IDEAS EN CIENCIAS DE LA INGENIERÍA
Facultad de Ingeniería, Universidad Autónoma del Estado de México

Las Metodologías de la Auditoría Informática y su relación con Buenas Prácticas y Estándares

Informatic Auditing Methodologies and its relations with Best Practices and Standards

Silvia Edith Albarrán Trujillo,[1,*]
Juan Carlos Pérez Merlos,[1] Mireya Salgado Gallegos,[1]
Laura Luz Valero Conzuelo[1]

Recibido: 24 de noviembre de 2017 - Aceptado: 23 de enero de 2019

Resumen
Las Auditorías Informáticas que se realizan en las organizaciones empresariales deben utilizar metodologías de apoyo, sin embargo, no existe una metodología única o una que sea reconocida de manera generalizada, su uso depende de la experiencia del auditor y del conocimiento de esta. Varios autores proponen metodologías de Auditoría Informática, y si bien, existen similitudes, se requiere complementarlas con buenas prácticas y estándares mundialmente aceptados. Estos apoyarían su uso en ¿cómo cumplir con los aspectos solicitados?, el fin es robustecerlas y minimizar la parte subjetiva que tienen de manera general las Auditorías, al ser ejecutadas. El objetivo de este artículo es realizar una revisión y descripción de las buenas prácticas para la gestión de las Tecnologías de Información que sirven para fortalecer las metodologías de las Auditorias Informáticas.

Palabras clave: Metodologías, Auditoría Informática, buenas prácticas de TI

Abstract
Informatics Auditing in the *enterprise organizations* could use methodologies to make easy the work, but there is not a unique methodology or one such general that can be used by everybody, the use of this depends on the experience of the auditor and whether him has confidence with it. Some authors around the world have proposed different methodologies and they have coincidences, but they need to be completed with *good practices* o *accepted standards*. The good practices help to answer the question, how to get the different aspects considered in audits? The idea is to make them stronger and minimize the subjective part of all activities of evaluation.
Key words: Auditing methodologies, good practices in IT.

[1]Universidad Autónoma del Estado de México, México.
*Autor de correspondencia: siedaltr@gmail.com.

Introducción

Las Auditorías Informáticas (AI) son realizadas en las organizaciones desde hace mucho tiempo, son evaluaciones basadas en la experiencia del auditor y metodologías propuestas por diversos autores, no hay metodologías utilizadas como estándar o de forma generalizada. Enrique Hernández (1993) señala que la función de Auditoría de Informática debe contar con un desarrollo de actividades basadas en un método de trabajo formal que sea entendido por todos los Auditores de Informática y complementado con técnicas y herramientas propias de la función. Estás técnicas y herramientas pueden ser tanto las buenas prácticas como los estándares internacionales.

Lo anterior se podría facilitar si los auditores de Informática cuentan con una metodología que oriente cada proyecto a una ejecución armoniosa y planeada en cada una de las tareas y actividades involucradas. Las metodologías de ai requieren herramientas que apoyen y/o justifiquen los resultados obtenidos y las buenas prácticas son una herramienta de apoyo.

Una buena metodología proporciona un alto nivel de confiabilidad, debe responder a cuestionamientos como el qué hacer, dónde se deben hacer las actividades, cómo plantearlas, por qué aprobarlas, cuándo revisar, cuándo empezar, quién debe hacer las actividades de la auditoría, por qué se deben hacer esas actividades, cómo aprobarlas, quiénes deben comprometerse, cuándo terminar, cómo justificar el resultado de la auditoría, entre otras, además de las respuestas que emergen a una situación que es necesario modi^{oo}ficar o mejorar (Aguinis & Bradley, 2014). Existen muchos autores que proponen metodologías para AI, algunos simplemente nombran sus fases. Se consideró una buena metodología de auditoría informática aquella que indica detalles (el qué se tiene que realizar) de cada fase.

Teresa Cabré Castellví (2009) sostiene que las buenas prácticas cumplen con las siguientes características:

- Presentan resultados valiosos para el usuario.
- Son sencillas y simples.
- Emergen como respuesta a una situación en la que es necesario modificar o mejorar.
- Son pertinentes y adecuadas al contexto local en donde se implementa.
- Son sostenible en el tiempo (puede mantenerse y producir efectos duraderos).
- Fomentan la replicación de la experiencia en una situación distinta, pero con condiciones similares.
- Son innovadoras (entendiendo que no solo implica una nueva acción, sino que puede ser un modo diferente y creativo de realizar prácticas tradicionales o de reorganizarlas).
- Consideran elementos de evaluación de resultados, retroalimentación de las acciones y reorganización de ellas a partir de lo aprendido.
- Su difusión recoge y valora el trabajo, los saberes y las acciones que realizan las personas en su trabajo cotidiano, permitiendo generar conocimiento válido empíricamente, transferible y útil.

Si bien una buena práctica es aquella que le da éxito a una empresa, como se mencionó en el párrafo anterior, Cerón (2015) menciona los siguientes parámetros de acción en el desarrollo de proyectos para que una metodología brinde el éxito en una empresa tal y como lo hace una buena práctica:

- Plan general detallado
- Tareas y acciones
- Tiempos
- Aseguramiento de calidad
- Involucrados
- Etapas (fases o módulos)
- Revisiones de avance
- Recursos requeridos

Las metodologías de auditoría en informática deberían ser realizadas por profesionales con experiencia y formación para tal actividad, capaces de dictar recomendaciones técnicas, operativas y jurídicas.

No existen metodologías para la Auditoría Informática estandarizadas, son propuestas de diversos autores, y si bien, las existentes no tienen el mismo número de fases o etapas a seguir ya que cada una tiene su método o forma de hacer el proceso.

Si se complementan las características de una metodología y las de la buena práctica y/o estándares se tendrá como resultado un plan general detallado, con tareas y acciones con

tiempos adecuados y sostenibles para que cada tarea y/o acción se lleve a cabo de la manera correcta, se tendrá un resultado pertinente y adecuado al contexto local en donde se implantará (INTOSAI, 2002).

Metodología

Este análisis se realizó mediante una revisión de la literatura existente, tanto de metodologías de auditoría en informática (Derrien, 1994; Delgado Rojas, 1998, Echenique García, 2001; Juliá, 2010; Muñoz Razo, 2002; Piattini & del Peso, 2001; Hernández Hernández, 1993; Rivas, 1989; Ponce Rodríguez & Naranjo Sánchez, 2006; Aguirre Bautista, 2005) como de las buenas prácticas y estándares (Delgado Picazo, 2009; COSO II, 2013; Galaz & Ruíz, 2015; Gantiva Vergara, 2014; Landivar, 2012; Boehmer, 2009; Martínez, 2016; Aguirre Sánchez, 2017), la gran mayoría menciona ITIL, COBIT y COSO como buenas prácticas e ISO/IEC 20000, ISO 27002 y BS 25999 como estándares. Posteriormente, se revisaron y detectaron las metodologías más completas considerando que todo el proceso fuera explicado de forma explícita (pasos o fases bien diferenciadas), se detectaron las características de buenas prácticas que apoyarán a realizar las actividades de las metodologías, con esta información se realizó un cuadro comparativo mediante un cruce de actividades de apoyo a metodologías y características de buenas prácticas y estándares; y verificando cuál o cuáles de estas cumplían o tenían más puntos de coincidencia. Con esto se determinó qué buenas prácticas son las que apoyan más en las metodologías. Finalmente, se presentan las conclusiones.

