LA IMPORTANCIA DE ESTABLECER POLÍTICAS Y PROCEDIMIENTOS UNIFORMES PARA LA REALIZACIÓN DE AUDITORÍAS INTERNAS EN LOS SISTEMAS DE INFORMACIÓN DE LAS DISTINTAS DEPENDENCIAS DE UNA ORGANIZACIÓN: EL CASO DE LA UNIVERSIDAD DEL ENTORNO

Por

Luis D. Ortiz
Auditor de Sistemas de Información

Norman E. Cruz
Facultad
Recinto de Puerto Rico
University of Phoenix

Resumen

Las auditorías internas son el examen crítico, sistemático y detallado de los sistemas de información de una organización; realizadas por profesionales con vínculos laborales con la misma. Estos profesionales utilizan técnicas determinadas con el objetivo de emitir informes y formular sugerencias para el mejoramiento de la entidad o negocio. Las auditorías internas son servicios que reportan al más alto nivel de la gerencia de la organización y tienen características de función asesora de control; por tanto no pueden ni deben tener autoridad sobre ningún funcionario de la empresa, a excepción de los que forman parte del personal de la oficina de auditoría interna. Tampoco, deben involucrarse o comprometerse con las operaciones de los sistemas de la empresa, pues su función es evaluar y opinar sobre los mismos; para que la alta gerencia tome las medidas necesarias para su mejor funcionamiento. Para este estudio, se utilizó el caso real de una institución de educación superior para observar el efecto de no seguir las políticas y procedimientos uniformes de auditoría interna en sus unidades o recintos universitarios.

Introducción

Los objetivos principales de este estudio de caso son: establecer si puede una organización continuar realizando, a largo plazo, auditorías internas en los sistemas de información de todas sus dependencias—localidades, departamentos o áreas funcionales—sin

utilizar políticas y procedimientos uniformes; y detallar que repercusiones puede tener en la confiabilidad de los recursos informáticos de la institución. Se desarrolló este estudio considerando las inconsistencias que suponen las auditorías internas realizadas con políticas y procedimientos variados entre las dependencias de cualquier organización; ya sea, con o sin fines de lucro; tales como: las instituciones bancarias o las instituciones de educación superior.

Desde finales del siglo XX, los sistemas informáticos se han constituido en las herramientas más poderosas para materializar uno de los conceptos más vitales y necesarios para cualquier organización, los sistemas de información de la empresa. El procesamiento de datos está bajo la administración integral de la compañía y; por eso, las políticas y procedimientos propiamente informáticos deben estar; por tanto, establecidos en la misma. En consecuencia, los departamentos de informática forman parte de lo que se ha denominado la gerencia de la empresa. Cabe señalar que la informática no administra propiamente la organización, ayuda a la toma de decisiones, pero no decide por sí misma. Por ende, debido a su importancia en el funcionamiento de una empresa, existe la auditoría de sistemas de información (Cánaves, 1999).

Antecedentes de la Investigación

Se conoce la práctica de las auditorías desde hace varios siglos. Muchos reyes o gente poderosa tenían como exigencia la correcta administración de las cuentas por parte de los escribanos, de modo que se pudieran evitar desfalcos o que alguna persona se aprovechara de las riquezas que en aquella época costaban tanto sudor y sangre conseguir. Sin embargo, los precedentes de la auditoría, los encontramos en el siglo XIX, por el año 1862, donde aparece por primera vez la profesión de auditor o de desarrollo de auditoría bajo la supervisión de la ley británica de Sociedades Anónimas (Antecedentes, 2007). Para evitar todo tipo de fraude en las

cuentas, era necesaria una correcta inspección de las cuentas por parte de personas especializadas y ajenas al proceso, que garantizaran los resultados sin sumarse o participar en la estafa.

Desde entonces, y hasta principios del siglo XX, la profesión de auditoría fue creciendo y su demanda se extendió por toda Inglaterra, llegando a Estados Unidos, donde los antecedentes de las auditorías actuales fueron forjándose, en busca de nuevos objetivos donde la detección y la prevención del fraude pasaban a segundo plano y perdía cierta importancia.

En la década del 1940 los objetivos de las auditorías abarcaban; no tanto el fraude, como las posiciones financieras de la empresa, socios o clientes que las constituían, de modo que se pudieran establecer objetivos económicos en función de dichos estudios (Instituto de Auditores Internos de los Estados Unidos, 2010a). De manera paralela a dicho crecimiento de la auditoría, aparece también el antecedente de la auditoría interna o auditoría de gobernanza que en 1921 fue establecida de manera oficial mediante la construcción de la Oficina General de Contabilidad de los Estados Unidos (GAO, s.f.).

Planteamiento del Problema

La auditoría interna debe facilitar la medición de los resultados obtenidos en el desempeño del auditado y el grado de cumplimiento de sus metas y objetivos. Debe estar constituido por políticas formalmente adoptadas; procedimientos efectivamente implantados y; de recursos humanos, físicos y financieros; cuyo funcionamiento coordinado debe orientarse a salvaguardar sus pertenencias, a lograr las metas y a mejorar su desempeño como parte de una organización.

La auditoría interna es el conjunto de los planes, métodos, procedimientos, y otras medidas; incluyendo la actitud de la administración de una institución para ofrecer garantía razonable de que se cumplen con los siguientes objetivos (Universidad de Buenos Aires, s.f.):

- Promover las operaciones metódicas, económicas, eficientes y eficaces; y los productos y servicios de calidad, acorde con la misión que la institución debe cumplir.
- Preservar los recursos frente a cualquier pérdida por despilfarro, abuso, mala administración, errores, fraude e irregularidades.
- Elaborar y mantener datos financieros y de administración fiables y presentarlos correctamente en los informes aplicables.

Para asegurarse la implantación y el mantenimiento de un sistema eficiente de auditoría interna es necesario que el auditado cuente con:

- Recursos tecnológicos suficientes y asociados a sus procesos productivos y de apoyo.
- Recursos humanos con aptitud, capacitación, experiencia y grado de incentivo necesario para cumplir eficaz y eficientemente con las tareas delegadas.
- Cadenas de mando (responsabilidades) claramente definidas y evaluadas.
- Liderazgo y capacidad de administración en los niveles altos (directivos), que garantice la dinámica del ente o programa auditado.
- Sistema de información que permita la permanente y sistemática evaluación preventiva de la ejecución y la toma de decisiones correctas y oportunas.

Por tanto, ¿cuán fundamental es ejecutar de manera invariable las políticas y procedimientos aprobados para realizar las auditorías internas en los sistemas de información entre las dependencias de una organización?

Justificación del Estudio

Durante el proceso de identificación y análisis del problema, se encontraron pocas fuentes en la literatura—inclusive al buscar a través de bancos de artículos de asociaciones profesionales y académicas—trabajos que establezcan la importancia de ejecutar políticas y procedimientos uniformes para la realización de auditorías internas en los sistemas de información de las distintas dependencias de una organización y, que paralelamente, busquen determinar qué consecuencias puede tener en la confiabilidad de los recursos informáticos de la institución.

