UN MARCO DE REFERENCIA PARA LA AUDITORÍA DE SISTEMAS DE INFORMACIÓN BASADOS EN WEB

Alberto Brandon Báez Camarena

INTRODUCCIÓN

La llegada de las principales técnicas de auditoría permite a los auditores identificar los riesgos y evaluar los controles sobre los sistemas de información críticos en sus organizaciones, tiene profundas consecuencias para muchas áreas de las actividades de las empresas. Aunque tales técnicas de auditoría están todavía en las primeras etapas de desarrollo, el impulso hacia su mejora es tal que se ha cambiado el carácter de la investigación llevada a cabo principalmente por la comunidad de investigación industrial. Una gran proporción del esfuerzo de investigación actual se limita a los investigadores que normalmente están ligados a asociaciones profesionales y organizaciones relacionadas con la auditoría de sistemas de información (Champlain, 1998). Argumentamos que la evaluación de los sistemas de información basados en Web (WBIS) es relevante para la industria y la academia, como consecuencia de ello, el trabajo relacionado con el desarrollo de metodologías y herramientas de auditoría se lleva a cabo ahora por sistemas científicos de la información (Akoka et al, 2000;. Atzeni et al, 2002;. Nicho 2008). El desarrollo teórico necesario para comprender las metodologías de auditoría está dando lugar a grandes avances y se espera que tengan repercusiones en los sistemas de información así como en las herramientas y técnicas de auditoría puesto que las metodologías de auditoría son cada vez más importantes ya que las organizaciones dependen en gran medida de estos sistemas información. La última década ha visto el desarrollo a un ritmo sin precedentes de los sistemas de información basados en Web (WBIS) que ha abierto la oportunidad para que se desarrollen cada vez más WBIS muy sofisticados, tales como portales, juegos en línea, portales de

gestión de información y entretenimiento, buscadores, aplicaciones de comercio electrónico, CRM (Customer Relationship Management) y aplicaciones EAI (Enterprise Application Integration).

SISTEMAS DE INFORMACIÓN BASADOS EN WEB

Durante la última década, el impacto de la web ha transformado el papel de las tecnologías de la información de sistemas apoyo en las organizaciones a sistemas estratégicos de recolección y entrega de datos que permiten la gestión estratégica de las organizaciones apoyándose en los mismos, permitiendo a las empresas por ejemplo, determinar los hábitos de compra de los clientes y darles un mejor servicio. Por lo general, se admite que las tecnologías aplicadas al comercio electrónico han reducido el costo de la recolección de datos de los compradores (Dewan et al. , 2000). Los sistemas de información basados en Web (WBIS) son sistemas de información específicos que toman ventajas de las tecnologías web, están integrados por cinco componentes principales: el sitio web, el sistema de procesamiento de negocios en línea, la gestión del conocimiento, la base de datos, y los agentes de software. Va mucho más allá de las oportunidades y los servicios ofrecidos por los sitios web mediante el apoyo a los procesos de negocio.
Teniendo en cuenta la necesidad de auditar este tipo de sistemas basados en Web, consideramos que se deben tener en cuenta dimensiones específicas en la forma y los medios para llevar a cabo dicho proceso de auditoría.

Auditoría para Sistemas de Información

El objetivo principal del auditor de sistemas de información es formular una opinión objetiva sobre la eficacia y la contribución de los sistemas de información a la empresa (Collier et al. , 1995). Su juicio puede ser influenciado por factores tales como su conocimiento sobre los sistemas de información de la

organización, y el grado de riesgo de cometer errores a través de esta evaluación. El propósito de una auditoría en tecnologías de información es evaluar los controles de TI (Mahnic et al., 2001), un auditor de TI evalúa y asesora sobre los siguientes aspectos de las tecnologías de la información: eficacia, eficiencia, exclusividad, etc (Hermanson, 2006). Se han propuesto un gran número de métodos de evaluación de los sistemas y tecnologías de información, así como de los WBIS, los que reciben una atención especial incluyen el cuadro de mando integral Balanced Score Card (Barrow et al., 2001), el método de desarrollo de sistemas dinámicos (Deschoolmeester et al., 2000), sistemas de simulación (Anderson, 2000), etc. Estos métodos son de carácter multidisciplinario, se basan en las teorías de evaluación tales como la teoría económica (Svavarsson, 2002), el enfoque interpretativo (Abu- Samaha, 2000), el enfoque crítico (Jones et al. , 2002), la teoría de la estructuración (Jansen et al. , 2004), la teoría de suelo (Jones et al., 2001), el enfoque de contingencia (Turk, 2000), la teoría de la opción (Svavarsson, 2002), y la teoría social (Berghout et al., 1996). La variedad de enfoques , tales como COBIT, ITIL, ValIT, etc. (ITGI, 2005) ilustra la falta de consenso (Chang et al, 2005;. Simonsson et al, 2007). Aunque no existe un entendimiento común sobre una teoría de evaluación adecuada hay tres conceptos principales que estructuran el proceso de auditoría (ITGI 2005): Procesos y dominios , criterios de auditoría, y el marco de la auditoría de sistemas de información.

