controles internos informáticos que ayudan a cumplir con las exigencias legales en materia de derecho informático y asegurar que los sistemas de información y servicios de TI funcionen de acuerdo a lo que se espera de ellos.

Figura 3. Áreas funcionales de la Organización



Los sistemas de información permiten realizar las actividades diarias a todo el personal de la empresa, y se convierten en una herramienta informática muy importante para el cumplimiento de sus tareas diarias.

La selección correcta de la plataforma informática para cada área es fundamental. El equipo de especialistas del área de sistemas tiene la tarea de realizar un estudio de necesidades, tomando como base las actividades y funciones que se realicen en cada área funcional de la organización.

Los escándalos “contables y administrativos” del siglo pasado y de este siglo, han provocado un aumento en la sensibilización, tanto de los reguladores como de las organizaciones (públicas y privadas) por el control interno. La existencia de nuevas normativas al respecto, las necesidades de transparencia en la gestión como un activo más de las organizaciones o la búsqueda de la eficiencia en los procesos internos, han actuado durante los últimos años como catalizadores para la mejora de los mecanismos de control interno en las organizaciones.

Ahora existen varias metodologías que permiten realizar una auditoría de sistemas de TI; diferentes autores e instituciones auditoras presentan sus etapas y procedimientos para realizar esta actividad, tomando en consideración que el objetivo de las auditorías de sistemas de TI, es verificar y comprobar el correcto funcionamiento de los recursos informáticos.

Con el propósito de aplicar correctamente esta metodología para realizar la auditoría de sistemas de TI, la cual puede ser aplicable para cualquier campo del área de sistemas e informática, a continuación se presentan todas las fases y pasos que se deben seguir para determinar la correcta funcionalidad de los recursos informáticos.

Figura 4. Elementos que integran un sistema de información



Etapas del Proceso de la Auditoría de Sistemas de TI

1a. Etapa “Conocimiento del área a Auditar”

En esta etapa se debe llevar a cabo una visita a las instalaciones de la empresa que se va a auditar con el objetivo de que el auditor y su equipo de trabajo conozcan las áreas, el personal y los procesos de la organización para poderse involucrar con los objetivos de la auditoría.

Tabla 1. Etapa 1 Conocimiento del área a auditar

Etapa 1	ACTIVIDADES A DESARROLLAR
<p>Conocimiento del área auditada o del sistema</p>	<p>1. Identificar el origen de la auditoría</p> <p>En este punto es de suma importancia determinar cuál fue el origen de la auditoría, que pudo ser por solicitud expresa de la gerencia o presidencia de la organización o por una entidad externa, con el objetivo de conocer el estado de los recursos informáticos de la organización.</p>
	<p>2. Realizar visitas para conocer procesos de la organización, activos informáticos y área auditada</p> <p>En este punto el auditor debe hacer una entrevista de acercamiento, con el objetivo de conocer las instalaciones, los trabajadores, los funcionarios y directivos, y también para poder identificar la problemática de la organización.</p>
	<p>3. Determinar las vulnerabilidades y amenazas informáticas a que está expuesta la organización</p> <p>Una vez hecha la visita preliminar, el auditor debe identificar las vulnerabilidades encontradas y amenazas para elaborar un plan que sirva de guía para la realización de la auditoría, siempre tomando en cuenta los objetivos de ésta.</p>
	<p>4. Determinar el objetivo de la auditoría de acuerdo a las vulnerabilidades, y amenazas informáticas encontradas</p> <p>El desarrollo de la auditoría de sistemas significa plantear todos los aspectos a evaluar.</p>

2a. Etapa “Planeación de la Auditoría de Sistemas de TI”

El primer paso para realizar una auditoría en sistemas de TI, es definir las actividades necesarias para su ejecución, lo cual se logrará mediante una adecuada planeación; es decir, se deben identificar claramente las razones por las que se va a realizar la auditoría y cuál es su objetivo, así como el diseño de los métodos, técnicas y procedimientos necesarios para llevarla a cabo y para preparar los documentos que servirán de apoyo para su ejecución, culminando con la elaboración documental de los planes, programas y presupuestos.

Concretamente, el responsable de la planeación de esta primera etapa de la metodología para una auditoría de sistemas de TI debe empezar por plantearse las siguientes preguntas:

1. ¿Por qué se realizará la auditoría?
2. ¿Se debe hacer una visita preliminar al área de sistemas?
3. ¿Cuál es el objetivo que se pretende alcanzar con esta auditoría?

