Artículo Original **Páginas:** 17 - 35 **ISSN 2071-081X/ISSN 2411-0035**

Fides Et Ratio - Vol. 11, Marzo 2016

La tecnología de la información como herramienta construccionista para el auditor financiero hibrido

The information technology as constructionist tool for financial auditor

William Espinoza Quinn[1]
Grupo financiero BISA, Bolivia
wespinoza@grupobisa.com

Resumen

El propósito de este artículo es demostrar la importancia de las habilidades y competencias con las que debe contar un licenciado en contaduría pública o auditoría (auditor) relacionadas con la tecnología de la información (TI), que a través del entendimiento de los riesgos y controles clave en TI pueda planificar, dirigir, supervisar y revisar el trabajo asignado. Así también, se cita la normativa aplicable que exige al auditor contar con conocimientos suficientes para afrontar su trabajo, en una realidad actual en la que proliferan los fraudes y delitos informáticos a escala mundial que van de la mano de los exponenciales avances tecnológicos.

Palabras Claves

Auditoría, competencias, controles, conocimiento suficiente, fraude, habilidades, normas internacionales de auditoría, riesgo, seguridad y tecnología de la información.

Abstract

The purpose of this article is to demonstrate the importance of skills and competencies that must have a certified public accountant or auditing (CPA), related to information technology (IT), which through the understanding of key IT risks and controls, plan, direct, supervise and

1 Magister en Administración y Dirección de Empresas (UPB-USACH), Especialidad en Gestión Contable y Financiera (UCV), Contador Público Autorizado (UCB), Auditor Interno Grupo Financiero BISA, Auditor Externo PWC, Ernst & Young y KPMG.

review the work assigned. Also, the applicable legislation requires the auditor to have enough knowledge to cope with the work of a global reality in which proliferate fraud and computer crimes that go hand in hand with technological advances increasing exponentially.

Key Words

Audit, competence, controls, sufficient knowledge, fraud, abilities, international standards audit, risk, security and information technology.

Introducción

La Norma Internacional de Auditoría (NIA) 401 "Auditoría de un ambiente de sistemas de información por computadora", establece que "el auditor debería tener suficiente conocimiento de los sistemas de información computarizada para planear, dirigir, supervisar y revisar el trabajo desarrollado, también establece que el auditor debería considerar si se necesitan habilidades especializadas en sistemas de información computarizado y que en caso de la necesidad de habilidades especializadas, el auditor buscaría la ayuda de un profesional con dichas habilidades, quien puede pertenecer al personal del auditor o ser un profesional externo", (IFAC, 2013, p. 2.) en este último caso optar por lo establecido por la NIA 620 "Uso del Trabajo de un Experto". (IFAC, 2005).

> Las Normas Internacionales para el Ejercicio Profesional de la Auditoría Interna (*IPPF por sus siglas en inglés*), emitidas por el Instituto Global de Auditores Internos, establecen en sus normas de implantación, aplicable a las actividades de aseguramiento, 1210.A3, la cual especifica que "los auditores internos deben tener conocimientos suficientes de los riesgos y controles clave en tecnologías de la información y de las técnicas de auditoría disponibles basadas en tecnología que le permitan desempeñar el trabajo asignado", asimismo, "la norma de implantación 1220.A2 indica que al ejercer el debido cuidado profesional el auditor interno debe considerar la utilización de auditoría basada en tecnología y otras técnicas de análisis de datos." (Instituto de Auditores Internos, Año 2013, p. 5.)

Dentro lo que establece el marco normativo citado, se puede observar que el auditor "debe" contar con "conocimientos suficientes" sobre tecnologías de la información para el desempeño de su trabajo, por lo que se plantea los siguientes dilemas: ¿Qué habilidades y competencias "debe" contar el auditor como "conocimientos suficientes" de acuerdo a la normativa que le permitan planear, dirigir, supervisar, revisar, identificar riesgos, evaluar controles claves y hacer uso de técnicas de auditoria disponibles basadas en tecnología en los sistemas de información tecnológica?

Por lo que es necesario aclarar que se entiende por "conocimiento suficiente", las temáticas que debe considerar el auditor dentro de sus habilidades y competencias.

