

Sistemas basados en conocimiento como herramienta de ayuda en la auditoría de sistemas de información

(Knowledge based systems as an aid in information systems audit)

Rodrigo Arturo Proaño Escalante¹, Ciro Napoleón Saguay Chafra²,
Segundo Bolívar Jácome Canchig³, Fanny Sandoval Zambrano⁴

Resumen:

Uno de los problemas que tiene el auditor informático al emitir una opinión sobre un hallazgo es la subjetividad que puede deberse a muchos aspectos, entre los principales: emocionales, capacidades o habilidades técnicas con lo cual esta opinión puede ser acertada o errada. Este es un problema importante debido a que el informe de auditoría emitido puede tener distorsiones de la realidad de los hechos. Por otro lado, el desarrollo de los sistemas expertos implica capturar el conocimiento del humano y trasladarlo a un programa de computador en el cual se emulen todas las características de este conocimiento y considerando un grupo de reglas, el sistema pueda tomar decisiones como lo haría un humano. Los avances de la inteligencia artificial en los últimos años, ofrecen que el desarrollo de estos sistemas basados en conocimiento sea cada vez mayor y los resultados obtenidos sean más reales. El uso de estos sistemas presenta un futuro bastante prometedor en el campo de la auditoría informática. El objetivo de este artículo es dar una idea general de la caracterización y uso de los sistemas basados en conocimiento, la forma como están implementados y su aplicación a la auditoría de sistemas de información como herramienta de ayuda a la emisión de opinión al momento de realizar una auditoría.

Palabras clave: auditoría de sistemas; sistemas basados en conocimiento; sistemas expertos.

Abstract:

One of the problems that the IT auditor has when expressing an opinion about a finding is the subjectivity that can be due to many aspects, among the main ones: emotional, technical skills or abilities with which this opinion can be right or wrong. This is a major problem because the audit report issued may have distortions of the facts. On the other hand, the development of the expert systems involves capturing the knowledge of the human and transferring it to a computer program in which all the characteristics of this knowledge are emulated and considering a group of rules, the system can make decisions as a human does. Advances in artificial intelligence over the last few years have led to the development of these knowledge-based systems increasing and the results obtained are more real. The use of these systems presents a promising future in the field of computer audit. The objective of this article is to give a general idea of the characterization and use of knowledge based systems, the way they are implemented and their application to the audit of information systems as a tool to help the opinion issue at the moment of realization of an audit.

Keywords: audit systems; knowledge based systems; expert systems.

¹ Universidad Tecnológica Equinoccial, Quito – Ecuador (rodrigo.proano@ute.edu.ec)

² Universidad Tecnológica Equinoccial, Quito – Ecuador (csaguay@ute.edu.ec)

³ Universidad Tecnológica Equinoccial, Quito – Ecuador (sbolivar.jacome@ute.edu.ec)

⁴ Universidad Tecnológica Equinoccial, Quito – Ecuador (fanny.sandoval@ute.edu.ec)

1. Introducción

En la actualidad, se vive en una sociedad donde cada vez se hace más evidente el uso de las tecnologías de información en todo ámbito. Los sistemas tecnológicos según Moeller (2010) se han vuelto cada vez más complejos y por ende requieren de profesionales expertos que tengan un amplio conocimiento de una gran variedad de tecnologías de información.

En las empresas el uso de sistemas de información computarizados se ha vuelto una práctica común, y por ende los riesgos en los mismos se han multiplicado volviéndose necesaria la auditoría de estos sistemas tecnológicos, proceso que es efectuado por auditores especializados. Pero no solo es el conocimiento lo que debe caracterizar al auditor; otros aspectos a tomar en cuenta según Granados (2016) son:

- Astucia para identificar aspectos claves para encontrar inconsistencias en los procesos que se están auditando.
- Creatividad para el cumplimiento de sus actividades.
- Inteligencia para una adecuada toma de decisiones.
- Honestidad para el desarrollo de sus actividades.
- Confidencialidad en el manejo de la información a la que tiene acceso.
- Organización para un trabajo sistemático y metódico.