Relación entre Metodología y Buenas prácticas

Las metodologías de AI, concebidas tiempo atrás, son marcos generales de trabajo en evaluaciones de recursos informáticos (RI), que no alineaban a los RI con los negocios, basados en la experiencia de los auditores, las buenas prácticas y estándares son herramientas que se pueden considerar en algunas fases de las metodologías que pueden ayudar a reducir la subjetividad de la evaluación, y sobre todo el alinear al negocio los RI, señalando puntos específicos que deben ser considerados en algunas.

Según Sánchez (2014), vicepresidente del IT Service Management Forum, dentro del marco de la Expo Tecnología 2014, las mejores prácticas dentro de una auditoría en informática son una forma de hacer las cosas o una serie de principios generalmente aceptados en un ámbito profesional; ya que éste servirá para aportar un valor al negocio, en el caso de las TI, a través del mejor manejo de información.

Las buenas prácticas son una serie de pasos para hacer las cosas, son aceptadas por medio del ámbito profesional y ayudarán a darle más valor al negocio, empresa, organización, etc. (Altonivel.com, 2010; Aguirre Sánchez, 2017; Ponce, et al., 2010; IMMPC, 2017). Algu-

nas de las mejores prácticas enfocadas en la auditoría informática son las siguientes (Aguirre, 2017; Delgado Picazo, 2009; OSO II, 2013; Galaz & Ruiz, 2015; Gantiva Vergara, 2014; Landivar, 2012; Martínez, 2016):

A. COBIT (*Control Objectives for Information and related Technology*): es el marco aceptado internacionalmente como una buena práctica para el control de la información, TI y los riesgos que conllevan, se utiliza para implementar el gobierno de TI (estructura de relaciones y procesos destinados a dirigir y controlar la empresa, con la finalidad de alcanzar sus objetivos y añadir valor mientras se equilibran los riesgos y el retorno sobre TI y sus procesos) y mejorar los controles de TI. El objetivo principal de COBIT es brindar buenas prácticas a través de un marco de trabajo de dominios y procesos, y presentar las actividades de una manera manejable y lógica. Estas prácticas están enfocadas más al control que a la ejecución. Contiene objetivos de control, directivas de aseguramiento, medidas de desempeño y resultados, factores críticos de éxito y modelos de madurez (Moreno Jiménez, 2003; Peña Ibarra, 2012; Osores, 2014, Prandini & Szuster, 2010; Ríos Vargas, 2004; Rodríguez Parada, 2013; Cárdenas, 2008; ISACA, 2017).

COBIT considera el desarrollo de las guías de gerencia que incluyen factores críticos de éxito, indicadores, clave de desempeño y medidas comparativas. Los factores críticos de éxito identificarán los aspectos o acciones más importantes para la administración y poder tomar, así, dichas acciones o considerar los aspectos para lograr control sobre sus procesos de TI (ISACA, 2017).

Los Indicadores Clave de Desempeño (KPI, por sus siglas en inglés) proporcionarán medidas de éxito que permitirán a la gerencia conocer si un proceso de TI está alcanzando los requerimientos de negocio. Las medidas comparativas definirán niveles de madurez que pueden ser utilizadas por la gerencia para: determinar el nivel actual de madurez de la empresa, como una función de sus riesgos y objetivos, y proporcionar una base de comparación de sus prácticas de control de TI contra empresas similares o normas de la industria. Esta adición, proporcionará herramientas a la gerencia para evaluar el ambiente de TI de su organización con respecto a los 34 Objetivos de Control de alto nivel de COBIT (ISACA, 2017). La primera versión de COBIT apareció en 1992, en la actualidad se utiliza la versión 5 (2012).
Las principales características de COBIT 5 son (ISACA, 2017):

- Orientado al negocio,
- Alineado con estándares y regulaciones "de facto",
- Basado en una revisión crítica y analítica de las tareas y actividades en ti, y
- Alineado con estándares de control y auditoría (COSO- *Sponsoring Organizations of*

the Treadway Commission -, IFAC-*International Federation of Accountants*-, IIA-*The Institute of Internal Auditors*-, ISACA- *Information Systems Audit and Control Association* -, AICPA- *Association of Certified Public Accountants* -).

B. COSO (*Sponsoring Organizations of the Treadway Commission*): tiene por objetivo evaluar el control interno, la gestión del riesgo empresarial, el fraude y los reportes financieros (COSO II, 2013; Galaz Ruíz, 2015; PWC Gobal, 2014). Además, busca proporcionar liderazgo intelectual a través del desarrollo de marcos generales y orientaciones sobre la Gestión del Riesgo, Control Interno y Disuasión del Fraude, diseñado para mejorar el desempeño organizacional y reducir el alcance del fraude en las organizaciones.

El Marco de COSO II (2013) mantiene la definición de control interno sus cinco componentes (ambiente de control, evaluación de riesgos, actividades de control, información y comunicación y supervisión y seguimiento), también incluye mejoras y aclaraciones con el objetivo de facilitar el uso y su aplicación en las entidades (COSO II, 2013; Galaz & Ruiz, 2015).

Por otro lado, propone desarrollar el marco original, empleando "principios" y "puntos de interés" con el objetivo de ampliar y actualizar los conceptos de control interno previamente planteado sin dejar de reconocer los cambios en el entorno empresarial y operativo.

A través de esta actualización, COSO propone desarrollar el marco original mediante:

- Inclusión de diecisiete principios de control, que representan el elemento fundamental, asociados a cada componente del control y que deben de estar operando en forma conjunta.
- Proporciona "puntos de enfoque", o características importantes de los principios, al tiempo que reconoce que el diseño y la implementación de controles relevantes para cada principio y componente requiere de juicio y serán diferentes de acuerdo a la organización.
- Responsabiliza a la administración quien deberá asegurar que cada uno de los componentes y principios relevantes del control interno debe estar presente y en funcionamiento con el fin de contar con un sistema eficaz de control interno.
- Concluyendo que una deficiencia importante en un componente o principio de control no se puede mitigar con eficacia por la función de otros componentes y principios de control.
- COSO verifica la relación entre componentes y principios, control interno.

(coso II, 2013; Galaz & Ruiz, 2015)

C. ITIL (*Information Technology Infrastructure Library*): su objetivo, en todas sus disciplinas, es la definición de las mejores prácticas para los procesos y responsabilidades que hay que establecer para gestionar de forma eficaz los servicios de TI de la organización, y cumplir así los objetivos empresariales en cuanto a la distribución de servicios y la generación de beneficios (Rodríguez Parada, 2013; AXELOS, 2011; AXELOS, 2017).