Debido a la importancia de identificar cada uno de los puntos que integran esta primera etapa de la metodología para la auditoría de sistemas de TI, a continuación se enlistan los principales puntos propuestos para su planeación:

Tabla 2. Etapa 2 Planeación de la Auditoria de Sistemas de TI

Etapa 2	ACTIVIDADES A DESARROLLAR
<p>Planeación de la Auditoria de Sistemas</p>	<p>1. Elaborar el plan de auditoría</p> <p>Este punto es de suma importancia ya que aquí se determinan todas las actividades que se realizarán para llevar a cabo la auditoría de sistemas. El auditor líder es total responsable del cumplimiento de todas las actividades planeadas para el desarrollo de la auditoría.</p>
	<p>2. Seleccionar los estándares a utilizar de acuerdo al objetivo de la auditoría</p> <p>Aquí se determinan los estándares a utilizar dependiendo del objetivo de la auditoría, y del segmento o área a revisar y evaluar (Cobit, Magerit, Octave, ISO 27000, ISO 27005).</p>
	<p>3. Seleccionar los ítems que serán evaluados</p> <p>Una vez que se han determinado los objetivos de la auditoría se deben relacionar los aspectos a evaluar, y para esto se deben considerar aspectos específicos del área de informática y de sistemas computacionales, tales como: la gestión administrativa del área informática y el centro de cómputo, el cumplimiento de las funciones del personal informático y usuarios de los sistemas, los sistemas en desarrollo, la operación de los sistemas en producción, los programas de capacitación para el personal del área y usuarios de los sistemas, protección de las bases de datos, datos confidenciales y acceso, protección de las copias de seguridad y la restauración de la información, entre otros aspectos.</p>
	<p>4. Seleccionar el equipo de trabajo y asignar actividades</p> <p>En este punto el auditor debe hacer un proceso de selección previo a la auditoría para adquirir su equipo de trabajo, asignar las actividades previamente establecidas y cumplir con los objetivos de la auditoría de sistemas de TI.</p>
	<p>5. Determinar las actividades que se llevarán a cabo</p> <p>Este punto se basa en el cumplimiento del plan de trabajo establecido al inicio de la auditoría. Asignar las actividades y los tiempos para el equipo de</p>

	auditores es una tarea de suma importancia para el auditor líder y también para la asignación de presupuestos.
	6. Seleccionar los instrumentos para la evaluación Aquí se determina la documentación y los medios necesarios para llevar a cabo la revisión y evaluación en la empresa, seleccionando o diseñando los métodos, procedimientos, herramientas e instrumentos necesarios de acuerdo a los planes, presupuestos y programas establecidos anteriormente.
	7. Diseñar el plan de pruebas Diseñar los sistemas, programas y métodos de pruebas para la auditoría.

3a. Etapa “Ejecución de la Auditoría de Sistemas de TI”

El siguiente paso después de la planeación de la auditoría es su ejecución, la cual estará determinada por las características concretas, los puntos y requerimientos que se estimaron en la etapa de planeación.

Debido a que esta etapa es especial, en la planeación sólo se indican los puntos más importantes que se aplicarán de acuerdo a las características específicas de la auditoría que se trate. Los principales puntos son los siguientes:

Tabla 3. Etapa 3 Ejecución de la Auditoría de Sistemas de TI

Etapa 3	ACTIVIDADES A DESARROLLAR
Ejecución de la Auditoría de Sistemas	<p>1. Realizar las acciones programadas para la auditoría</p> <p>De acuerdo con el programa de auditoría, cada auditor tiene que realizar las actividades que le corresponden conforme fueron diseñadas, de acuerdo a la cronología asignada a cada una, y a los tiempos y recursos que se deben utilizar. El propósito es ejecutar los eventos programados y alcanzar el objetivo.</p>
	<p>2. Aplicar los instrumentos y herramientas para la auditoría</p> <p>Conforme a la guía de auditoría, se tienen que utilizar uno a uno los instrumentos y herramientas elegidos para llevar a cabo la evaluación, ya sea mediante la recopilación y análisis de la información, la observación, las pruebas y simulaciones de los sistemas, o mediante cualquier otro instrumento de los que se diseñaron previamente para esta revisión.</p>
	<p>3. Identificar y elaborar los documentos de desviaciones encontradas</p> <p>Una vez que se realizaron las actividades diseñadas en el programa de trabajo de auditoría, que se utilizaron los instrumentos de recopilación de información y/o se utilizaron los instrumentos determinados para la auditoría, entonces se buscan las posibles desviaciones y se procede a elaborar los documentos de desviaciones, en los cuales se anotan las situaciones encontradas, las causas que las originaron y sus posibles soluciones, así como los responsables de solucionar dichas desviaciones y las posibles fechas para hacerlo.</p>
	<p>4. Elaborar el dictamen preliminar y presentarlo a discusión</p> <p>Una vez que el auditor determinó las desviaciones encontradas durante la evaluación, debe elaborar un documento que contenga todas las desviaciones detectadas, o lo puede elaborar con cada una de las desviaciones por separado, de acuerdo a las necesidades de la empresa.</p>