Procesos y Dominios de los Sistemas de Información

Para asegurarse de que los sistemas de información están funcionando de manera eficiente y eficaz para ayudar a la organización a alcanzar sus objetivos estratégicos, se debe realizar un proceso de auditoría, esta tarea implica el análisis de los procesos de los sistemas de información. Las actividades individuales dentro de un sistema de información se pueden agrupar en procesos. El marco COBIT (ITGI 2005) identifica

34 procesos de tecnología de la información. Este último se agrupan en cuatro dominios (figura 1).

MONITOREAR Y EVALUAR
ME1 Monitorear y evaluar el desempeño de TI.
ME2 Monitorear y evaluar el control interno
ME3 Garantizar cumplimiento regulatorio.
ME4 Proporcionar gobierno de TI.
PLANEAR Y ORGANIZAR
PO1 Definir el plan estratégico de TI.
PO2 Definir la arquitectura de la información
PO3 Determinar la dirección tecnológica.
PO4 Definir procesos, organización y relaciones de TI.
PO5 Administrar la inversión en TI.
PO6 Comunicar las aspiraciones y la dirección de la gerencia
PO7 Administrar recursos humanos de TI.
PO8 Administrar calidad.
PO9 Evaluar y administrar riesgos de TI
PO10 Administrar proyectos.
ADQUIRIR E IMPLANTAR
AI1 Identificar soluciones automatizadas.
AI2 Adquirir y mantener el software aplicativo.
AI3 Adquirir y mantener la infraestructura tecnológica
AI4 Facilitar la operación y el uso.
AI5 Adquirir recursos de TI.
AI6 Administrar cambios.
AI7 Instalar y acreditar soluciones y cambios.
ENTREGAR Y DAR SOPORTE
DS1 Definir y administrar niveles de servicio.

DS2 Administrar servicios de terceros.
DS3 Administrar desempeño y capacidad.
DS4 Garantizar la continuidad del servicio.
DS5 Garantizar la seguridad de los sistemas.
DS6 Identificar y asignar costos.
DS7 Educar y entrenar a los usuarios.
DS8 Administrar la mesa de servicio y los incidentes.
DS9 Administrar la configuración.
DS10 Administrar los problemas.
DS11 Administrar los datos.
DS12 Administrar el ambiente físico.
DS13 Administrar las operaciones.

Fig. 1. Dominios y procesos de TI de acuerdo a COBIT 4.0

Los sistemas heredados (o Legacy), así como los sistemas de información basados en la Web incluyen tanto componentes técnicos como de gestión, las tareas de auditoría se pueden llevar a cabo a lo largo de las dimensiones relacionadas con los dominios de los Sistemas de Información (figura 2):

Dimensión de Gestión y Organizacional	**Dimensión Tecnológica**
Sistemas de información de planeación estratégica Sistemas de información funcionales (marketing, recursos humanos, logística, sistemas de información contable, etc.) Sistemas de procesamiento de datos y	Seguridad informática Operaciones de procesamiento de datos Aplicaciones actuales Nuevos proyectos de sistemas de información Costos de sistemas de información Compras y subcontratación

procedimientos de la organización Normas de contabilidad y regulación	Telecomunicaciones y sistemas de redes de cómputo

Fig. 2. Dominios de los sistemas de información.

Cualquier enfoque de auditoría se puede realizar en uno de los 34 procesos de COBIT o uno de los doce dominios descritos anteriormente.

Criterio de Auditoria

Para satisfacer los objetivos del negocio los sistemas de información deben cumplir con ciertos criterios que permitan medidas de control adecuadas. El conjunto de criterios considerados por las diferentes metodologías no son estrictamente equivalentes pero a menudo se superponen. En general, los criterios de auditoría son generalmente segmentada de acuerdo con tres puntos de vista (Nicho , 2008; Olsina et al, 2001):

- Los requisitos de calidad de productos que abarca, por ejemplo, la eficiencia y el rendimiento.
- Los requisitos de seguridad descritos en los criterios de coherencia, seguridad, conformidad y fiabilidad.
- Requisitos de legibilidad que comprende viabilidad, auditabilidad y la capacidad de evolucionar.