Por otro lado, el concepto de auditoría según Piattini (2001) es emitir de una opinión de tipo profesional de un objeto en análisis que muestre correctamente la realidad que pretende reflejar. La auditoría informática a opinión de Echenique (2001) trata sobre la salvaguarda de los activos de los sistemas de computadoras, considerando algo importante como la integridad de los datos para de esta manera alcanzar los objetivos organizacionales de forma eficiente. Bajo este contexto, al hablar de activos de computadoras, se considera hardware, software, datos, entre otros, con lo cual el horizonte de cobertura de la auditoría informática se amplía sustancialmente. Por tanto al conjugar estos elementos y pretender dar una opinión razonable sobre su realidad, se puede caer en contradicciones o ambigüedades según el punto de vista del auditor.

La Inteligencia Artificial (IA) tiene aplicación en muchos aspectos del vivir diario, por ejemplo cuando se le da una orden verbal a algún dispositivo para realizar alguna acción, un sistema inteligente interpreta la orden, la reconoce y la ejecuta. Así se puede ver la utilidad y aplicabilidad de la IA a través de técnicas especiales como son los sistemas basados en conocimiento y sistemas expertos, en los cuales se incorpora el conocimiento de los auditores informáticos experimentados que, sumado a los hechos y evidencias encontradas para un problema en particular dan una respuesta acorde y objetiva a la realidad del objeto auditado.

En este escenario, el propósito es eliminar la subjetividad al momento de analizar los hechos y que la opinión se ajuste adecuadamente a la realidad presente. Es en este sentido que según Agarwal (2014) se recurre a la inteligencia artificial para hacer máquinas o computadoras que puedan pensar y se comporten como un humano, en especial el uso de los Sistemas Basados en Conocimiento (SBC).

En este artículo se hace una descripción del funcionamiento de los sistemas basados en conocimiento, las metodologías usadas para su desarrollo y la aplicación de los mismos en la auditoría informática.

2. Materiales y Métodos

2.1. Sistemas basados en conocimiento

Los SBC según Palma y Marín (2008) presentan entre otras las siguientes propiedades fundamentales:

- Aplicables a problemas complejos que requieren excesivos recursos computacionales o temporales.
- Pueden ser utilizados por usuarios no expertos.
- Recrean el razonamiento humano.
- Representan el conocimiento humano, el cual si bien es difícil de caracterizarlo, una vez almacenado y procesado adecuadamente se constituye en algo invaluable.

2.2. Elementos del SBC

Según García (2013), una técnica de IA es el razonamiento basado en conocimiento, que conlleva a los SBC, que a diferencia de cualquier programa convencional en el cual para una misma entrada se produce siempre la misma salida en función del algoritmo utilizado, este tipo de sistemas hace uso de una base de conocimientos, la cual contiene información almacenada sobre un problema en particular, normalmente proporcionada por un experto (en este caso el auditor informático) y un motor de inferencia que es el encargado de razonar sobre soluciones posibles para el problema planteado a través de búsquedas de información en la base de conocimientos, con lo cual se lograría emitir una conclusión razonable comparable al pensamiento de un humano. En las siguientes secciones se explican los principales elementos que componen un SBC.

2.2.1. Base de conocimiento

La base de conocimiento contiene el conocimiento sobre un determinado problema en el cual el sistema es experto, esta base almacena una representación de los conceptos y relaciones de las

tareas. Este conocimiento según Montoya (2014) se representa normalmente usando lógica de predicados o lógica proposicional, los elementos que constituyen el conocimiento se clasifican en hechos, heurísticas y reglas.