En toda entidad bien organizada y para poder mantener la vigilancia sobre la cadena de mando de la administración, se hace necesario la creación de un programa sistemático de fiscalización para comprobar que las responsabilidades delegadas han sido bien encausadas y, que las políticas y procedimientos establecidos se han llevado; tal como estaba previsto. Además, es de suma importancia que exista una revisión frecuente por personal calificado para determinar que el sistema de control interno es el adecuado, y mediante pruebas constantes, determinar que han resultado operativamente efectivos. De existir fallas, deficiencias o cambios en las condiciones existentes, debido a lo cual el sistema de control interno resulte inefectivo; debe ser modificado apropiadamente efectuando los cambios necesarios a las nuevas situaciones (Hernández Meléndez y Sánchez Gómez, 2007).

Marco Conceptual

Fundada en 1969, ISACA desarrolla estándares internacionales de auditoría y control de sistemas de información que ayudan a sus miembros a garantizar la confianza y el valor de los sistemas de información. Asimismo, legitima los avances y habilidades de los conocimientos de tecnología informática a través de la Certificación de Auditor en Sistemas de Información

(CISA, por sus siglas en inglés), la Certificación de Gerente de Seguridad de la Información (CISM, por sus siglas en inglés), la Certificación en Gobernanza de Tecnologías de la Información Empresarial (CGEIT, por sus siglas en inglés) y el Certificado en Control de Riesgos y de Sistemas de Información (CRISC, por sus siglas en inglés). Además, ISACA actualiza continuamente CobiT®, que ayuda a los profesionales y líderes empresariales de las tecnologías de información (TI) a cumplir con sus responsabilidades de administración; particularmente en las áreas de cumplimiento, seguridad, riesgo y control, para proveer valor añadido a la organización (ISACA, 2011).

Preguntas de Investigación

El presente trabajo de investigación se basó en las siguientes preguntas:

Pregunta 1: ¿Puede una organización, por tiempo indefinido, realizar auditorías internas en los sistemas de información de todas sus dependencias sin utilizar políticas y procedimientos uniformes?

Pregunta 2: ¿Cuáles son las repercusiones que puede tener esta situación—falta de políticas y procedimientos uniformes—en los recursos informáticos de la institución?

Limitaciones y Delimitaciones del Estudio

Esta investigación se limitó a la importancia de establecer políticas y procedimientos uniformes para la realización de auditorías internas en los sistemas de información de las distintas dependencias de una organización; en específico, el caso de la Universidad del Entorno.

Con el pasar del tiempo, han proliferado las actividades ilegales que ponen en peligro la protección y el buen funcionamiento de los sistemas informáticos. Este hecho, imposibilita desarrollar políticas y procedimientos que garanticen resolver continuamente; todos los problemas relacionados con la confiabilidad de los sistemas de información. También, se puede

dar el caso de que este estudio quede obsoleto en el futuro, tras el avance vertiginoso de la tecnología; donde nuevas tecnologías de informática pueden ser más efectivas y eficaces que las actuales.

Importancia del Estudio

La auditoría de sistemas de información persigue el control de la función informática, el análisis de la eficiencia de los sistemas informáticos que permite la verificación del cumplimiento de los procedimientos de la empresa en este ámbito y la revisión de la eficaz administración de los recursos informáticos.

El auditor informático ha de velar por la correcta utilización de los amplios recursos que la empresa pone en juego para disponer de un eficiente sistema de información. Claro está, que para la realización de una auditoría informática eficaz, se debe entender a la empresa en su más amplio sentido; ya que una universidad es tan organización como una empresa privada. Todos utilizan la informática para administrar sus negocios de forma rápida y eficiente con el fin de obtener beneficios económicos.

Por eso, al igual que los demás componentes de la empresa, los sistemas de información están sometidos al control correspondiente, o al menos debería estarlo. La importancia de llevar un control de esta herramienta se puede deducir de varios aspectos. He aquí algunos:

- Las computadoras y los centros de procesamiento de datos se convirtieron en blancos deseables no solo para el espionaje, sino para la delincuencia y el terrorismo. En este caso, interviene la auditoría informática de seguridad.
- Las computadoras creadas para procesar y difundir resultados o información elaborada pueden producir resultados o información errónea si dichos datos son, a su vez, erróneos. Este concepto obvio es a veces olvidado por las mismas

> empresas que terminan perdiendo de vista la naturaleza y calidad de los datos de entrada a sus sistemas informáticos, con la posibilidad de que se provoque un efecto cascada y afecte a aplicaciones independientes. En este caso, interviene la auditoría informática de datos.

Un sistema informático mal diseñado puede convertirse en una herramienta muy peligrosa para la empresa; ya que las máquinas obedecen ciegamente las órdenes recibidas y la operación de la empresa está determinada por las computadoras que conforman los sistemas de información. La administración y la organización de la empresa no puede depender de un conjunto de programados y aplicaciones mal diseñadas; además, de equipos mal configurados. Éstos son solo algunos de los inconvenientes que puede presentar un sistema informático; por ello, la necesidad de la auditoría de sistemas de información (Cánaves, 1999).

Para desarrollar esta investigación, el enfoque se hizo a través de los siguientes temas: las auditorías internas en los sistemas de información, las políticas y procedimientos en el campo de la informática, y sus efectos si no hay uniformidad en los mismos. Aunque no excluye a otros sectores, este es un estudio de caso de una institución de educación superior—la Universidad del Entorno. A continuación, se discute qué son las auditorías internas y su función en las organizaciones.

Revisión de Literatura

Auditoría Interna

Según el Instituto de Auditores Internos de los Estados Unidos (2010b, p. 4), la auditoría interna es:

> Una actividad independiente y objetiva de garantía y consulta, concebida para agregar valor y mejorar las operaciones de una organización. Ayuda a una organización a

cumplir sus objetivos aportando un enfoque sistemático y disciplinado para evaluar y mejorar la eficacia de los procesos de manejo de riesgos, control y gobierno.

La auditoría interna surge con posterioridad a la auditoría externa por la necesidad de mantener un control permanente y más eficaz dentro de la empresa y de hacer más rápida y eficaz la función del auditor externo. Generalmente, la auditoría interna clásica se ha venido ocupando fundamentalmente del sistema de control interno; es decir, del conjunto de medidas, políticas y procedimientos establecidos en las empresas para proteger el activo, minimizar las posibilidades de fraude, incrementar la eficiencia operativa y optimizar la calidad de la información económico-financiera. Se ha centrado en el terreno administrativo, contable y financiero (León Lefcovich, 2007).

Según el autor, la necesidad de la auditoría interna se pone de manifiesto en una empresa a medida que ésta aumenta en volumen, extensión geográfica y complejidad y hace imposible el control directo de las operaciones por parte de la gerencia. Con anterioridad, el control lo ejercía directamente la gerencia de la empresa por medio de un permanente contacto con sus mandos intermedios, y hasta con los empleados de la empresa. En la gran empresa moderna esta peculiar forma de ejercer el control; ya no es posible, y de ahí la emergencia de la llamada auditoría interna.

Además, León Lefcovich (2007) indica que el objetivo principal es ayudar a la gerencia en el cumplimiento de sus funciones y responsabilidades, proporcionándole análisis objetivos, evaluaciones, recomendaciones y todo tipo de comentarios pertinentes sobre las operaciones examinadas. Este objetivo se cumple a través de otros más específicos como los siguientes:

- Verificar la confiabilidad o grado de razonabilidad de la información contable y no contable, generada en los diferentes niveles de la organización.