Marcos de referencia de Auditoría

Los marcos de auditoría de TI buscan cumplir el concepto de seguridad y permite la alineación de los objetivos de TI con los objetivos empresariales (Grembergen et al, 2005;. Yip et al, 2006) con el fin de satisfacer las necesidades de información del

negocio y los objetivos de las organizaciones. Los conceptos de dominios de sistemas de información y los procesos de TI, así como los criterios de auditoría juegan un papel central en el proceso de auditoría que permite a las empresas reforzar los objetivos de control interno. Se han propuesto varios marcos de control interno (o marcos de auditoría): COSO, COCO, Cadbury, COBIT y eSAC (Brown et al, 2005.). El marco COSO (COSO, 1992) ha sido diseñado para proporcionar seguridad respecto al logro de los objetivos de la información financiera y en el cumplimiento de las leyes y reglamentos. El marco COCO (COCO, 1995) es muy similar a COSO pero presenta conceptos adicionales no incluidos en COSO tales como los controles que permiten a los auditores identificar los riesgos en la capacidad de las organizaciones para explotar oportunidades. El marco de Cadbury (Cadbury, 1994) tiene como objetivo proporcionar una garantía de la disposición y el mantenimiento de registros contables adecuados. A diferencia de los tres marcos descritos anteriormente, el informe eSAC es el primer marco que tiene por objeto proporcionar "una buena orientación sobre el control y la auditoría de los sistemas de información y tecnología" (Stott, 2008).

En el contexto de la era del Internet, los nuevos sistemas de información basados en la web están diseñados, desarrollados e implementados con gran rapidez. Como consecuencia de ello, cada vez es más difícil de realizar auditorías eficaces de sistemas de información basados en la web utilizando metodologías tradicionales de auditoría tales como COBIT.

El proceso de auditoría de sitios web sólo está comenzando a hacer sentir su presencia más allá de la comunidad de investigación industrial, como se puede ver, hay muy pocos trabajos que tratan explícitamente la auditoría de los sitios web más allá de los aspectos de calidad. Se define a continuación un enfoque específico para la auditoría de un WBIS.

El objetivo de esta metodología es contribuir a la base de conocimientos existente en la evaluación de sistemas de información ofreciendo una metodología de auditoría basada en los dominios de los sistemas de información y los criterios combinados para formar un árbol jerárquico ponderado, esto permitirá:

- Reducir al mínimo el tiempo y los esfuerzos necesarios para llevar a cabo el proceso de auditoría. Esto sólo se puede lograr si la metodología tiene un modelo teórico subyacente (en nuestro enfoque es un modelo de análisis multicriterio jerárquico)
- Adaptar esta metodología a nuevas aplicaciones tales como sistemas de información basados en la web.
- Implementar una herramienta de auditoría asistida por computadora, lo que aumenta la eficacia y la eficiencia del proceso de auditoría.

La Auditoria de un sistema de información basado en Web – Un método basado en dominios

La característica fundamental de este marco, llamado INFAUDITOR, es que los dominios de auditoría y criterios de auditoría se pueden combinar para formar un árbol jerárquico que se define como un conjunto finito de nodos de tal manera que:
los nodos no terminales representan los dominios de auditoría y subdominios (por ejemplo, las aplicaciones heredadas, las aplicaciones basadas en web, metodología de desarrollo, las características del sistema y la documentación, la seguridad del sistema, el sistema de información de marketing , etc.), los nodos terminales representan dominios elementales a las que se deben aplicar las pruebas de control.

INFAUDITOR considera dos tipos de árboles:

- Un árbol general que abarque todos los ámbitos del sistema de información y pruebas de control.
- Varios sub- árboles que no son independientes correspondientes a la auditoría de determinados dominios de información del sistema, como un WBIS.

Cuando la auditoría de un dominio particular tal como en un WBIS, los pesos se atribuyen a los nodos del árbol en general, lo que lleva a un sub-árbol personalizado. Para cada prueba de control se da a los nodos terminales del sub-árbol un grado (o una apreciación cualitativa). Los pesos y las calificaciones que el auditor pueda determinar, resultará de diferentes dominios, dando lugar a una puntuación global de auditoría . Basándose en estas evaluaciones, el auditor puede escoger la opinión que mejor clasifica los sistema de información del cliente. La estructura del árbol jerárquico de auditoría se representa de la siguiente manera (figura 3), donde D indica dominio, SD para el subdominio, T para la prueba de control, G para el grado y W para el peso. Por ejemplo , la prueba de control T1 , 2 da como resultado un grado G1 , 2 , el dominio D1 puede entonces ser evaluada para W1 , 1 * G1 , 1 + W1 , 2 * G1 , 2 . Entonces la evaluación D1 se pondera por W1 en el grado de evaluación global.