ITIL describe las mejores prácticas que se pueden utilizar y mejor se adecúan a una organización, incluye cinco disciplinas que proporcionan las empresas flexibilidad y estabilidad para ofrecer servicios de TI: Gestión de incidencias, Gestión de problemas, Gestión de cambios, Gestión de versiones, y Gestión de configuración (Rodríguez Parada, 2013; AXELOS, 2011; AXELOS 2017). Incluye también cinco disciplinas que soportan los servicios TI de calidad y bajo costo de las empresas: Gestión del nivel de servicio, Gestión de la disponibilidad, Gestión de la capacidad, Gestión financiera para servicios TI, y Gestión de la continuidad de los servicios TI.

Por tanto, ITIL se utiliza como línea directriz en la implantación de una gestión de servicios en un entorno informático.

A continuación, se dan a conocer algunos de los estándares que apoyan a la implementación de las mejores prácticas dentro de la auditoría informática, para contar con una certificación que verifique la seguridad de la organización, así como de sus procesos.

A. ISO/IEC 20000 (anteriormente BS 15000): la ISO, a través de las normas recogidas en la familia ISO/IEC 20000, establece una implementación efectiva y un planteamiento estructurado para desarrollar servicios de tecnología de la información confiables en lo referente a servicios de TI. Esta familia de normas impulsa el uso de un enfoque integral de gestión de procesos para brindar servicios que satisfagan las necesidades de los clientes y requerimientos del negocio (ISO, 2017; Rodríguez Parada, 2013; UNIT-ISO/IEC 20000,2016).

Es el primer estándar internacional certificable para la gestión de servicios TI o que necesitan de una gestión para su provisión donde existe un número elevado de infraestructuras y/o configuraciones a gestionar de un modo controlado para beneficio de la prestación de los servicios. Proviene del estándar británico BS 15000 que ha quedado derogado tras la publicación del estándar ISO/IEC 20000 a nivel internacional (ISO, 2017; Rodríguez Parada, 2013).

La serie de normas ISO/IEC 20000 define un conjunto completo y relacionado de procesos de la gestión de los servicios, y se compone de dos partes (ISO, 2017):

ISO/IEC 20000-1: especificaciones en las cuales se describe la adopción de un proceso de mejora integrado para el desempeño y gestión de los servicios acorde a los requisitos del negocio y del cliente.

El documento ISO/IEC 20000-1 ha sido revisado y publicado en una nueva edición en 2011 y comprende 9 secciones: "Alcance", "Términos y definiciones", "Requisitos de un sistema de gestión", "Planificación e implantación de la gestión de servicio", "Planificación e implantación de servicios nuevos o modificados", "Proceso de entrega de servicios", "Procesos de relación", "Procesos de resolución", "Procesos de control" y "Procesos de liberación".

ISO/IEC 20000-2: código de prácticas donde se describen las mejores prácticas para la gestión de los servicios y dentro del ámbito indicado por la norma ISO 20000-1.

El código de práctica es de uso particular para empresas que serán auditadas según la norma ISO/IEC 20000-1, o que están planificando mejoras en sus servicios. Si bien esto puede causar un poco de confusión sobre qué es entonces ISO/IEC 20000, una norma o una buena práctica, Zayas (2008) afirma que "La parte 2 del ISO/IEC 20000 proporciona una guía para auditores y proveedores de servicio".

La guía de bolsillo del estándar ISO/IEC 20000 (2009), sostiene que: "la parte 2 de esta norma describe las mejores prácticas más detalladamente, y provee de guía y recomendaciones para los procesos de gestión dentro del alcance de la norma oficial". De acuerdo con los puntos de vista anteriores las ISO son consideradas normas o estándares, sin embargo, dentro de este se encuentra una guía para el uso de este estándar.

Estas normas pueden ser usadas por organizaciones que buscan servicios y que necesitan garantías de que los requerimientos de los servicios serán cumplidos. Entre estas organizaciones se pueden encontrar: una que requiere un enfoque coherente para todos sus prestadores de servicios; un prestador de servicios que tiene la intención de demostrar su capacidad para el diseño, transición, provisión y mejora de los servicios; o un prestador de servicios, para hacer seguimiento de sus servicios y de sus procesos de gestión de servicios.

Dentro de la familia de normas ISO/IEC 20000 la de mayor trascendencia sea la ISO/IEC 20000-1 establecida en México como UNIT-ISO/IEC 20000-1-, Requisitos del Sistema de Gestión del Servicio (SGS), la cual establece los requisitos que se deben cumplir en el diseño, la implementación y el mantenimiento de la gestión de servicios de TI, esta norma puede utilizarse para la certificación. Le sigue la norma ISO/IEC 20000-2 establecida en México como UNIT-ISO/IEC 20000-2-, describe buenas prácticas que deberían ser adoptadas por las organizaciones en relación con los procesos de gestión del servicio de TI, que permite cubrir las necesidades de negocio del cliente, con los recursos acordados, así como asumir un riesgo entendido y aceptable.

La norma ISO/IEC 20000-3 proporciona orientación sobre la definición del alcance, aplicabilidad y la demostración de la conformidad con los proveedores de servicios orientados a satisfacer los requisitos de la norma ISO/IEC 20000-1. UNIT, como representante exclusivo de ISO en Uruguay es el responsable de la Normalización Técnica en esta materia y también quién está promocionando en nuestro país la Capacitación en Gestión del Servicios de TI y la Certificación de los correspondientes

Sistemas (UNIT-ISO/IEC 20000, 2016).

B. ISO 27002 (anteriormente denominada ISO 17799): la reciente publicación de la revisión de las normas ISO/IEC 27001:2013; ISO/IEC 27002:2013 (ISO, 2017) ambas aprobadas en la misma fecha: 25 de septiembre de 2013. Es una guía de buenas prácticas que describe los objetivos de control y controles recomendables en cuanto a seguridad de la información. Contiene 39 objetivos de control y 133 controles, agrupados en 11 dominios (ISO, 2017).

El Estándar Internacional ISO/IEC 27002 va orientado a la seguridad de la información en las empresas u organizaciones, de modo que las probabilidades de ser afectados por robo, daño o pérdida de información se minimicen al máximo.

ISO/IEC 27002 proporciona recomendaciones de las mejores prácticas en la gestión de la seguridad de la información a todos los interesados y responsables en iniciar, implantar o mantener sistemas de gestión de la seguridad de la información (ISO, 2017).

La versión de 2013 del estándar describe catorce dominios principales (UNIT-ISO/IEC 20000, 2016): políticas de seguridad, organización de la seguridad de la Información, seguridad de los recursos humanos, gestión de los activos, control de accesos, cifrado, seguridad física y ambiental, seguridad de las operaciones, seguridad de las comunicaciones, adquisición de sistemas, desarrollo y mantenimiento, suministradores, incidentes, continuidad del negocio y cumplimiento.