2.2.1.1. Hechos

Un hecho es una expresión que normalmente tiene asociado un valor verdadero y que se le puede ver como una expresión de la forma *Si - condición entonces* –enunciado. Por Ejemplo:

- *Si no existen respaldos entonces hay riesgo de pérdida de información.*

2.2.1.2. Heurística

La heurística, es la forma de llegar a una solución por métodos no rigurosos en este caso, la heurística resulta de la experiencia obtenida del auditor al momento de tomar una decisión y las reglas o relaciones que vinculan los hechos. En la práctica no existe una única heurística, en circunstancias similares ante evidencias similares de un hallazgo la decisión puede ser diferente por algún elemento que permita direccionar esta decisión, esto hace la diferencia con un programa computacional tradicional en el cual a entradas iguales o similares produce siempre las mismas salidas.

2.2.1.3. Reglas

Las reglas desde el punto de vista de la lógica de predicados hacen referencia a la reglas de inferencia lógica, según Palma (2008) son *modus ponens* y *generalización universal*.

2.2.2. Motor de inferencia

El motor de inferencia según Palma (2008) explora la base de conocimiento con el propósito de obtener una salida. En este motor se implementa el método de resolución del problema que utilizando los hechos, las reglas y las heurísticas, decide las acciones a tomar para llegar a una solución.

2.2.3. Interfaz

Evidentemente para que el SBC pueda interactuar con el usuario, es necesario dotarlo de la respectiva interfaz de entrada/salida.

Un elemento adicional que no siempre está presente en un SBC es una interfaz de aprendizaje o entrenamiento por medio de la cual se puede alimentar en forma directa la base de conocimiento con instrucciones propias de los usuarios, normalmente expertos o de retroalimentación de las salidas del sistema.

Este tipo de SBC se utiliza para la resolución de problemas donde por la complejidad de los mismos, no es posible utilizar las técnicas convencionales de programación debido a que el esfuerzo y el consumo de recursos son representativos en tiempo, memoria y procesamiento.

La *Figura 1* muestra los componentes básicos de un SBC.

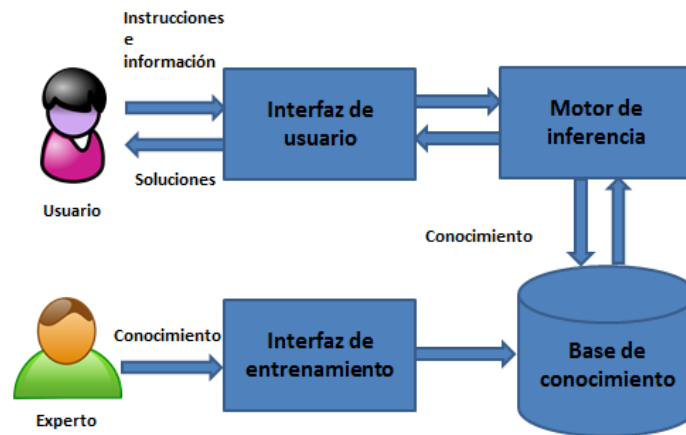


Figura 1. Esquema general de los elementos que forman el SBC.

2.3. Metodologías para el desarrollo de sistemas basados en conocimiento

El problema de desarrollar SBC ha sido tratado con el uso de distintos métodos, según Palma (2008), se puede mencionar algunos de ellos:

DENDRAL que fue utilizado a finales de los años sesenta por Buchanan y otros y que para la interpretación de espectrogramas de masas usaba el conocimiento heurístico de los expertos, puede ser considerado el primer sistema inteligente y su aporte ha sido muy importante al desarrollo de estos modelos. Este sistema ha sido usado por biólogos y químicos por más de 10 años para evaluar aspectos reales.

MYCIN desarrollado en 1984 por Buchanan y Shottliffe empleado para diagnóstico médico. Es considerado el primer sistema experto desarrollado como ayuda para la investigación y diagnóstico de enfermedades infecciosas de la sangre.

XCON/R1 propuesto por McDermott, Barker y O'Conner en 1989. Es un sistema de producción basado en reglas usado por la empresa DEC como herramienta de ayuda para la selección de los componentes de los sistemas de computación solicitados por los clientes.

KADS por Wielinga y otros en 1992. Que considera el desarrollo de los SBC como una actividad de modelado con comportamientos que pueden observarse de fenómenos del mundo real.