- Vigilar el buen funcionamiento del sistema de control interno (lo cual implica su evaluación y reemplazo), tanto el sistema de control interno contable como el operativo.

CobiT®

Según indica el IT Governance Institute (2007), la misión de CobiT® es investigar, desarrollar, hacer público y promover un marco de referencia sobre el control de gobernanza de las tecnologías de información autorizado, actualizado y aceptado internacionalmente para la adopción por parte de las empresas; y el uso diario por parte de gerentes de negocio, profesionales de tecnología de información (TI) y profesionales de cumplimiento. Un marco de referencia para la gobernanza de TI define las razones de por qué se necesita, quiénes son los interesados y qué se necesita cumplir en la gobernanza de TI.

La orientación a los negocios es el tema principal de CobiT®. Está diseñado para ser utilizado no solo por proveedores de servicios, usuarios y auditores de TI; sino también y principalmente, como guía integral para la gerencia y para los dueños de los procesos de negocio.

El marco de trabajo CobiT® proporciona la información que la empresa requiere para lograr sus objetivos, la empresa necesita invertir en, y administrar y controlar los recursos de TI usando un conjunto estructurado de procesos que provean los servicios que entregan la información empresarial requerida. El marco de trabajo CobiT® ofrece herramientas para garantizar la alineación con los requerimientos del negocio.

Para satisfacer los objetivos del negocio, la información necesita adaptarse a ciertos criterios de control, los cuales son referidos en CobiT® como requerimientos de información del

negocio. Con base en los requerimientos más amplios de calidad, mandatorios y de seguridad, se definieron los siguientes siete criterios de información.

- La efectividad tiene que ver con que la información sea relevante y pertinente a los procesos del negocio, y se proporcione de una manera oportuna, correcta, consecuente y utilizable.
- La eficiencia consiste en que la información sea generada con el óptimo—más productivo y económico—uso de los recursos.
- La confidencialidad se refiere a la protección de información sensitiva contra revelación no autorizada.
- La integridad está relacionada con la precisión y completitud de la información, así como con su validez de acuerdo a los valores y expectativas del negocio.
- La disponibilidad se refiere a que la información esté disponible cuando sea requerida por los procesos del negocio en cualquier momento. También concierne a la protección de los recursos y las capacidades necesarias asociadas.
- El cumplimiento tiene que ver con acatar aquellas leyes, reglamentos y acuerdos contractuales a los cuales está sujeto el proceso de negocios; es decir, criterios de negocios impuestos externamente, así como políticas internas.
- La confiabilidad se refiere a proporcionar la información apropiada para que la gerencia administre la entidad y ejerza sus responsabilidades mandatorios y de gobernanza.

Los procesos requieren de controles y éstos se definen como las políticas, procedimientos, prácticas y estructuras organizacionales diseñadas para brindar una seguridad razonable, que los objetivos de negocio se alcanzarán, y los eventos no deseados serán

prevenidos o detectados y corregidos. IT Governance Institute (2007), Los objetivos de control de TI proporcionan un conjunto completo de requerimientos de alto nivel a considerar por la gerencia para un control efectivo de cada proceso de TI, que:

- Son sentencias de acciones de gerencia para aumentar el valor o reducir el riesgo.
- Consisten en políticas, procedimientos, prácticas y estructuras organizacionales.
- Están diseñadas para proporcionar un aseguramiento razonable de que los objetivos de negocio se conseguirán y que los eventos no deseables se prevendrán, detectarán y corregirán.

La gerencia de la empresa necesita tomar decisiones relativas a estos objetivos de control:

- Seleccionando aquellos aplicables.
- Decidir aquellos que deben implantarse.
- Elegir como implantarlos—frecuencia, extensión, automatización, entre otros.
- Aceptar el riesgo de no implantar aquellos que podrían aplicar.

Mientras, la gerencia de operaciones usa los procesos para organizar y administrar las actividades de TI en curso. CobiT® brinda un modelo genérico de procesos que representa todos los procesos que normalmente se encuentran en las funciones de TI, proporcionando un modelo de referencia general y entendible para la gerencia de operaciones de TI y para la gerencia de negocios. Para lograr una gobernanza efectiva, los gerentes de operaciones deben implementar los controles necesarios dentro de un marco de control definido para todos los procesos TI. Ya que los objetivos de control de TI de CobiT® están organizados por procesos de TI, el marco de trabajo brinda vínculos claros entre los requerimientos de gobernanza de TI, los procesos de TI y los controles de TI.

Cada uno de los procesos de TI de CobiT® tiene un objetivo de control de alto nivel y varios de objetivos de control detallados. Como un todo, representan las características de un proceso bien administrado.

En resumen, los controles efectivos reducen el riesgo; aumentan la probabilidad del valor añadido y aumentan la eficiencia; debido a que habrá menos errores y un enfoque de administración más consecuente. Además, CobiT® ofrece ejemplos ilustrativos para cada proceso, los cuales no son exhaustivos o preceptivos de:

- Entradas y salidas genéricas—tareas divididas por fases o etapas
- Actividades y guías sobre roles y responsabilidades en una matriz—por ejemplo, el Modelo RACI (Osiatis, 2011):

  Encargado (Responsible) - Es la persona encargada de hacer la tarea en cuestión.

  Responsable (Accountable) - Es la única persona responsable de la correcta ejecución de la tarea.

  Consultado (Consulted) - Son las personas que deben ser consultadas para la realización de la tarea.

  Informado (Informed) - Son las personas que deben ser informadas sobre el progreso de ejecución de la tarea.
- Metas de actividades clave—las cosas más importantes a realizar
- Métricas—para corroborar el desempeño actual contra el desempeño deseable

La Universidad del Entorno

La Universidad del Entorno consiste de varias unidades o recintos. Todas las unidades deben regirse por las políticas, procedimientos y reglamentos aprobados por la Oficina de

Auditoría Interna de la Junta de Síndicos de la Universidad del Entorno (Universidad del Entorno, s.f.).

La Oficina de Auditoría Interna

Según establece la Junta de Síndicos de la Universidad del Entorno (2010a), la Oficina de Auditoría Interna (OAI) se creó en 1960 por disposición administrativa. En febrero de 1979, el Consejo de Educación Superior (CES), ahora Junta de Síndicos, determinó que la Oficina pasara a formar parte de la Secretaría Ejecutiva de dicho Cuerpo. En ese momento se ratificó la adopción del Sistema de Auditoría Operacional para la Universidad del Entorno.

La Carta Constitutiva o el Reglamento Sobre el Funcionamiento y Operación de la Oficina de Auditoría Interna de la Universidad del Entorno es el documento formal que establece la estructura, el propósito, el alcance y la responsabilidad de la actividad de auditoría interna. El mismo dispone la posición de la OAI dentro de la Universidad del Entorno; autoriza el acceso a los récords, al personal y a los bienes universitarios relevantes para la ejecución de los trabajos (Junta de Síndicos de la Universidad del Entorno, 2010b).

El Comité de Auditoría (CA) de la Junta de Síndicos es el encargado de la supervisión general de los procesos de auditoría interna y su administración en la Universidad, así como en lo relativo a los informes del Contralor. Los auditores internos y el CA tienen metas y objetivos entrelazados, por lo que mantienen una relación estrecha para cumplir con los mismos. El Director de la OAI responde funcionalmente al CA y participa en sus reuniones.