Dentro de cada sección, se especifican los objetivos de los distintos controles para la seguridad de la información. Para cada uno de los controles se indica asimismo una guía para su implantación. El número total de controles suma 114 entre todas las secciones, aunque cada organización debe considerar previamente cuántos serán realmente los aplicables según sus propias necesidades (ISO, 2017).

C. BS 25999: el plan de continuidad del negocio fue visto en sus inicios como parte del sector de las TI, desarrollado por organizaciones tales como el Business Continuity Institute (BCI) y *Survive* a lo largo de 1980 y 1990 como algunas de las mejores prácticas. El creciente conocimiento internacional sobre este tema se dio en Japón, Australia, Singapur y Austria, todos por delante del Reino Unido en la elaboración de guías o normas nacionales en este ámbito. El British Standards Institute *(*BSI) publicó en 2006 la norma BS 25999-1, un código de buenas prácticas dedicado a la gestión de la continuidad de negocio. Para las empresas resulta cada vez más importante disponer de planes de continuidad de negocio para que, en caso de un desastre o cualquier otro tipo de interrupción, la inactividad de la organización sea reducida, y por el contrario aprovechar estos momentos para que la empresa tome mayor posicionamiento. El Instituto de Continuidad de Negocio (Business Continuity Institute*,* en adelante BCI) fue establecido en 1994 con el objetivo de apoyar a sus socios y

para orientar los profesionales de la continuidad de negocio. A través de su plan de certificación, el instituto proporciona a sus miembros un estatus internacionalmente reconocido puesto que la afiliación profesional del BCI demuestra la capacidad de sus miembros a llevar a cabo una gestión de continuidad de negocio a un nivel muy elevado. De manera más amplia, su papel consiste en promocionar las normas más elevadas en materia de competencias profesionales y ética de las prestaciones |y del mantenimiento de servicios y planificación de la continuidad de negocios (Burtles, 2016).

"El BS-25999 es un estándar británico que establece mejores prácticas, recomendaciones y actividades específicas para lograr la continuidad de negocio teniendo en cuenta los riesgos a los que se enfrenta una organización" (Arango López, 2010; Rodríguez Lache & Correa Cano, 2008; Cuate, 2011; Boehmer, 2009). Este estándar se basa en el Plan de Continuidad del Negocio – o Business Continuity Planning (por sus siglas en inglés BCM) el cual, al ser implementado en una organización, se le debe hacer un seguimiento con el fin de conocer su evolución permanente en los procesos de la empresa.

La norma ha sido publicada en dos partes (Arango, 2010; Rodríguez Lache & Correa Cano, 2008; Cuate, 2011; Boehmer, 2009; (Burtles, 2016):

- BS 25999-1 Gestión de la continuidad del negocio. Código de práctica: Publicada en noviembre de 2006, como una guía de implantación del modelo de gestión.
- BS 25999-2 Gestión de la continuidad del negocio. Especificación: Publicada en diciembre 2007 como una especificación de requisitos para un sistema de gestión de continuidad de negocio y, por lo tanto, con la posibilidad de certificación de aquellas organizaciones que cumplan los requisitos de esta norma.

La metodología contiene etapas, que definen a los involucrados, las revisiones conforme al tiempo y al avance y los recursos requeridos; una buena práctica se complementa considerando elementos de evaluación de resultados, retroalimentación de las acciones y reorganización de ellas a partir de lo aprendido, también ayuda a valorar las acciones que realizan las personas en su trabajo cotidiano permitiendo generar conocimiento válido empíricamente, transferible y útil.

Para llevar a cabo el análisis se tomó en cuenta las siguientes metodologías, que no siendo comerciales llevan el nombre de su autor; de cada una de ellas se exponen, de manera general, sus fases y requerimientos:

A. Metodología de Rivas (1989): 1) Toma de contacto: se recaba la información relativa a la empresa a auditar, en puntos tales como: organización, organigrama, planes, situación

del mercado, estructura del departamento, recursos, etc.; 2) planeación de la operación: fijar las áreas que cubrirá, colaboradores, plan de trabajo, tareas, calendario, resultados parciales, presupuesto, equipo auditor necesario, entre otros; 3) desarrollo de la auditoría: se efectuarán las entrevistas, se complementan cuestionarios, se realiza observación de situaciones difíciles y procedimientos, etc.; 4) diagnóstico: analizar e interpretar todos los datos obtenidos y ser capaces de concluir con un diagnóstico de la situación real encontrada. Todo esto basado en experiencia del auditor y los modelos establecidos para realizar el contraste de datos observaciones u obtenidos; 5) presentación de conclusiones: suficientemente argumentadas, probadas y documentadas para no ser refutadas; y 6) formación del plan de mejoras: reconsideración de los sistemas o de los medios, humanos y materiales con que se cuenta, llegando, si es preciso, a reconsideraciones en el plan informático (Rivas, 1989).

B. Metodología Ponce Rodríguez y Naranjo Sánchez (2006): 1) Planificación de la auditoría: comprender el ambiente del negocio en el que se ha de realizar la auditoría y el ambiente normativo en el que opera el negocio; 2) programa de auditoría: planeación previa, donde se identifican los recursos y destrezas que se necesitan para realizar el trabajo, así como las fuentes de información para pruebas o revisión y lugares físicos o instalaciones donde se va auditar; 3) recopilación de evidencia: relevamiento de los procesos del negocio e informáticos, el plan informático y los informes emitidos de las actividades realizadas; 4) evaluación del control interno: evaluación de debilidades y fortalezas, también se deben determinar las observaciones o hallazgos de la auditoría; 5) evaluación de la gestión informática: definición de indicadores; y 6) el informe de auditoría: producto final de este proyecto. Indica las observaciones y recomendaciones a la gerencia, también se expone la opinión sobre lo adecuado o inadecuado de los controles revisados durante la auditoría, además, contiene la opinión sobre los indicadores aplicados para la evaluación de la gestión informática.