Ejecución de la Auditoría de Sistemas	<p>Una vez hecho esto, es obligación del auditor comentarlas con las personas involucradas directamente en las desviaciones, a fin de encontrar de manera conjunta las causas que las originaron y a partir de ese intercambio de opiniones determinar las posibles soluciones para cada causa. También puede asignar a los responsables de solucionarlas y, de ser posible, las fechas para hacerlo.</p>
	<p>5. Integrar el legajo de papeles de trabajo de la auditoría</p> <p>El auditor tiene la obligación de conservar en el llamado legajo de papeles de la auditoría cada uno de los instrumentos aplicados en la evaluación, con el propósito de sustentar, llegado el caso, las observaciones reportadas.</p>

4a. Etapa “Dictamen de la Auditoría de Sistemas de TI”

El último paso de la metodología que hemos estudiado en este artículo es emitir el dictamen, que es el resultado final de la auditoría de sistemas de TI. Para ello presentamos los siguientes puntos:

Tabla 4. Etapa 4 Dictamen de la Auditoría de Sistemas de TI

Etapa 4	ACTIVIDADES A DESARROLLAR
<p>Dictamen de la Auditoría de Sistemas</p>	<p>1. Analizar la información y elaborar un informe de situaciones detectadas</p> <p>La actividad previa, o más bien paralela, a la detección de las desviaciones, es el análisis de los papeles de trabajo y la elaboración en borrador de las llamadas situaciones detectadas; el propósito es que el auditor elabore su borrador y comente las desviaciones con los auditados. Después de comentarlas, debe elaborar las modificaciones pertinentes, así como el informe definitivo de las situaciones encontradas.</p>
	<p>2. Elaborar el dictamen final</p> <p>El auditor debe terminar de elaborar el informe de auditoría de sistemas y complementarlo con el dictamen final (opinión del auditor), y después presentarlo a los directivos del área de sistemas auditada para que conozcan la situación actual de dicha área, antes de presentarlo al responsable de la empresa.</p>
	<p>3. Presentar el informe de Auditoría</p> <p>El último paso de esta metodología que hemos estudiado es presentarle formalmente el dictamen de la auditoría al más alto directivo de la empresa, con el propósito de informarle sobre los resultados. Esta presentación se debe hacer con toda la formalidad del caso, con la elaboración correcta y profesional del dictamen de la auditoría y en medio de una reunión directiva. El informe de auditoría debe contener los siguientes puntos:</p> <ol style="list-style-type: none"> 1. La carta de presentación 2. El dictamen de la auditoría 3. El informe de situaciones relevantes 4. Anexos y cuadros adicionales

Conclusiones

El contenido de este artículo ofrece un panorama más amplio y actual de la implementación de una auditoría de sistemas de TI en las empresas de este siglo. A través de ésta se asegura y comprueba que los sistemas de información y los servicios de TI funcionen correctamente y, sobre todo, cumplan los objetivos para los cuales fueron implementados.

Siguiendo esta metodología se pueden alcanzar los objetivos propuestos en este artículo. El objetivo de la auditoría de sistemas de TI es revisar y evaluar los mecanismos de control, seguridad y respaldo de la información dentro de las empresas del siglo XXI, sobre todo con una visión a futuro que permita involucrar la planeación estratégica de TI y minimizar los riesgos físicos, lógicos y humanos que producen fraudes en las empresas.

Bibliografía

- Anónimo (2007). ¿Qué son los sistemas ERP? Consultado en <http://www.informatica-hoy.com.ar> – (Qué son los sistemas ERP)
- Avron, Barr (2009). Comité IEEE Learning Technology Standards. Consultado en <http://ltsc.ieee.org/index.html>
- Hackathon (2016). IEEE Learning Technology Standards Committee (LTSC) Systems Interoperability in Education and Training. Consultado en <http://ltsc.ieee.org/>
- Jennifer Bayuk, (2009). Information Systems Audit: The Basics. Consultado en <http://www.csoonline.com/article/2124025/it-audit/information-systems-audit--the-basics.html>
- Manauere, Adolfo (2013). ISACA Actualiza los Estándares de Auditoría y Aseguramiento de SI. Consultado en <http://www.cioal.com/2013/07/23/isaca-230713/>
- Muñoz, C. (2001). Auditoría de Sistemas Computacionales, núm. 3, primera edición, Editorial Prentice Hall, 137 pp.
- Piattini, M., Del Peso, E., Del Peso, M. (2008). Auditoría de Sistemas y Tecnologías de Información, primera edición, Alfaomega 53 pp.
- Patrocinador IEEE Computer Society (1992). 1002-1987 - IEEE Standard Taxonomy for Software Engineering Standards. Consultado en <http://standards.ieee.org/findstds/standard/1002-1987.html>
- Yusmeri Brito, Leimar Suárez, Liskelic Pineda. Estándares para la Auditoría de Sistemas. Consultado en <http://auditorianormasorg.jimdo.com/estandares-de-auditoria-de-sistemas/>
- Vidal Gonzales, Bernabé (2014). Auditoría Interna. Consultado en <http://myslide.es/documents/auditoria-interna-55845ffbea609.html>