El aporte de todos estos modelos ha sido significativo en el desarrollo de los SBC en la medida en que han establecido los lineamientos básicos para la formulación y construcción de este tipo de

sistemas, los cuales como se puede evidenciar tienen aplicación en todos los ámbitos organizacionales.

En los últimos años surgen algunos modelos basados en metodologías de desarrollo en espiral las cuales proponen el desarrollo del sistema en ciclos que contiene las siguientes etapas:

1. Definición de objetivos.
2. Valoración de riesgos.
3. Desarrollo del SBC.
4. Planificación para un nuevo ciclo de depuración.

Bajo estos puntos de vista, surgen algunas metodologías utilizadas recientemente como lo explica Palma (2008):

KSM (Knowledge Structure Manager), metodología resultado del grupo de investigación ISYS (Intelligent Systems) del Departamento de Inteligencia Artificial de la Universidad Politécnica de Madrid que según Henao (2001) se enfoca en identificar los modelos de entendimiento que pueden ser computables en el problema a solucionarse. Tiene como característica el uso de modelos genéricos que pueden ser reutilizados sin mucha dificultad.

CommonKADS, que según Chávez (2015), es una mejora de la tecnología KADS (Knowledge Acquisition and Design Structuring), la cual según Henao (2001) ha sido desarrollada en las universidades de Amsterdam, Países Bajos y Bruselas como parte del proyecto europeo SPRIT. en el Departamento de Inteligencia Artificial de la Universidad Politécnica de Madrid.

Esta metodología según Giraldo (2015) es diseñada para el análisis y construcción de SBC. Considera 3 niveles para el desarrollo de un SBC, los cuales permiten manejar el conocimiento y la información de un sistema en el entorno organizacional. Cada nivel a su vez incorpora modelos los cuales utilizan ciertos formularios para capturar en forma detallada las actividades, procesos, información y el conocimiento de la organización. El detalle de cada nivel con sus modelos según Giraldo (2015) es el siguiente:

1. Nivel de Contexto: nivel en el cual se analiza la organización, tiene tres modelos:
 - 1.1. Modelo de organización (OM), permite analizar la organización, a través de esta herramienta se puede identificar problemas y oportunidades de mejora con el uso del SBC que se pretende introducir.
 - 1.2. Modelo de tareas (TM), describe en forma general las tareas que son realizadas o las nuevas tareas que van a realizarse dentro de la organización en la cual va a instalarse el SBC, es un mecanismo para distribuir las tareas entre los distintos agentes.

- 1.3. Modelo de agentes (AM), los agentes son entidades ejecutoras de una tarea y pueden ser personas, software o cualquier otro elemento. Este modelo describe características, competencias y restricciones de los agentes.
2. Nivel de Concepto: nivel en el cual se comprende la organización. Los dos modelos a este nivel son:
 - 2.1. Modelo de conocimiento o modelo de experiencia (EM), es la parte esencial de esta metodología y modela el conocimiento para la resolución de problemas que usa el agente para ejecutar una tarea. Al hablar de conocimiento, es necesario distinguir los dos tipos de conocimiento que existen en una organización: *Conocimiento explícito*, el cual se conoce, se puede compartir y se lo puede documentar y transmitir como por ejemplo una fórmula, un manual de especificaciones e incluso un programa informático. Y *conocimiento tácito o implícito*, el cual está ahí en forma desarticulada y es difícil de explicarlo, ejemplo la habilidad o experiencia de una persona.
 - 2.2. Modelo de comunicación (CM), describe el intercambio de información y conocimiento entre los distintos agentes ejecutores de tareas en el TM.
3. Nivel de Implementación: nivel en el cual se modela la organización, el modelo en este nivel es el siguiente:
 - 3.1. Modelo de diseño (DM), los modelos anteriores OM, TM, AM, EM y CM tratan del análisis del SBC a diferencia del DM el cual describe la arquitectura y el diseño técnico del SBC.