C. Metodología de Hernández Hernández (1993): 1) etapa preliminar: diagnóstico de la situación actual, diagnóstico de Negocio; 2) la opinión de la Alta Dirección para estimar el grado de satisfacción y confianza que se tiene hacia los productos, servicios y recursos de informática en el negocio, así mismo es posible detectar en esta etapa las fortalezas, aciertos y apoyo que brinda dicha función desde la perspectiva de los directivos del negocio, áreas de oportunidad que tiene la Informática para hacer más competitivo y rentable al negocio, sea este soporte directo o indirecto, en alto o menor grado, actividades del Auditor de Informática, conocimiento del negocio, apoyo al negocio, conocimiento de la función de Informática, entrevistas, cuestionarios, documentación, servicios, aspectos de Control; 2) etapa de Justificación: revisión o evaluación de las áreas o funciones críticas relacionadas con Informática. Los productos terminados más importantes de la

etapa son tres: matriz de riesgos, plan de auditoría de informática y Vo. Bo. por escrito. El primero porque define las áreas que serán auditadas y el segundo porque establece las tareas, tiempos, responsables, etc. del Proyecto, el tercero debido a que le da el visto bueno al líder de proyecto para continuar con las siguientes etapas contempladas en el Plan General; 3) etapa de adecuación: análisis, adecuación y actualización de todos los elementos que se involucran en un proyecto de Auditoría de Informática pero a un nivel detallado; 4) etapa de formalización: corresponde a la Alta Dirección, dar su aprobación y apoyo formal para el desarrollo del Proyecto de Auditoría de Informática presentado por el Líder de Proyecto y del Responsable de la Función de Auditoría de Informática. Verificación de Prioridades, Restricciones y Alcances del Proyecto; 5) presentación formal del plan de Auditoría de Informática, aprobación formal del Proyecto de Auditoría de Informática, etapa de desarrollo: se empiezan a ejecutar las tareas de su trabajo de acuerdo con el Plan aprobado en la Etapa de Formalización.

D. Metodología Aguirre Bautista (2005): 1) investigación preliminar: consiste básicamente en encuentros con un prospecto de cliente, con el objeto de conocer las necesidades y características del trabajo que se va a realizar, y de la institución auditada, es decir, se va a realizar un estudio general del escenario planteado por el cliente; 2) planeación de la auditoría en informática: consiste en la elaboración de los programas de trabajo que se llevarán a cabo durante la revisión a la entidad auditada y puede constar de varias etapas, sin embargo, las más relevantes desde un punto de vista objetivo son: diagnóstico informático, elaboración del programa de la auditoría en informática (actividades que han de realizarse, fechas de inicio y término, así como los tiempos), documentación para la auditoría en informática (evidencia suficiente y competente que soporta la opinión del auditor), análisis, clasificación y evaluación de la información (podrán realizarse por métodos estadísticos, se pone a prueba el talento del auditor, porque se requiere para entender e interpretar la información y continuar con el siguiente paso), documentación del software de aplicación, del hardware y de la biblioteca (solicitudes del trabajo, autorizaciones, minuta de reuniones, establecimiento de prioridades, licitaciones, estudios de factibilidad y formas de respaldo y resguardo debidamente documentadas por módulo o por sección), software de aplicación (manuales se solicitan a los desarrolladores de sistema o al líder del proyecto del ciclo de vida del desarrollo de un sistema o al responsable de sistemas); 3) análisis, evaluación y presentación de la auditoría: separar lo importante de lo urgente, con el objeto de reconocer qué información es útil y principal y cuál es de soporte y secundaria; y 4) dictamen de la auditoría en informática: estructura: Principio (lugar y fecha de emisión, destinatario, antecedentes, alcance de la auditoría, limitaciones al trabajo, personal asignado), Cuerpo (hallazgos y observaciones, secciones o apartados

especiales, resumen evaluativo de correcciones operadas durante la auditoría) y Final (opinión y conclusiones del auditor, comentarios y puntos de vista de los auditores, sugerencias y recomendaciones, párrafo de cierre; mencionar las facilidades, atenciones brindadas al auditor y firma).

Teniendo en consideración las metodologías anteriores y las características que deben tener las expuestas por Cerón (2015), se identifican los siguientes elementos:

Característica 1. Plan general detallado
Característica 2. Tareas y acciones
Característica 3. Tiempos
Característica 4. Aseguramiento de calidad
Característica 5. Involucrados
Característica 6. Etapas (fases o módulos)
Característica 7. Revisiones de avance
Característica 8. Recursos requeridos

La Tabla 1 se diseña a partir de lo anterior, la primera columna muestra cada una de las fases de las diferentes metodologías consideradas y en el primer renglón las características que debe tener una buena metodología, en el cruce entre ambas se coloca una marca de la metodología que cumple con una característica positiva y se indica en las columnas 4 y 6 qué buenas prácticas pueden apoyar en cada fase.

Dependiendo del número de características con las que cumpla en total la metodología se tomará la decisión de cuál es la mejor opción para emplearla junto con una buena práctica. Después de esta tarea se detectan las buenas prácticas que apoyan a la fase de la metodología y se hacen observaciones acerca del por qué se relacionan. Lo mismo se aplicó para los estándares que apoyan tanto a la fase de la metodología como de la buena práctica y las observaciones.

Tabla 1.

Análisis de metodologías, buenas prácticas y estándares.

Metodología	Fases	Características que cumple según Cerón (2015)		Buena práctica que apoya en la fase de la metodología	Observaciones	Estándares que apoyan a la fase	Observaciones
Metodología de Rivas (2014)	F.1. Toma de contacto	Carac. 1 Carac. 2 Carac. 3	✓	COBIT	En esta metofología se toma como buena práctica de apoyo COSO y COBIT debido a que COBIT sirve para planear, organizar, dirigir y controlar toda la función informática dentro de una empresa. Actúa sobre la dirigencia yayuda a estandarizar la organización. COSO está enfocado a toda la organización, contempla políticas, procedimientos y estructuras organizacionales además de procesos para definir el modelo de control interno.	ISO/IEC 20000 ISO/IEC 27002	El estándar ISO/IEC 20000 y el ISO/IEC 27002, cada una de las fases de esta metodología toma en cuenta el proceso de mejora para el desempeño de los servicios y la seguridad. Los estándares que la apoyan se basan en seguridad y que se mejore la gestión de servicios acorde a las necesidades del negocio y del cliente.
	F.2. Planificación de la operación	Carac. 2 Carac. 3	✓	COBIT COSO		ISO/IEC 20000 ISO/IEC 27002	
	F.3. Dsarrollo de la Auditoría	Carac. 2 Carac. 3 Carac. 4 Carac. 5 Carac. 7	✓	COBIT COSO		ISO/IEC 20000 ISO/IEC 27002	
	F.4. Diagnóstico	Carac. 1 Carac. 4 Carac. 6 Carac. 7	✓	COBIT COSO		ISO/IEC 20000 ISO/IEC 27002	
	F.5. Presentación de Conclusiones	Carac. 1 Carac. 2 Carac. 4 Carac. 7 Carac. 8	✓	COBIT COSO		ISO/IEC 20000 ISO/IEC 27002	
	F.6. Formulación de plan de mejoras.	Carac. 1 Carac. 4 Carac. 5 Carac. 8	✓	COBIT COSO		ISO/IEC 20000 ISO/IEC 27002	
Metodología de Ponce Rodríguez & Naranjo Sánchez (2006)	F.1. Planificación de la Auditoría	Carac. 2 Carac. 4	✓	COSO	En esta metodología se toma como apoyo: COBIT, ambas buscan el mejor control interno.	BS25999	Los estándares que apoyan tanto a las metodologías como a las buenas prácticas se muestran en la columna anterior, esta metodología busca la continuidad del negocio, enalgunas de sus fases hace referencia a los controles de seguridad de la información.
	F.2. Programa de Auditoría	Carac. 1 Carac. 8	✓	COBIT		ISO/IEC 27002	
	F.3. Recopilación de evidencia	Carac. 2 Carac. 7	✓	COBIT COSO		NINGUNO	
	F.4.Evaluación de Control Interno	Carac. 2 Carac. 4	✓	COBIT COSO		NINGUNO	
	F.5. Evaluación de Gestión Informática	Carac. 1	✓	COBIT		NINGUNO	
	F.6. Informe de Auditoría	Carac. 1 Carac. 2 Carac. 3	✓	COBIT		ISO/IEC 27002	