La OAI está facultada para realizar proyectos de auditorías, proyectos especiales y trabajos de consultoría, entre otros. El tipo de proyecto dependerá del objetivo de la evaluación. Según establece la Norma 1210.A.2 del Instituto de Auditoría Interna (IIA en sus siglas en inglés), el auditor interno debe tener suficientes conocimientos para evaluar el riesgo de fraude y

la forma en que la Gerencia lo maneja, pero no se espera que tenga la pericia de aquellas personas cuya responsabilidad principal es la detección e investigación del fraude.

Al realizar su trabajo, el auditor debe estar alerta a situaciones que puedan ser indicadoras de posibles fraudes o irregularidades. A continuación una breve descripción de los tipos de auditorías que se realizan (Junta de Síndicos de la Universidad del Entorno, 2010c):

- Auditorías Operacionales

  Es el examen independiente, objetivo y sistemático de las operaciones de un área o actividad con enfoques o alcances en alguna de las siguientes áreas:

  Operacionales, Financieras y de Cumplimiento - Para determinar el grado de efectividad, economía y eficiencia de las operaciones, procesos o funciones y si se cumple con las leyes, políticas y reglamentos aplicables.

  Evaluación de programa - Para determinar si los programas lograron los objetivos deseados.

- Auditorías de Tecnologías de Informática

  Es el examen de la administración, operación y seguridad de las tecnologías de informática utilizadas en la institución. En términos generales, el propósito de este tipo de auditoría es verificar que las operaciones computadorizadas se ejecutan según lo autorizado por la Gerencia, las transacciones se registran correctamente para la generación de informes confiables, el acceso a los activos es permitido de acuerdo con lo establecido por la Gerencia y éstos se utilizan para apoyar los objetivos institucionales.

- Proyectos Especiales

  Es el examen de una operación o de un grupo de operaciones específicas de un proyecto, programa o de una parte de la información financiera realizado en cualquier momento con un fin determinado. Estas usualmente no han sido programadas, en su lugar surgen de una petición especial de la Gerencia, una recomendación de la OAI al CA en el transcurso del año fiscal o alguna confidencia recibida. Puede incluir una combinación de objetivos financieros, de cumplimiento y operacionales. Generalmente, éstos son realizados por el área de Prevención, Consultoría y Calidad (OAIQ).

- Servicios de Consultoría

  La OAI ofrece servicios de consultoría, asesoramiento y servicios relacionados cuya naturaleza y alcance se establece en acuerdo con el solicitante. Estos están dirigidos a añadir valor y a mejorar los procesos de gobernanza, manejo de riesgos y control sin que el auditor asuma responsabilidades de la

Gerencia. Los acuerdos sobre objetivos, alcance y limitaciones del trabajo deben formalizarse por escrito en conjunto con la Gerencia.

- Seguimientos a la resolución de los hallazgos de las auditorías

  Es el proceso de examinar las acciones correctivas implementadas para resolver los hallazgos de auditorías previas. La OAI tiene la responsabilidad de dar seguimiento a los hallazgos identificados en nuestros informes y los informes del Contralor.

- Supervisión de Inventarios

  Es la supervisión de la toma y valoración de los inventarios al cierre del año fiscal. Esta labor se realiza a base de la materialidad del inventario, prioridades de trabajo y disponibilidad de recursos humanos en el momento.

Procedimientos de la Oficina de Auditoría Interna

La Junta de Síndicos, en su reunión ordinaria del 20 de febrero de 2010, habiendo considerado la recomendación de su Comité de Auditoría y con el endoso del Presidente de la Universidad del Entorno, acordó establecer lo siguiente: Procedimiento para dar seguimiento y cumplir con las disposiciones de ley y de reglamento en relación con los informes de auditorías a la Universidad del Entorno por la Oficina del Contralor, la Oficina de Auditoría Interna de la Junta de Síndicos y los auditores externos (Junta de Síndicos de la Universidad del Entorno, 2010d).

Por otro lado, la Oficina de Auditoría Interna acordó establecer lo siguiente: Procedimiento para ofrecer información a la Oficina de Auditoría Interna sobre un posible uso ilegal o no autorizado de fondos o propiedad de la Universidad del Entorno (Junta de Síndicos de la Universidad del Entorno, 2010e).

Procedimientos Alternos

A pesar de que los procedimientos antes descritos, deben ser aplicados a todas las unidades del Sistema de la Universidad del Entorno como estipulan los mismos; lo cierto es que, hay dependencias que han desarrollado sus procedimientos internos para atender de manera particular sus actividades. Este es el caso, del Recinto Tres. Su personal del Centro de Tecnología de Información hizo una revisión, el 27 de julio de 2010, del Procedimiento para la disposición de información sensitiva y programados de equipos computadorizados y almacenamiento de datos (Recinto Tres de la Universidad del Entorno, 2010).

Por otro lado, está el Manual de Normas y Medidas de Seguridad dirigidas al Usuario de Tecnologías de Información del Recinto Universitario Ocho de la Universidad del Entorno (2007). Además, están los procedimientos para los servicios específicos de la Oficina de Sistemas de Información del Recinto de Recinto Dos de la Universidad del Entorno (s.f.).

En resumen, se han establecido las bases para el desarrollo de este estudio y se introduce el concepto de uniformidad en las políticas y procedimientos para la realización de auditorías internas en los sistemas de información de todas las unidades de la Universidad del Entorno.

Metodología

Los objetivos principales de esta investigación son: establecer si puede una organización continuar realizando, a largo plazo, auditorías internas en los sistemas de información de todas sus dependencias sin utilizar políticas y procedimientos uniformes; y detallar qué repercusiones puede tener en la confiabilidad de los recursos informáticos de la institución. Para cumplir con los objetivos antes mencionados, se consideró el uso de una metodología genérica como preámbulo para realizar las auditorías en los sistemas informáticos.

Fases de una Auditoría de Sistemas de Información

Las personas que participan en las auditorías internas de los sistemas informáticos de una organización ejercen múltiples tareas a través las siguientes fases (Soto, s.f.). Refiérase a la Figura 1.