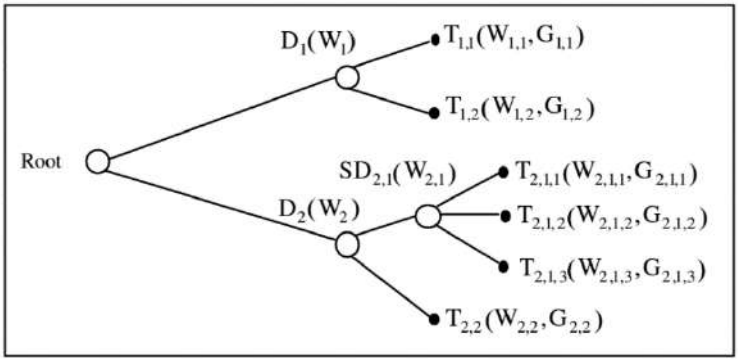

Fig. 3. Estructura del árbol jerárquico de decisiones.

Todos los resultados se dan en una escala cuantitativa. En cualquier nivel del árbol, la suma de los pesos de los hijos de un nodo es igual a 1. Los pesos de los nodos indican no sólo su participación en la evaluación final, sino también las pruebas que el auditor debe realizar.

El árbol de auditoría general es muy amplio, ya que el sistema de auditoría de información involucra a muchos dominios. Una originalidad de INFAUDITOR es que abarca todos los aspectos del sistema de auditoría de la información, mientras que otros métodos por lo general se centran tanto en los aspectos de gestión (marketing, recursos humanos, sistemas de información logística, etc.) o en los aspectos técnicos (red informática, la seguridad del sistema, las aplicaciones, nuevos proyectos, etc.) INFAUDITOR incorpora así el conocimiento de los diferentes ámbitos de sistemas de información.

El árbol de auditoría en general se lleva a cabo por las reglas. Para cada nodo del árbol (que representa el dominio o subdominio a auditar), una regla representa el vínculo entre este nodo y su padre. El manejo del árbol por las normas hace que sea fácil de mantener y favorece un enfoque de creación de prototipos. El enriquecimiento del árbol requiere sólo la adición de nuevas normas, sin tener que volver a escribir toda la estructura.

Esta capacidad de personalización a través de reglas es una importante contribución de INFAUDITOR. Este proceso de personalización se ha aplicado a los WBIS resultantes en la auditoría sub-árbol proporcionada a continuación (figura 4). Argumentamos que los tres criterios (calidad, seguridad, facilidad de lectura) mencionados anteriormente son adecuados para la evaluación de los WBIS. Estos criterios se han descompuesto en varios sub- criterios, teniendo en cuenta las características específicas de WBIS. La primera columna representa los criterios globales (calidad, seguridad, facilidad de

lectura). La segunda columna representa sus respectivos sub-criterios. Por ejemplo, la conformidad, la facilidad de uso, etc. son los sub -criterios de calidad. Este proceso de descomposición se repite para cada sub-criterio que conduce a la sexta columna.

Este enfoque de la auditoría puede ser utilizado en diferentes niveles de detalle (dominio, dominios sub-dominio, elementales) como herramienta de auditoría de los auditores y los usuarios finales (figura 4).