Metodología	Fases	Características que cumple según Cerón (2015)		Buena práctica que apoya en la fase de la metodología	Observaciones	Estándares que apoyan a la fase	Observaciones
Metodología de Hernández Hernández (1993)	F.1. Preliminar	Carac. 1 Carac. 2 Carac. 3 Carac. 4	✓	ITIL COBIT	Las buenas prácticas que apoyan esta metodología son: ITIL, COBIT y COSO. Esta metodología es muy completa y cada una de sus fases puede complementarse con los aspectos considerados encada buena práctica.	BS25999	En esta metodología pueden utilizarse todos los estándares descritos, cada fase se centra en un aspecto específico: gestión, seguridad y control interno.
	F.2.Diagnóstico de Informática	Carac. 1 Carac. 4	✓	ITIL COBIT		ISO/IEC 27002	
	F.3. Justificación	Carac. 1 Carac. 2 Carac. 4 Carac. 7 Carac. 8	✓	COSO		ISO/IEC 20000	
	F.4. Adecuación	Carac. 1 Carac. 2 Carac. 4 Carac. 7 Carac. 8	✓	ITIL		ISO/IEC 20000	
	F.5. Formalización	Carac. 1 Carac. 2 Carac. 4 Carac. 7 Carac. 8	✓	ITIL COBIT		ISO/IEC 20000	
	F.6.Desarrollo	Carac. 1 Carac. 2 Carac. 4 Carac. 7 Carac. 8	✓	ITIL		ISO/IEC 20000	
Metodología de Aguirre Bautista (2005)	F.1. Investigación preliminar	Carac. 2	✓	COBIT ITIL	Las buenas prácticas que apoyan esta metodología son: ITIL, COBIT y COSO. Para planear, organizar, dirigir y controlar toda la función informátca dentro de una empresa las buans parácticas apoyanen la dirección y a la estandarización. Ásí mismo, ITIL apoya enlos procesos, se mejora el servicio con una mejora continua.	ISO/IEC 20000 BS25999	Esta metodología contien un plan de continuidad del negocio, gestión de servicio de TI y controles de seguridad, por lo que tanto ISO cmo BS apoyan en sus activiadades.
	F.2. Planeación de la Auditoría Informática	Carac. 1 Carac. 2 Carac. 3 Carac. 5 Carac. 6	✓	ITIL COBIT COSO		ISO/IEC 20000 BS25999	
	F.3. Documentación para la Auditoría Informática	Carac. 1 Carac. 2 Carac. 3 Carac. 5 Carac. 8	✓	COBIT		ISO/IEC 27002	
	F.4. Análisis, clasificación y evaluación de la información	Carac. 1 Carac. 7	✓	COBIT COSO		ISO/IEC 20000 BS25999	
	F.5. Dictamen de la Auditoría Informática	Carac. 7	✓	COBIT ITIL		ISO/IEC 20000 ISO/IEC 27002 BS25999	

Fuente: elaboración propia.

Se puede observar que, entre todas las metodologías propuestas, las fases cumplen con al menos una característica común de una buena metodología: deben brindar a los interesados los parámetros de acción que propuso Cerón (2015) para el buen desarrollo de sus proyectos.

La metodología de Rivas (1989) se puede reforzar con las buenas prácticas de COBIT Y COSO, ya que ambas se complementan. COBIT sirve para planear, organizar, dirigir y controlar toda la función informática dentro de una empresa además de que ayuda a estandarizar la organización. Y, por otro lado, COSO está enfocado a toda la organización, contempla políticas, procedimientos y estructuras organizativas, además de procesos para definir el modelo de control interno.

Ahora bien, la metodología que proponen Ponce Rodríguez y Naranjo Sánchez (2006), se puede hacer un buen complemento con las buenas prácticas de COBIT, COSO e ITIL, esta última solo se utiliza en la última fase de la metodología, se observa también que no cumple con algunas características propuestas por Cerón (2015).

En la metodología de Hernández Hernández (1993) se observa que se puede aplicar en sus fases las buenas prácticas de COSO, COBIT e ITIL, además de que cumple con la mayoría de las características que expone Cerón (2015).

Por último, la metodología de Aguirre Bautista (2005) cumple en su mayoría con las características de Cerón (2015), puesto que logra hacer un complemento con las tres buenas prácticas (ITIL, COBIT y COSO), desde que se empezó el análisis de esta metodología se pudo notar que era la más completa, con respecto a las características y definiciones de metodología.

Cada tarea o acción definida en la fase debe hacerse de la mejor manera posible, en otras palabras se tendrán que hacer de calidad para que se lleve a cabo de manera exitosa la metodología, este aspecto puede complementarse con el uso de buenas prácticas.

Caso: Auditoría Informática utilizando COBIT 5.0 en un Departamento de Tecnologías de Información y Comunicaciones (DTIC).

Para ejemplificar la combinación de metodologías de Auditorías Informática y el uso de buenas prácticas se presenta de manera general la Auditoría de un DTIC utilizando la Metodología de Jesús Aguirre y el Uso de COBIT 5.0 en el área de Proceso para la Gestión de TI con la *actividad* de monitorear, evaluar y valorar (Tabla 2):

Tabla 2.

Relación en un ejemplo de la metodología de Auditoría Informática y cobit 5.0.

Fase de la Metodología	Actividades	Uso de cobit	Actividades de la Metodología en la que utilizó cobit	Producto Obtenido
F.1. Investigación preliminar	Estudio general del escenario Determinar necesidades Determinar alcance Determinar equipo de trabajo	Identificación Proceso Flujograma del Proceso Matriz RACI	Estudio general del escenario Determinar necesidades	Reporte de las condiciones del escenario, flujograma del proceso y matriz RACI, alcance de la auditoría y necesidades del área auditada.
F.2. Planeación de la Auditoría Informática	Diagnóstico informático Elaboración de programa de trabajo, donde se especifican actividades, fechas de inicio y termino.	Selección Escenarios de evaluación	Elaboración de programa de trabajo, donde se especifican actividades, fechas de inicio y termino.	Programa de trabajo considerando dos escenarios de evaluación.
F.3. Documentación para la Auditoría Informática	Solicitar la Información requerida para la auditoría informática: Documentación del software de aplicación, del hardware y de la biblioteca Solicitudes del trabajo, autorizaciones, minuta de reuniones, establecimiento de prioridades, licitaciones, estudios de factibilidad y formas de respaldo y resguardo debidamente documentadas por módulo o por sección	Información Escenario Cumplimiento Legal Revisión de Cumplimiento según escenarios	Solicitar la Información requerida para cada uno de los escenarios, así como requerimientos legales para proporcionar servicios y documentación existente.	Toda la información física y digital
F.4. Análisis, clasificación y evaluación de la información	Uso de métodos estadísticos para entender e interpretar la información	Controles críticos asociados al proceso evaluado para mitigar riesgos Matriz de riesgos y efectos de mitigación	Comparación y análisis de controles críticos utilizando análisis estadístico para interpretar la información	Uso de paquetería de ofimática y paquetes estadístico pzrz generar los repostes que permitan realizar la interpretación de los datos que se obtuvieron de la recopilación de información. Generación de repostes de resultados.
F.5. Dictamen de la Auditoría Informática	Redacción del informe y sugerencia de los aspectos no satisfactorios encontrados	Recomendaciones	Dentro del informe de auditoría se encuentra un apartado de recomendaciones.	Reportes y análisis de los mismo, veredicto de la auditoría por medio de un informe y recomendaciones en los puntos medulares con problemática encontrada.