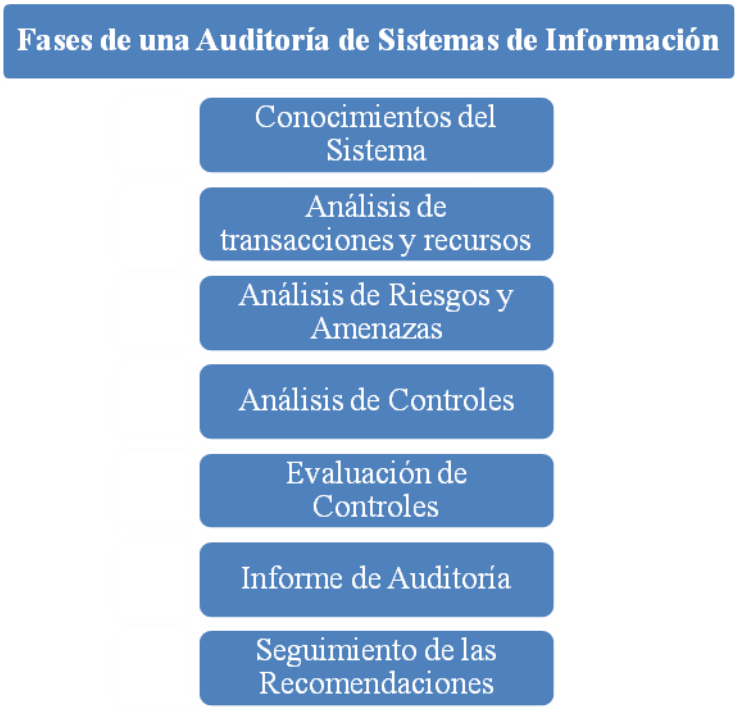

Figura 1. **Diagrama de las Fases de una Auditoría de Sistemas de Información**

Fase 1 - Conocimientos del Sistema

La primera fase consiste en los aspectos legales y políticas internas. Sobre estos elementos está cimentado el sistema de control y; por tanto, constituyen el marco de referencia para su evaluación. Por otro lado, en esta fase se incluyen las características del sistema operativo; tales como: el organigrama del área que participa en el sistema; el manual de las funciones y responsabilidades de las personas que participan en los procesos del sistema; y los informes de auditoría realizadas anteriormente. Finalmente, en esta fase se reúnen las características de la aplicación de computadora; tales como: el manual técnico de la aplicación

del sistema; los usuarios autorizados para administrar la aplicación; los equipos utilizados en la aplicación de computadora; la seguridad de la aplicación (contraseñas y/o claves de acceso); y los procedimientos para la generación y almacenamiento de los archivos de la aplicación.

Fase 2 - Análisis de las Transacciones y Recursos

En la segunda fase, dependiendo del tamaño del sistema, las transacciones se dividen en procesos y éstos en subprocesos. La importancia de las transacciones deberá ser asignada con la ayuda de los administradores. Por otro lado, en esta fase se incluye el análisis de las transacciones donde se establece el flujo de los documentos. En esta etapa se hace uso de los flujo gramas ya que facilita la visualización del funcionamiento y recorrido de los procesos. Además, se hace el análisis de los recursos donde se identifican y codifican los recursos que participan en el sistema. Finalmente, se establece la relación entre las transacciones y los recursos.

Fase 3 - Análisis de Riesgos y Amenazas

En la tercera fase, se hace un análisis de riesgos y amenazas al sistema que incluye la identificación de riesgos; por medio, de los daños físicos o destrucción de los recursos; la pérdida por fraude o desfalco; el extravío de documentos, archivos o informes; el robo de dispositivos o medios de almacenamiento; la interrupción de las operaciones del negocio; la pérdida de integridad de los datos; la ineficiencia de las operaciones y; de errores cometidos voluntaria o involuntariamente por individuos a cargo. Por otro lado, en esta fase se incluye la identificación de las amenazas; tales como: las amenazas sobre los equipos; las amenazas sobre los documentos; las amenazas sobre los programados o aplicaciones. Finalmente, se establece la relación entre los recursos, las amenazas y los riesgos potenciales. La relación entre estos

elementos deberá establecerse a partir de la observación de los recursos en su ambiente real de funcionamiento.

Fase 4 - Análisis de Controles

En la cuarta fase, se hace una codificación de controles. Los controles se aplican a los diferentes grupos que utilizan los recursos disponibles, luego la identificación de los controles debe contener una codificación; la cual, identifique el grupo al cual pertenece el recurso protegido. Además, en esta fase se establece la relación entre los recursos, las amenazas y los riesgos potenciales. La relación con los controles debe establecerse para cada recurso, amenaza y riesgo potencial identificado. Para cada uno de ellos, debe establecerse uno o más controles. Finalmente, se establece el análisis de cobertura de los controles requeridos. Este análisis tiene como propósito determinar si los controles que el auditor identificó como necesarios proveen una protección adecuada de los recursos.

Fase 5 - Evaluación de Controles

En la quinta fase, se establecen los objetivos de la evaluación; se verifica la existencia de los controles requeridos; y se determina la eficacia de los controles existentes. Además, se desarrolla el plan de pruebas de los controles que incluye la selección del tipo de prueba a realizar. Aquí, se debe solicitar al área respectiva, todos los elementos necesarios de prueba. Luego, se desarrollan las pruebas de controles y; finalmente, se analizan los resultados obtenidos de las pruebas.

Fase 6 - Informe de Auditoría

En la sexta fase, se redacta el informe detallado de las recomendaciones. Además, se hace una evaluación de las respuestas obtenidas durante la ejecución de la auditoría. Finalmente, se redacta el informe resumen para la alta gerencia. Este informe debe prepararse una vez

obtenidas y analizadas las respuestas de compromiso de las áreas afectadas. Este informe debe incluir, por lo menos, lo siguiente:

1. Introducción
    - Objetivo y contenido del informe de auditoría
2. Objetivos de la auditoría
3. Alcance
    - Cobertura de la evaluación realizada
4. Opinión
    - Relacionado a la suficiencia del control interno del sistema evaluado
5. Hallazgos
6. Recomendaciones

Fase 7 - Seguimiento de las Recomendaciones

En la séptima fase, se redacta el informe o los informes de seguimiento a las recomendaciones. Además, de hacer una evaluación de los controles implantados para determinar si éstos permiten la apropiada resolución de las deficiencias encontradas y señaladas en el Informe de Auditoría.

Con el establecimiento, aprobación y ejecución de una metodología para realizar auditorías internas de los sistemas informáticos de una organización se busca contribuir a lograr las metas y objetivos establecidos—la detección de irregularidades o ilegalidades en sus unidades, por medio de políticas y procedimientos uniformes. Aquí, se discutió la metodología que propone este estudio. A continuación, se ventilan los hallazgos obtenidos; además, de las conclusiones y recomendaciones de la investigación realizada.

Hallazgos

Los hallazgos de esta investigación se apoyaron en el análisis hecho a las operaciones descritas en los documentos disponibles en las páginas cibernéticas de la Oficina de Auditoría Interna de la Junta de Síndicos y los Recintos Universitarios de la Universidad del Entorno. A continuación, se detallan los resultados obtenidos dado la naturaleza de las auditorías internas que se realizan a cada una de las diferentes dependencias de la Universidad del Entorno.

Utilización de Formularios

Existe una serie de formularios para atender asuntos sobre ofrecer información confidencial, acciones correctivas, y evaluación del servicio prestado; que se presentan a continuación (Junta de Síndicos de la Universidad del Entorno, 2010f):

- Solicitud de Prórroga para Informes de Planes de Acción Correctiva

  Formulario para solicitar prórroga en el tiempo de entrega de informes de acción correctiva relacionados con los informes de auditoría o la Oficina del Contralor.

- Evaluación del Servicio de Auditoría

  Formulario que deberá completar el auditado, donde evalúa el servicio de auditoría que recibió. Su contribución nos ayudará a identificar fortalezas y evaluar debilidades para mejorar el servicio y así añadir valor a las actividades y operaciones de la Universidad del Entorno.

- Formulario de Informe de Acciones Correctivas

  El funcionario designado por el cuerpo rector de la Unidad auditada deberá completar este formulario con el detalle de las acciones que se realizarán para atender los hallazgos y las recomendaciones de la Oficina de Auditoría

Interna (OAI). El mismo deberá ser enviado a la OAI conforme a las instrucciones impartidas.