Estos modelos en los distintos niveles actúan en forma sinérgica con el propósito de conseguir la integración final del SBC.

La *Figura 2* muestra la interacción entre los distintos modelos.

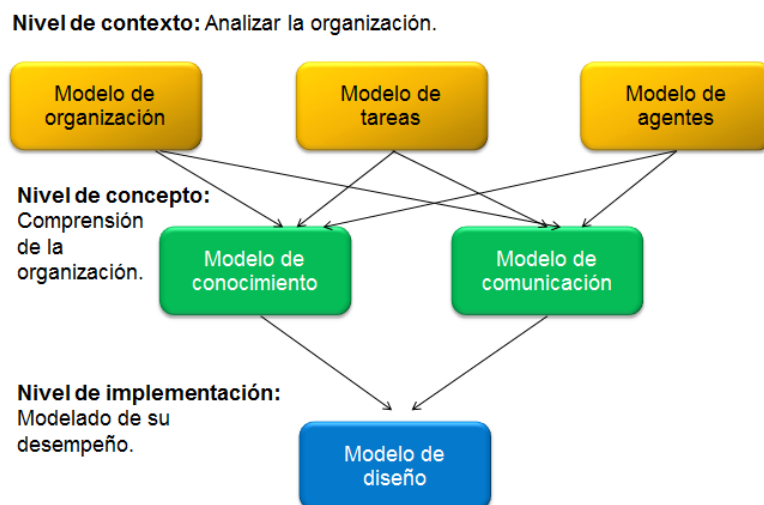


Figura 2. Niveles considerados por el modelo CommonKADS para desarrollo de un SBC. Chávez (2015).

3. Resultados y discusión

3.1. Sistemas expertos usados en auditorías de seguridad de la información.

Los sistemas expertos son un tipo de SBC que intentan actuar o comportarse en todo aspecto como un humano. Son diseñados para resolver problemas muy complejos sin utilizar procedimientos comunes como es el caso de la programación convencional, utilizan razonamiento sobre el conocimiento de la misma manera que un experto humano.

El núcleo de un sistema experto según Atymtayeva (2012) es la base de conocimientos, la cual debe ser cuidadosamente diseñada y construida para que refleje el dominio del problema a analizar, considerando conceptos claves e identificando relaciones entre estos. En el área de seguridades de información, es muy difícil identificar claramente el proceso y el camino adecuado para formular un esquema de sistema experto para auditoría de estas seguridades; para facilitar el proceso, se puede acudir a las ontologías que no son otra cosa que una herramienta de comunicación entre los humanos y los sistemas de toma de decisión.

A continuación se lista la secuencia de pasos para el desarrollo de esta ontología:

1. Desarrollo del glosario de términos.
2. Definición de relaciones jerárquicas, y equivalencias para estructurar el diccionario basado en conceptos.
3. Identificación de axiomas.

Para el desarrollo de la base de conocimiento se pueden usar algunas fuentes de conocimiento, entre las cuales según Atymtayeva (2012) se mencionan:

- Modelo del sistema derivado del proceso de modelado de la base de conocimiento.
- Documentación y procesamiento de seguridades de información que pueden provenir de estándares de seguridad como ISO 27002:2005.
- El conocimiento de expertos en el área, en este caso de seguridades de la información.

La ontología anteriormente mencionada se transforma en un modelo de conocimiento considerando aspectos como activos, amenazas, vulnerabilidades y controles.

La *Figura 3* describe el modelo de conocimiento y sus relaciones en el ámbito de la auditoría informática.



Figura 3. Niveles del modelo CommonKADS para desarrollo de un SBC. Adaptado de Atymtayeva (2012)

Sin importar la metodología de evaluación de seguridades de información que se utilice, los conceptos manejados aquí según la ISO/IEC (2015) son:

- Riesgo: Es la “combinación de la probabilidad de un evento y sus consecuencias.”
- Activo: cualquier cosa de valor de la organización.
- Amenaza: Es la “causa potencial de un incidente no deseado que puede resultar perjudicial para un sistema o la organización.”
- Vulnerabilidad: Es una “debilidad física, técnica o administrativa que puede ser explotada por una amenaza.”
- Control: es un elemento usado para mitigar las vulnerabilidades implementando medidas físicas u organizacionales.