Fuente: Elaboración propia.

Como se puede observar en el cuadro, el uso de buenas prácticas son apoyo y complemento en las fases de las metodologías informáticas.

Conclusiones

El auditor tiene la responsabilidad moral de darle un sentido crítico y práctico para orientar los esfuerzos de todas las áreas del negocio para encontrar un mejor modo de hacer las cosas desde el punto de vista profesional en el campo de Informática, y de ser posible en las áreas del negocio involucradas.

Con base en las características de las metodologías de los autores mencionados y las que debe cumplir una metodología, así como las buenas prácticas y estándares que se relacionan se puede decir que las metodologías pueden fortalecerse con el uso de buenas prácticas. Algunas como la de Aguirre Bautista (2005) y la de Hernández Hernández (1993) pueden ser más completas y se robustecen con mejores prácticas, como COBIT.

El uso de diferentes metodologías puede tener ventajas y desventajas, lo que hace necesaria la búsqueda de un ámbito adecuado para evitar al máximo las pérdidas por las debilidades o amenazas que presenta la organización; y es aquí donde las buenas prácticas cobran importancia, ya que contribuyen apoyando con un aspecto objetivo (uso de indicadores, por ejemplo) a las auditorías.

El desarrollo exitoso de la Auditoría de Informática depende de un conjunto de factores interrelacionados entre sí. Las mejores prácticas son los factores que se pueden utilizar para que sea exitosa dicha acción, el análisis de las buenas prácticas sirvió para poder relacionar una mejor práctica dentro del proceso de una auditoria informática.

Sánchez (2014) vicepresidente del IT Service Management Forum, mencionó dentro del marco de la Expo Tecnología 2014, que las mejores prácticas en la auditoría informática eran una forma de hacer las cosas o bien una serie de principios aceptados profesionalmente.

Tanto las mejores prácticas como las metodologías ayudan a complementar y mejorar la auditoria informática, una mejor práctica lleva un método de cómo hacer las cosas y una metodología contiene fases y tareas que ayudan a que todo se realice en tiempo y forma para un mejor resultado.

Se puede acoplar una buena práctica a una metodología para mayor beneficio, como se mencionó en el análisis, cada metodología tiene fases, tareas, tiempos, herramientas y un orden de cómo hacer cada actividad que sea necesaria para llevar a cabo la auditoria informática, y una mejor práctica indica cómo hacer las cosas, la mejor manera de realizar las actividades.

El Responsable de la Función de Auditoría de Informática puede valerse de la información consolidada, contenida en la Tabla 1 de descripción general de la Metodología de Auditoría de Informática, para darle un seguimiento oportuno y estructurado a cada uno de los proyectos.

Las organizaciones exitosas son aquellas que, entre otras cosas, reconocen los beneficios que las TIC les proporcionan para cumplir sus objetivos. Además, comprenden la necesidad de administrar los riesgos del empleo de las TIC, la información es uno de sus activos más importantes (Sánchez, 2014).

La función de la Auditoría Informática en dichas organizaciones comienza con la implantación de un proceso para supervisar el control de las tecnologías y de los procesos asociados, y evoluciona hacia un enfoque proactivo participando en todas las fases del ciclo de gestión del control.

Las metodologías informáticas son guías para realizar las evaluaciones y tienen como resultado un diagnóstico y sugerencias de los auditores para lograr mejoras, su éxito depende en parte, de la experiencia del auditor. Las buenas prácticas pueden apoyar a dar objetividad a las evaluaciones y las sugerencias finales de los informes de auditoría.

Finalmente, una metodología y una mejor práctica y/o un estándar se complementan para llegar a un fin en común: alinear las TIC al negocio con éxito. Las buenas prácticas y los estándares pueden complementar diferentes fases en las metodologías de auditorías informáticas.

Referencias

1. Altonivel.com. (2010). Adoptando buenas prácticas empresariales. Recuperado de http://www.altonivel.com.mx/adopta-buenas-practicas-empresariales
2. Aguirre Bautista J. J. (2005). *Auditoría en Informática. 13/12/2017*, UNAM. Recuperado de http://fcasua.contad.unam.mx/apuntes/interiores/docs/2005/informatica/6/1664.pdf
3. Aguinis, H., & Bradley, K. J. (2014). Best practice recommendations for designing and implementing experimental vignette methodology studies. *Organizational Research Methods*, 17(4), 351-371.
4. Aguirre Sánchez Y. (2017). *Propuesta de implantación del área de auditoría en informática en un órgano legislativo*. 13/12/2017. Recuperado de http://olea.org/~yuri/propuesta-implantacion-auditoria-informatica-organo-legislativo/ch03s02.html.
5. AXELOS Global Best Practices. (2017). ITIL. 13/12/2017, de AXELOS Global Best Practices Recuperado de https://www.axelos.com/best-practice-solutions/itil?utm_source=itil.co.uk&utm_medium=redirect&utm_campaign=redirects
6. AXELOS. (2011). The ITIL® Continual Service Improvement Book. En *The ITIL® Continual Service Improvement Book* (246). UK: ITIL Training Academy.
7. Burtles, J. (2016). *Principles and Practice of Business Continuity: Tools and Techniques*. Rothstein Publishing.
8. Cabré Castellví, M. T. (2009). *Terminología y buenas prácticas*. Publifarum. Recuperado de http://www.publifarum.farum.it/ezine_articles.php?art_id=161.