- Formulario para ofrecer Información Confidencial

  Formulario para ofrecer información a la OAI sobre un posible uso ilegal de fondos o propiedad y violaciones a leyes, políticas o reglamentos en la universidad.

Lo cierto es, que no todas las unidades del sistema de la Universidad del Entorno siguen los mismos procedimientos para éstas y otras actividades de la Oficina de Auditoría Interna. Esto debido a que varias dependencias se rigen por sus propias políticas y procedimientos internos de su Oficina de Sistemas de Información, como por ejemplo: el Recinto Dos, el Recinto Tres, el Recinto Seis y el Recinto Ocho.

Respuestas a las Preguntas del Estudio

Este trabajo de investigación exploratorio basó su análisis en las siguientes preguntas:

Pregunta 1: ¿Puede una organización, por tiempo indefinido, realizar auditorías internas en los sistemas de información de todas sus dependencias sin utilizar políticas y procedimientos uniformes?

Según lo indagado, se puede responder en la negativa. Es difícil ejecutar auditorías y poder determinar objetivamente cuáles unidades, del Sistema de la Universidad del Entorno, están cumpliendo con las directrices establecidas. Porque se puede dar el caso, de que las dependencias con políticas y procedimientos (normativas) más estrictos e inflexibles sean las mismas que obtengan las evaluaciones más bajas; aunque ello, no signifique que están desempeñándose peor que las demás. Pues, éstas últimas, pueden obtener mejores resultados en las evaluaciones dado a sus procedimientos menos exigentes y de más fácil cumplimiento.

Además, el tener distintos criterios de evaluación, le permite a cada unidad justificar sus posibles deficiencias. Esto, porque no tiene con cuáles dependencias compararse efectivamente. Por ejemplo, desde la falta de uniformidad en elementos tan básicos, como lo es el diseño de las páginas cibernéticas hasta la estructura de las direcciones en la red de cada recinto. Refiérase a la Tabla 1 para un resumen de los hallazgos obtenidos sobre el uso de normativas a través de las páginas cibernéticas de cada unidad del sistema de la universidad.

Tabla 1

Unidades del Sistema de la Universidad del Entorno y las Normativas utilizadas

Unidad	Normativas Utilizadas
Recinto Uno (2008)	Oficina de Auditoría Interna (OAI)
Recinto Dos (s.f.)	Híbrido—OAI e internas de la unidad que no siguen todo lo establecido por la OAI
Recinto Tres (2010)	Internas de la unidad que no siguen todo lo establecido por la OAI
Recinto Cuatro (2008)	OAI
Recinto Cinco (2008)	OAI
Recinto Seis (2009)	Híbrido—OAI e internas de la unidad que no siguen todo lo establecido por la OAI
Recinto Siete (2008)	OAI
Recinto Ocho (2007)	Híbrido—internas de la unidad y OAI que no siguen todo lo establecido por la OAI
Recinto Nueve (2010)	OAI
Recinto Diez (2008)	OAI
Recinto Once (s.f.)	OAI

En definitiva, esto acabará por disminuir el poder de la toma de decisiones de la alta gerencia—la Junta de Síndicos de la Universidad del Entorno a través de su Oficina de Auditoría

Interna, haciendo ineficaces las políticas y procedimientos institucionales que aprueben en el futuro sobre los sistemas informáticos.

Pregunta 2: ¿Cuáles son las repercusiones que puede tener esta situación—falta de políticas y procedimientos uniformes—en los recursos informáticos de la institución?

Las consecuencias pueden ser irreparables—desde multas económicas, pérdida de acreditaciones hasta sanciones punitivas. El aspecto más relevante en una auditoría de sistemas de información es identificar las posibles violaciones a los reglamentos establecidos; además, de las vulnerabilidades que pueden ser explotadas por individuos no autorizados. Conocer las debilidades de los sistemas de seguridad posibilita delinear un orden de prioridad frente a aquellos temas que significan riesgos menores.

Basado en el Modelo de Madurez para el Control Interno que describe CobiT® (IT Governance Institute, 2007, p. 175), se puede clasificar a la Universidad del Entorno entre un nivel 2—'Repetible pero Intuitivo' y un nivel 3—'Definido'. Refiérase a la Tabla 2 para más detalles.

Tabla 2

Modelo de Madurez para el Control Interno

Nivel de Madurez	Estado del Entorno de Control Interno	Establecimiento de Control Interno
0 (No existente)	No se reconoce la necesidad del control interno. El control no es parte de la cultura o misión organizacional. Existe un alto riesgo de deficiencias e incidentes de control.	No existe la intención de evaluar la necesidad del control interno. Los incidentes se manejan conforme van surgiendo.
1 (Inicial / ad Hoc)	Se reconoce algo de la necesidad del control interno. El enfoque hacia los requerimientos de riesgo y control es "ad Hoc" y	No existe la conciencia de la necesidad de evaluar lo que se necesita en términos de controles de TI. Cuando se llevan a cabo, son solamente de forma "ad

	desorganizado, sin comunicación o supervisión. No se identifican las deficiencias. Los empleados no están conscientes de sus responsabilidades.	Hoc", a alto nivel y como reacción a incidentes significativos. La evaluación sólo se enfoca al incidente presente.
2 (Repetible pero Intuitivo)	Existen controles pero no están documentados. Su operación depende del conocimiento y motivación de los individuos. La efectividad no se evalúa de forma adecuada. Existen muchas debilidades de control y no se resuelven de forma apropiada; el impacto puede ser severo. Las medidas de la gerencia para resolver problemas de control no son consecuentes ni tienen prioridades. Los empleados pueden no estar conscientes de sus responsabilidades.	La evaluación de la necesidad de control sucede solo cuando se necesita para ciertos procesos seleccionados de TI para determinar el nivel actual de madurez del control, el nivel meta que debe ser alcanzado, y las brechas existentes. Se utiliza un enfoque de taller informal, que involucra a los gerentes de TI y al equipo interesado en el proceso, para definir un enfoque adecuado hacia el control para los procesos, y para generar un plan de acción acordado.
3 (Definido)	Existen controles y están documentados de forma adecuada. Se evalúa la efectividad operativa de forma periódica y existe un número promedio de problemas. Sin embargo, el proceso de evaluación no está documentado. Aunque la gerencia puede manejar la mayoría de los problemas de control de forma predecible, algunas debilidades de control persisten y los impactos pueden ser severos. Los empleados están conscientes de sus responsabilidades de control.	Los procesos críticos de TI se identifican con base en impulsores de valor y de riesgo. Se realiza un análisis detallado para identificar requisitos de control y la causa raíz de las brechas, así como para desarrollar oportunidades de mejora. Además de facilitar talleres, se usan herramientas y se realizan entrevistas para apoyar el análisis y garantizar que los dueños de los procesos de TI son realmente los dueños e impulsan al proceso de evaluación y mejora.
4 (Administrado y Medible)	Existe un ambiente efectivo de control interno y de administración de riesgos. La evaluación formal y documentada de los controles	Se define de forma periódica qué tan críticos son los procesos de TI con el apoyo y acuerdo completo por parte de los dueños de los procesos