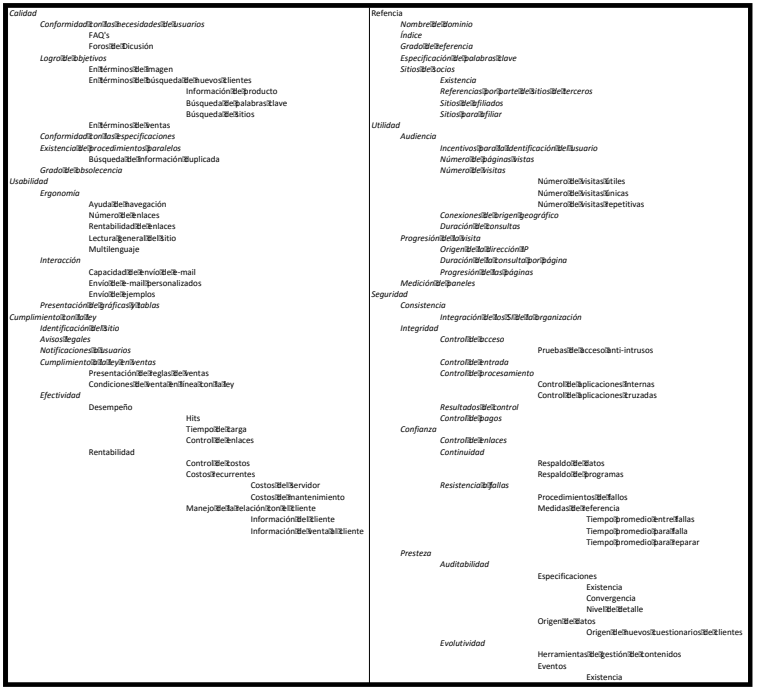

Figura 4. Árbol de auditoría de WBIS

CONCLUSIONES

La auditoría de sistemas web ofrece una importante ocasión de volver a evaluar la afirmación de que los marcos tradicionales de auditoría no son adecuados para la evaluación del sitio web. Hemos definido un enfoque basado en dominios para que los auditores realicen de forma eficaz y eficiente un proceso de auditoría de sitios web, tomándolo como un enfoque de ahorro de costos en la práctica de auditoría de WBIS. Con el uso de un proceso analítico jerárquico, el proceso de auditoría se estructura como un árbol jerárquico de evaluación, por lo tanto los controles de auditoría sólo se realizan en los nodos terminales, minimizando el tiempo y el esfuerzo necesarios para evaluar todo el dominio (recordemos que COBIT no tiene ninguna estructura jerárquica) por lo tanto, se deben realizar todas las pruebas de auditoría. Finalmente, nuestro enfoque ha sido ampliamente utilizado para auditar varios dominios que ofrecen una alternativa a COBIT. Una limitación fundamental de todo el enfoque de auditoría de WBIS tal como se presenta en este trabajo es la falta de consideración de las interdependencias entre los criterios. Estas interdependencias se pueden manejar mediante el uso de enlaces entre los criterios. Otra limitación es la falta de instrumento de orientación que permita a los auditores para decidir la mejor forma de proceder durante un proceso de auditoría, la forma de acceder a las explicaciones sobre lo que ha ocurrido durante las misiones de auditorías anteriores y la forma de acceder a la cada vez mayor información histórica que puede ser utilizada, por ejemplo al momento de decidir los valores que se asignan a los diferentes criterios. Por último, una limitación conocida es el relacionado con el proceso de jerarquía analítica subyacente de múltiples criterios de toma de decisiones.

REFERENCIAS

Akoka J., Comyn-Wattiau I. (2000) Auditing Computer and

Management Information Systems –Concepts, Methodologies and Applications, en Encyclopedia of Library and Information Science, Kent A. (Editor), Marcel Dekker, Inc. New York.

Atzeni P., Merialdo P., Sindoni G. (2002) Web Site Evaluation : Methodology and Case Study, DASWIS 2001, , Notas de lectura en Computer Science, N° 2465, Springer-Verlag, 2002.

Brown, W., Nasuti, F. (2005). What ERP Systems can Tell us about Sarbanes-Oxley. Information Management and Computer Security, 13(4), 311-327. Cadbury Report (1994) "Internal Control and Financial Reporting.

Champlain J.J (1998) Auditing Information Systems – A Comprehensive Reference Guide, John Wiley & Sons, Inc., New York.

Chang, J. C.-J., & King, W. R. (2005). Measuring the Performance of Information Systems: A Functional Scorecard. Journal of Management Information Systems, 22(1), 85-115.

Collier P., Dixon R., (1995) "The Evaluation and Audit of Management Information Systems", Managerial Auditing Journal, Vol. 10.

Danna E., Laroche A., (2000) "Auditing Web Sites Using Their Access Patterns", http://www9.org/final-posters/poster25.html, 9th WWW Conference, Amsterdam.

Deshpande Y., Chandrarathna A., Ginige A. (2002) "Web Site Auditing – First Step Towards Reengineering", Proceedings of SEKE'02.

Dewan R., Jing B., Seidmann A. (2000) "Adoption of Internet Based Product Customization and Pricing Strategies, Journal of Management Information Systems, Fall 2000, Vol. 17, N°2.

Grembergen, W. V., Haes, S. D., & Moons, J. (2005). Linking Business Goals to IT Goals and COBIT Processes. Information Systems Control Journal, 4, 18-22.