9. Cárdenas, E. (2008). *Tendencias del Control Interno Informático: COBIT.* Recuperado de http://galeon.com/iclass/Cobi.doc.
10. Cerón, M. T. (2015). *Tecnologías de la Información Y [Información de Blog]*. Recuperado de https://scholar.google.es/citations?hl=es&user=nbzNHOMAAAAJ.
11. COSO II: Internal Control Integrated Framework. (2013). México: COSO. Recuperado de http://www.coso.org/documents/Internal%20Control-Integrated%20Framework.pdf.
12. Cuate, M. U. (2011). Sistema de Gestión de Continuidad del Negocio de Acuerdo con BS25999 e ISO 22301. *Latin América CACS, México.*
13. Derrien, Y. (1994). *Técnicas de la Auditoría Informática*. España: Editorial Marcombo.
14. Delgado Rojas, X. (1998). *Auditoría Informática*. Costa Rica: Editorial Universidad Estatal a Distancia.
15. Delgado Picazo, M. (2009). *Analisis de Impacto y Desarrollo de Buenas Prácticas de Auditoria en Bases de Datos.* (Tesis). Universidad Carlos III de Madrid.
16. Echenique García, J. A. (2001). *Auditoría en Informática*. México: Editorial Interamericana/ Mc-Graw-Hill.
17. Galaz, Y. & Ruiz U. (2015). *Doloitte. COSO: Marco de referencia para la implementación, gestión y control de un adecuado Sistema de Control Interno.* Recuperado de http://www2.deloitte.com/content/dam/Deloitte/mx/Documents/risk/COSO-Sesion1.pdf.
18. Gantiva Vergara, J. G. (2014). *Conocimiento de normas, estándares, buenas prácticas y Mejores Prácticas en el ejercicio de la ingeniería relacionada con las TIC en Colombia*. Recuperado de http://www.acofipapers.org/index.php/ei/2014/paper/viewFile/665/246.
19. Hernández Hernández, E. (1993). *Auditoría de Informática: Un Enfoque Metodológico* (Master). Universidad Autónoma de Nuevo León.
20. IMMPC (2017). ¿Qué son las *mejores prácticas corporativas?* México: Instituto Mexicano de Mejores Prácticas Coorporativas (IMMPC) Recuperado de http://www.immpc.org.mx/mejores-practicas-corporativas
21. INTOSAI Professional Standards Committee (2002). *Principios para las Mejores Prácticas de Auditoría de las Instituciones Internacionales*. Viena. Recuperado de http://www.efsur.org/sites/default/files/files/issai_5000_s.pdf.
22. ISACA (2017). *What is COBIT 5?* Recuperado de http://www.isaca.org/cobit/pages/default.aspx
23. ISO (2017). *ISO/IEC 27002:2013*. International Standar Organization (ISO) Recuperado de https://www.iso.org/standard/54533.html
24. Juliá, S. (2010). *¿Para qué sirve una auditoría informática en la empresa?* Recuperado de http://www.gadae.com/blog/para-que-sirve-una-auditoria-informatica-en-la-empresa/.
25. Landivar, F. (2012). *Estándares y Buenas Prácticas sobre Seguridad Informática ISO/IEC 27002*. Recuperado de http://pdf.usaid.gov/pdf_docs/PA00JRCT.pdf.

26. Martínez, V. (2016). *Buenas Prácticas de Auditoría y Control Interno en las Organizaciones*. Recuperado de http://blogs.portafolio.co/buenas-practicas-de-auditoria-y-control-interno-en-las-organizaciones/.
27. Moreno Jiménez, L. C. (2003). *La Auditoría en la Informática* (Maestría). Facultad de Ingeniería Mecánica y Eléctrica. Colima.
28. Muñoz Razo, C. (2002). *Auditoría en Sistemas Computacionales*. México: Editorial Pearson Educación.
29. Osores, M. (2014). *Mejores prácticas de TI: Más valor para el negocio*. Recuperado de http://searchdatacenter.techtarget.com/es/cronica/Mejores-practicas-de-TI-Mas-valor-para-el-negocio.
30. Peña Ibarra, J. A. (2012). COBIT 5. Trabajo presentado en Evento Técnico de ISACA: Monterrey Chapter, Monterrey. Recuperado de http://www.isaca.org/chapters7/Monterrey/Events/Documents/20120305%20CobiT%205.pdf.
31. Piattini, M., & del Peso, E. (2001). *Auditoría Informática Un enfoque Práctico*. Mexico: Editorial Alfaomega.
32. Ponce Rodriguez, N. I., & Naranjo Sánchez, B. A. (2006). *Auditoria a la Gestión Informática con una Visión de Negocios Integral en una Empresa Comercial* (Doctorado). Instituto de Ciencias Matemáticas, Escuela Superior Politécnica del Litoral.
33. Ponce, R., Estanga, O., Garcia, M., Jaimes, S. y Pimentel, N. (2010). *Mejores Prácticas para el manejo de Tecnología de Información en las organizaciones*. Recuperado de http://es.slideshare.net/rosmelys/mejores-practicas-para-el-manejo-de-tecnologa-de-informacin-en-la-organizaciones.
34. Prandini, P. & Szuster, R. (2012). Re-Evolución COBIT 5. Trabajo presentado en el XIX Congreso y Feria Interamericana de Seguridad de la Información, Buenos Aires. Recuperado de www.isaca.org/Knowledge-Center/cobit/.../COBIT5-and-InfoSec-Spanish.ppt.
35. PWC Global. (2014). *2014, año de transición al nuevo COSO 2013*. PWC Global. Recuperado de https://www.pwc.com/mx/es/publicaciones/archivo/2014-02-punto-vista.pdf
36. Ríos Vargas, F. (2004). *COBIT, mejores prácticas para el manejo de información*. Costa Rica: Universidad Latinoamericana de Ciencia y Tecnología. Recuperado de http://bb9.ulacit.ac.cr/tesinas/publicaciones/037190.pdf.
37. Rivas, G. A. (1989). *Auditoría informática*. España: Editorial Díaz de Santos.
38. Rodríguez Lache E. Y. & Correa Cano D. (2008). *BS 25999*. UVM. Recuperado de http://es.calameo.com/read/0014410056e31dc57b8fa
39. Rodríguez Parada, T. C. (2013). *Estándares Internacionales TIC Estándares: ITIL COBIT ISO*. Recuperado de https://issuu.com/iname/docs/proyecto_2.
40. Sánchez, O. (2014), *The IT Service Management Forum*. ITSMF International. Recuperado de http://www.itsmfi.org/.

41. UNIT-ISO/IEC 20000 (2016). *Gestión de los Servicios de TI*. Instituto Uruguayo de Normas Técnicas. Recuperado de http://www.unit.org.uy/normalizacion/sistema/20000/
42. Zayas, A. (2008). ISO/IEC 20000 Tecnologías de Información y la Alineación con la Gestión. Trabajo presentado en XII Foro Mundial de la Calidad y de la Gestión para la mejora, Acapulco. Recuperado de http://www.inlac.org/documentos/ISO_20000_Tecnologia_de_la_Informacion_y_la_Alineacion_con_la_Gestion.pdf
43. IMMPC. (2017). *¿Qué son las mejores prácticas corporativas?* Instituto Mexicano de Mejores Prácticas Corporativas (IMMPC). Recuperado de http://www.immpc.org.mx/mejores-practicas-corporativas.