	ocurre de forma periódica. Muchos controles están automatizados y se realizan de forma periódica. Es probable que la gerencia detecte la mayoría de los problemas de control, aunque no todos los problemas se identifican de forma rutinaria. Hay un seguimiento consecuente para manejar las debilidades de control identificadas. Se aplica un uso de la tecnología táctico y limitado a los controles automatizados.	correspondientes. La evaluación de los requisitos de control se basa en las políticas y en la madurez real de estos procesos, siguiendo un análisis meticuloso y medido, involucrando a los interesados (Stakeholders) clave. La rendición de cuentas sobre estas evaluaciones es clara y está reforzada. Las estrategias de mejora están apoyadas en casos de negocio. El desempeño para lograr los resultados deseados se supervisa de forma periódica. Se organizan de forma ocasional revisiones externas de control.
5 (Optimizado)	Un programa organizacional de riesgo y control proporciona la solución continua y efectiva a problemas de control y riesgo. El control interno y la administración de riesgos se integran a las prácticas empresariales, apoyadas con una supervisión en tiempo real, y una rendición de cuentas completa para la vigilancia de los controles, administración de riesgos, e implantación del cumplimiento. La evaluación del control es continua y se basa en autoevaluaciones y en análisis de brechas y de causas raíz. Los empleados se involucran de forma pro-activa en las mejoras de control.	Los cambios en el negocio toman en cuenta que tan críticos son los procesos de TI, y cubren cualquier necesidad de reevaluar la capacidad del control de los procesos. Los dueños de los procesos realizan autoevaluaciones de forma periódica para confirmar que los controles se encuentran en el nivel correcto de madurez para satisfacer las necesidades del negocio, y toman en cuenta los atributos de madurez para encontrar maneras de hacer que los controles sean más eficientes y efectivos. La organización evalúa por comparación con las mejoras prácticas externas y busca asesoría externa sobre la efectividad de los controles internos. Para procesos críticos, se realizan evaluaciones independientes para proporcionar seguridad de que los controles se encuentran al nivel deseado de madurez y funcionan como fue planeado.

Cabe señalar que se lanzó la versión 5 de CobiT® (ISACA, 2012). Esta versión proporciona un marco de referencia con autoridad de gobernanza y administración de los sistemas de información empresarial y tecnología relacionada, a partir de la corriente ampliamente reconocida y aceptada de CobiT®; que vincula y se refuerza entre sí con todos los otros marcos de referencia importantes de ISACA, tales como:

- Board Briefing on IT Governance, 2nd Edition
- Business Model for Information Security ™
- IT Assurance Framework ™ (ITAF ™)
- Risk IT Framework
- Taking Governance Forward
- Val IT ™ Framework

Además, se entrelaza con otros marcos de referencia y estándares del mercado; tales como: ITIL e ISO, entre otros. Creando una mayor armonización entre todas las metodologías disponibles.

Conclusiones

Del estudio realizado se desprende que las políticas y procedimientos (normativas) que se aprueban en una organización, para las operaciones del área funcional encargada de las auditorías internas en los sistemas de información, deben ser ejecutadas de la misma manera por todos los involucrados. Con el fin de garantizar una auditoría uniforme para todas las dependencias; en este caso, cada una de las unidades del Sistema de la Universidad del Entorno.

La función de auditoría interna y sus tradicionales esquemas de trabajo se han visto impactados por la evolución de los sistemas de tecnología de la información y por la aplicación de nuevas estrategias administrativas motivadas por las necesidades de las instituciones de

expandir sus segmentos de mercado y, por la diversificación y garantía de la calidad en sus productos y servicios.

Estas realidades han propiciado que la demanda de los servicios de auditoría cobre relevancia; en este sentido los profesionales dedicados a la práctica de la auditoría interna, desde sus diversos ámbitos de actuación, buscan y desarrollan nuevos modelos de trabajo que satisfagan los requerimientos presentes de las organizaciones. Sin embargo, así mismo se debe reflexionar que la implantación de estos nuevos modelos de evaluación puede revolucionar los servicios que actualmente la auditoría interna proporciona a la organización, con la perspectiva de ofrecer más con menos recursos (Banca Central de México, s.f.).

También, se observa que para que estos nuevos modelos funcionen se necesita un cambio radical en la cultura y esquemas de control en las organizaciones que deberá estar apoyado por la decisión de los más altos niveles gerenciales de la misma—entiéndase, la Junta de Síndicos de la Universidad del Entorno a través de su Oficina de Auditoría Interna. En este ámbito de transformación de la auditoría interna, los sistemas informáticos de la organización representan un reto y una solución cuando son utilizados como un medio de evaluación constante de controles.

Por otro lado, la auditoría de los sistemas de información dará a las organizaciones; en definitiva, la posibilidad de conocer cómo trabajan en relación a la información y; en consecuencia, respecto al conocimiento. Proporcionará una "fotografía" del uso de la información que permitirá; a su vez, la identificación de las áreas de la organización que estén produciendo conocimiento y aquellas donde haya una necesidad de implantación de mecanismos para la transferencia de los mismos (Serrano González y Zapata Lluch, 2003).

Así, una vez realizada la auditoría, la organización se encontrará en disposición de desarrollar o mejorar su estrategia de manejo de la información y será capaz de sustentar el desarrollo de una correcta estrategia de manejo del conocimiento que; además, le permitirá acceder a sus fuentes de conocimiento, explotarlo mediante unos valores, una cultura y un liderazgo transformador que ayude a transferir o compartir formalmente los conocimientos a través del trabajo en equipo, utilizar la tecnología como un instrumento que facilita el aprendizaje y; por último, producir nuevo conocimiento como consecuencia de éste aprendizaje organizacional; ya sea individual o colectivo.

La auditoría de la información se presenta; por tanto, como punto de partida para el manejo del conocimiento o medio para saber qué conoce una organización. A través de las técnicas para la evaluación de operaciones procesadas a través de sistemas informáticos se podrá desarrollar un sistema automatizado de revisión, el cual permitirá a la auditoría cambiar de un enfoque de revisión periódica a un enfoque de revisión constante.

Recomendaciones

Se recomienda a quien esté interesado en continuar este tipo de estudio, incluir una mayor cantidad de casos sobre la función de auditoría de sistemas de información en las organizaciones, para comparar el desempeño de las que establecen y ejecutan las mismas políticas y procedimientos en cada una de sus dependencias—en este estudio, los recintos universitarios—con las que no siguen unos procedimientos idénticos. De esta forma se podría validar o no los resultados obtenidos en esta investigación.

También, se sugiere incluir en otros estudios cómo las auditorías internas pueden contribuir a erradicar las vulnerabilidades y los riesgos de los sistemas informáticos en las organizaciones. Posiblemente, esto permitirá desarrollar y justificar metodologías uniformes

para auditorías internas de sistemas de información en las instituciones de cualquier sector o industria—como por ejemplo: empresa privada, agencia de gobierno u organización sin fines de lucro.

En el caso particular del Sistema de la Universidad del Entorno, es imperativo que se le exija a cada una de las unidades que sigan—sin excusas o subterfugios—las normativas establecidas y aprobadas a nivel central. Esto con el fin, de lograr la anhelada uniformidad en los procesos de auditoría interna. La falta de políticas y procedimientos homogéneos suelen producir resultados no esperados y de difícil solución a corto plazo; provocando el gasto excesivo de recursos económicos y no económicos. Además, evita que la universidad pueda ser catalogada—al menos—como una organización administrable y medible; según el Nivel 4 del Modelo de Madurez para el Control Interno que describe CobiT®.