Estos conceptos, en el modelo se transforman en relaciones de la siguiente manera:

- Las vulnerabilidades son explotadas por las amenazas, en este caso, es necesario introducir un factor de ponderación o coeficiente de severidad de forma tal que el sistema experto puede interpretar la severidad de la amenaza.
- La vulnerabilidad es mitigada por los controles.
- Los controles son implementados para los activos de información con el propósito de disminuir el riesgo (riesgo residual).
- Los activos presentan vulnerabilidades.

3.2. Evaluación de riesgos.

Según Elky (2014), identificar y evaluar los riesgos puede ser una tarea compleja, normalmente el riesgo se calcula como una función de la probabilidad de la amenaza que se ejerce sobre la vulnerabilidad.

En la actualidad, los riesgos sobre la seguridad de la información pueden afectar sobremanera aspectos como integridad, confiabilidad y disponibilidad de la misma.

Para hacer la evaluación de riesgos, se debe considerar algunos aspectos:

- Obtener información de los activos de la organización: la cual sirve para alimentar la base de conocimiento.
- Identificar amenazas: para cada activo de información, se debe identificar las amenazas a las que está expuesto, por ejemplo un activo puede ser robado.
- Identificar vulnerabilidades: para poder calcular la probabilidad de las amenazas, es necesario buscar las vulnerabilidades asociadas con cada amenaza.
- Identificar controles: después de identificar las vulnerabilidades, el sistema encuentra los controles asociados, propuestos normalmente por estándares de seguridad.
- Evaluar la efectividad de los controles, y se ingresa nuevamente en el ciclo debido a que el sistema se basa en la aplicación de controles sobre los activos.
- Calcular el riesgo residual. El cual queda luego de aplicar los controles.

Todos los elementos aquí mencionados se han aplicado en distintos sistemas de uso comercial, según Bonilla (2014) entre los cuales se pueden mencionar los que se muestran en la *Tabla 1*.

Tabla 1. Aplicación de sistemas expertos en la auditoría, contabilidad y análisis financiero.

Nombre del sistema	Referencias	Área de Gestión	Funcionalidad
AUDITPLANNER	Steinbart et al. 1987	Auditoría	Ayuda a los auditores a determinar los juicios de materialidad de las cifras en la etapa de planificación de la auditoría.
RISK ADVISOR	Graham et al. 1991	Riesgo de la auditoría	Valorar los riesgos en auditoría y evaluar el rendimiento económico de un cliente.
BUCKS (Business Control Knowledge System)	Brown y Phillips 1990	Contabilidad de Costos y de Gestión	Ayuda a los directores a analizar el rendimiento de los proyectos de la división y las actividades de asesoría de las regiones.
FSA (Financial Statement Analyzer)	Mui y McCarthy 1987 O'Leary 1987 Murria y Murria 1988 Van Dijk y Williams 1990 Keyes 1991	Contabilidad Financiera	Realiza la revisión analítica de los registros de los estados financieros de una compañía.
ANIBAL	Eritel 1991 Núñez 1991 Fortuna et al. 1991	Análisis contable y financiero	Le facilita a los analistas financieros la evaluación de la gestión comercial y financiera de la empresa.

4. Conclusiones y Recomendaciones

El uso de sistemas basados en conocimientos resulta de gran ayuda en la auditoría de sistemas de información; aprovechando el conocimiento de un experto en auditoría, se pueden desarrollar sistemas expertos que apliquen este conocimiento a través de herramientas informáticas que permitan tomar o guiar decisiones en un proceso de auditoría de sistemas.

El uso de este tipo de herramientas no es todavía aprovechado en todo su potencial, hay algunos trabajos al respecto, sin embargo a futuro se puede aplicar en distintos tipos de auditorías, especialmente de sistemas.

A pesar de que se pueden usar sistemas expertos como ayuda para la auditoría, la opinión del auditor aún juega un papel preponderante.

No está muy lejos el pensar en auditorías de sistemas de información inteligentes en las que el uso de herramientas de inteligencia artificial sobrepasen y complementen la opinión humana del auditor.

Independientemente de la metodología utilizada, el desarrollo de un sistema experto es de mucha utilidad a la hora de realizar la auditoría informática.

A través de estas técnicas, se propone fomentar la investigación y el aporte de la Inteligencia Artificial en los procesos de auditoría informática.

Como trabajos futuros se plantea el estudio de estos sistemas focalizados a casos prácticos en donde se pueda medir la eficiencia de los mismos.

Bibliografía

- Agarwal, M. & Goel, S. (2014) *Expert System and it's Requirement Engineering Process*. International Conference on Recent Advances and Innovations in Engineering (ICRAIE-2014), Jaipur, 2014, pp. 1-4. Recuperado Marzo 23, 2015 de <http://ieeexplore.ieee.org>
- Atymtayeva, L., Bortsova, G., Inoue A., Kozhakhmet, K. (2012). *Methodology and ontology of expert system for information security audit*. SCIS-ISIS 2012, Kobe, Japan, November 20-24, 2012, pp. 1-6. Recuperado Marzo 18, 2015 de <http://ieeexplore.ieee.org>
- Bonilla, L. (2014). *Inteligencia Artificial aplicada en la Prevención y Detección de Lavado de activos y Financiamiento del Terrorismo*, pp 10-17. Recuperado Abril 16, 2015 de www.felaban.net/archivos_noticias/archivo20141107151058PM.

- Chávez, A. (2015). *metodologa-commonkads*. Recuperado Enero 15, 2016 de http://es.slideshare.net/uni_fcys_sistemas/metodologa-commonkads
- Echenique, J. (2001). *Auditoría en Informática*, pp. 2-20. México: McGraw-Hill.
- Elky, S. *Risk management*. Recuperado Enero 21, 2016 de <http://www.sans.org> -1204
- García, A. (2013) *Inteligencia Artificial. Fundamentos, práctica y aplicaciones*, pp 171-175. México: AlfaOmega.
- Giraldo, I. y Montoya, D. (2015). *Aplicación de la metodología de Commonkads en la gestión del conocimiento*. Revista CEA, 1(2), 99-108. Recuperado Febrero 6, 2017 de itmojs.itm.edu.co/index.php/revista-cea/article/download/804/761
- Granados, E. (2016). *Auditoría de Sistemas*. Recuperado Marzo 12, 2016 de <http://artemisa.unicauca.edu.co>
- Henao, M. (2001). *CommonKADS-RT: Una Metodología para el Desarrollo de Sistemas Basados en el Conocimiento de Tiempo Real*, Tesis Doctoral, pp. 27-30. Recuperado Febrero 7, 2017 de <http://users.dsic.upv.es/grupos/ia/sma/thesis/pdf/TesisMonicaH.pdf>
- ISO/IEC (2015). *Information technology — Security techniques — Code of practice for information security management*, 2005 Recuperado Agosto 14, 2016 de <https://www.iso.org>
- Moeller, R. (2010). *IT Audit, Control, and Security*, pp 135-140. New York: John Wiley & Sons.
- Montoya, D., Giraldo, J., Perdomo W. (2014). *Caracterización, Arquitectura de los SBC, y el proceso de realización de las auditorías en Colombia*, pp 1-6. Recuperado Agosto 20, 2016 de www.iiis.org/CDs2013/CD2013SCI/CISCI_2013/PapersPdf/CA923DT.pdf
- Palma J., Marín R (2008). *Inteligencia Artificial: Métodos, técnicas y aplicaciones*, pp. 83-97 Madrid: McGraw-Hill.
- Piattini , M., Del Peso E. (2001). *Auditoría Informática, Un enfoque práctico*, pp. 3-8 México: AlfaOmega.