Referencias

Antecedentes (2007). *Antecedentes de la Auditoría*. Extraído el 15 de febrero de 2011 de la página http://www.antecedentes.net/antecedentes-auditoria.html

Banca Central de México (s.f.). *Mejores Prácticas en la Auditoría Interna*. Presentado durante la V Reunión de Auditores Internos de la Banca Central y Extraído el 18 de febrero de 2011 de la página http://www.cemla.org/pdf/aud-991109-mex.PDF

Cánaves (1999). *Auditoría Informática.* Extraído el 10 de febrero de 2011 de la página http://www.monografias.com/trabajos/auditoinfo/auditoinfo.shtml

GAO (s.f.). *La Historia de la Oficina de Contabilidad del Gobierno de los Estados Unidos*. Extraído el 15 de febrero de 2011 de la página http://gao.gov/about/ history/

Hernández Meléndez, E. y Sánchez Gómez, A.R. (2007). *La Auditoría Interna*. Extraído el 21 de febrero de 2011 de la página http://www.gestiopolis.com/ canales7/fin/la-auditora-y-el-control-interno.htm

Instituto de Auditores Internos de los Estados Unidos (2010a). *Historia y Metas del Instituto de Auditoría Interna*. Extraído el 15 de febrero de 2011 de la página http://www.theiia.org/theiia/about-the-institute/history-milestones/

Instituto de Auditores Internos de los Estados Unidos (2010b). *Definición de Auditoría Interna*. Extraído el 15 de febrero de 2011 de la página http://www.theiia.org/ guidance/standards-and-guidance/ippf/definition-of-internal-auditing/?search= internal audit definition

ISACA (2011). *Acerca de ISACA*. Extraído el 8 de febrero de 2011 de la página http://www.isaca.org/spanish/Pages/default.aspx

ISACA (2012). *COBIT® 5 Initiative—Status Update.* Extraído el 21 de mayo de 2012 de la página http://www.isaca.org/Knowledge-Center/cobit/Pages/COBIT-5-Initiative-Status-Update.aspx

IT Governance Institute (2007). *COBIT® 4.1*. Extraído el 8 de febrero de 2011 de la página http://www.isaca.org/Knowledge-Center/cobit/Documents/cobiT4.1 spanish.pdf

Junta de Síndicos de la Universidad del Entorno (2010a). *Oficina de Auditoría Interna*. Extraído el 28 de febrero de 2011 de su página cibernética

Junta de Síndicos de la Universidad del Entorno (2010b). *Reglamento sobre el funcionamiento y operación de la Oficina de Auditoría Interna de la Universidad del Entorno*. Extraído el 28 de febrero de 2011 de su página cibernética

Junta de Síndicos de la Universidad del Entorno (2010c). *Servicios de la Oficina de Auditoría Interna*. Extraído el 28 de febrero de 2011 de su página cibernética

Junta de Síndicos de la Universidad del Entorno (2010d). *Procedimiento para dar seguimiento y cumplir con las disposiciones de ley y de reglamento en relación con los informes de auditorías a la Universidad del Entorno por la Oficina del Contralor, la Oficina de Auditoría Interna de la Junta de Síndicos y los auditores externos*. Extraído el 28 de febrero de 2011 de su página cibernética

Junta de Síndicos de la Universidad del Entorno (2010e). *Procedimiento para ofrecer información a la Oficina de Auditoría Interna sobre un posible uso ilegal o no autorizado de fondos o propiedad de la Universidad del Entorno*. Extraído el 28 de febrero de 2011 de su página cibernética

Junta de Síndicos de la Universidad del Entorno (2010f). *Formularios de la Oficina de Auditoría Interna*. Extraído el 28 de febrero de 2011 de su página cibernética

León Lefcovich, M. (2007). *Auditoría interna: Un enfoque sistémico y de mejora continua*. Publicado el 22 de junio de 2007 y Extraído el 15 de febrero de 2011 de la página http://www.monografias.com/ trabajos14/audito-interna/audito-interna.shtml

Osiatis (2011). *RACI*. Extraído el 28 de febrero de 2011 de la página http://itilv3.osiatis. es/diseno_servicios_TI/modelo_RACI.php

Recinto Uno de la Universidad del Entorno (2008). *Políticas Institucionales.* Extraído el 28 de febrero de 2011 de su página cibernética

Recinto Dos de la Universidad del Entorno (s.f.). *Servicios de la Oficina de Sistemas de Información*. Extraído el 28 de febrero de 2011 de su página cibernética

Recinto Tres de la Universidad del Entorno (2010). *Procedimiento para la disposición de información sensitiva y programados de equipos computadorizados y almacenamiento de datos.* Centro de Tecnología de Información. Extraído el 28 de febrero de 2011 de su página cibernética

Recinto Cuatro de la Universidad del Entorno (2008). Oficina de Sistemas de Información. Extraído el 28 de febrero de 2011 de su página cibernética

Recinto Cinco de la Universidad del Entorno (2008). *Políticas de Uso de las Tecnologías.* Extraído el 28 de febrero de 2011 de su página cibernética

Recinto Seis de la Universidad del Entorno (2009). Oficina de Sistemas de Información. Extraído el 28 de febrero de 2011 de su página cibernética

Recinto Siete de la Universidad del Entorno (2008). *Política Institucional sobre el Uso Aceptable de los Recursos de la Tecnología de la Información en la Universidad del Entorno.* Extraído el 28 de febrero de 2011 de su página cibernética

Recinto Ocho de la Universidad del Entorno (2007). *Normas y Medidas de Seguridad dirigidas al Usuario.* Oficina de Sistemas de Información. Extraído el 28 de febrero de 2011 de su página cibernética

Recinto Nueve de la Universidad del Entorno (2010). *Políticas Institucionales.* Extraído el 28 de febrero de 2011 de su página cibernética

Recinto Diez de la Universidad del Entorno (2008). *Política Institucional sobre el Uso Aceptable de los Recursos de la Tecnología de la Información en la Universidad del Entorno.* Extraído el 28 de febrero de 2011 de su página cibernética

Recinto Once de la Universidad del Entorno (s.f.). *Políticas Institucionales.* Extraído el 28 de febrero de 2011 de su página cibernética

Serrano González, S. y Zapata Lluch, M. (julio-agosto 2003). Auditoría de la información, punto de partida de la gestión del conocimiento. *El profesional de la información, 12, 4,* 290-297.

Soto, L. (s.f.). *Fases Auditoría Informática*. Presentación como parte de un curso de informática. Extraído el 8 de marzo de 2011 de la página http://www.mitecnologico.com/Main/FasesAuditoriaInformatica

Universidad de Buenos Aires (s.f.). *Manual de Procedimientos de Auditoría Interna: Auditoría General Universidad de Buenos Aires*. Extraído el 28 de febrero de 2011 de la página http://www.uba.ar/download/institucional/informes/manual.pdf

Universidad del Entorno (s.f.). *Portal de la Universidad del Entorno*. Extraído el 28 de febrero de 2011 de su página cibernética