Objetivos

Los principales objetivos a los que se pretende llegar son:

- Resaltar lo establecido por las normas internacionales de auditoria sobre la exigencia de que el auditor debe contar con conocimientos suficientes.
- Aclarar la importancia de contar con habilidades y competencias sobre tecnología de la información para cualquier tipo de auditoría.
- Identificar las temáticas en TI que el auditor debe tomar en cuenta para mejorar sus habilidades y competencias.
- Impulsar al auditor a obtener conocimientos sobre tecnología para desempeñarse como un auditor competitivo.
- Analizar si las mallas curriculares para la carrera de contaduría pública o auditoría, contienen asignaturas relacionadas a tecnologías sobre la información y si estos son suficientes.

Marco conceptual

- **Enfoques de auditoría "tradicional" y "basado en riesgos"**

Hasta hace unos 20 años el enfoque de la auditoría, sea en el sector público y/o privado, era netamente un enfoque tradicional, es decir, mayor cantidad de auditores y de horas de trabajo, costos altos (solo alcanzable para

grandes empresas), sin exigencia legal ni profesional, grandes volúmenes de papeles de trabajo (físicos hechos manualmente), en ese entonces apenas se tenía conocimiento de las hojas electrónicas. Por otro lado, las empresas iban automatizando poco a poco sus sistemas de información, que en esas épocas eran bastante lentas, costosas, complejas y burocráticas, por lo que su implementación no fue rápida.

A medida que los negocios iban evolucionando, el volumen de información y de las transacciones se incrementaban, por lo que las organizaciones tuvieron la necesidad de recurrir a la automatización de sus sistemas de información, por ejemplo, tuvieron que automatizar los registros contables y varios procesos operativos, los cuales tenían que ser soportados por activos de tecnología como servidores, redes, software y hardware especializado. Pero así como la tecnología ha ido evolucionando, los fraudes y delitos informáticos han ido a la par, a tal punto que en la actualidad un delincuente informático puede sustraer recursos económicos de una organización desde la comodidad de su hogar, sin dejar rastro alguno, o estructurar grandes delitos desde el interior de la organización.

Esta situación sumados a los grandes desfalcos financieros ocurridos a nivel mundial, incluyendo delitos informáticos, han obligado al auditor un cambio de enfoque y la necesidad de que el auditor cuente con nuevas habilidades y conocimientos, sobre todo el área de tecnología. Algunos de los hechos fraudulentos más importantes ocurridos en los últimos años se citan e n la siguiente sección

- **Fraudes y delitos informáticos**

Entre los hechos fraudulentos ocurridos durante el último siglo, se han suscitado casos a nivel mundial que inclusive involucran a grandes firmas internacionales de auditoría, como los casos de la distribuidora de energía Enron (2001), el laboratorio Merck (2002), la telefónica Worldcom (2002), empresa de retail La Polar (2010) y en Bolivia el caso de la inmobiliaria Finsa (1991), financiera Roghel (2008), farmacéutica LV Pharma (2008), entre muchos otros. A estos hechos, el riesgo para el auditor es aún mucho mayor con la evolución de la tecnología en las empresas, Según Ramón J. Pérez, (2015) han surgido nuevos tipos de delitos:

- Estafa.
- Delito contra la intimidad de menores y acoso.
- Descubrimiento y revelación de secretos.
- Amenazas y coacciones.
- Falsificación documental.
- Daños y sabotaje informático.
- Suplantación de identidad.
- Incumplimiento de contrato
- Delitos contra la propiedad intelectual
- Descargas ilegales

Entonces el nuevo enfoque de auditoría se la denomina "auditoría basada en riesgos", el cual pretende enfocar y centrar los esfuerzos en aquello que es realmente importante y que sean un riesgo para la organización en el logro de sus objetivos. Este enfoque de auditoría se caracteriza principalmente por ser un enfoque "de arriba hacia abajo", lo cual repercute en una menor cantidad de auditores, realizar evaluaciones de negocio y riesgo, mayor énfasis en criterio profesional, diseñar y ejecutar auditorías a medida y el uso de las técnicas de auditoría con ayuda del computador (TAAC). Por lo cual, el auditor debe ser capaz de analizar y evaluar cualquier tipo de riesgo.

- **Nuevas tendencias en tecnología 2016**

Según Nahum Frett (2016), hoy en día, van apareciendo una serie de riesgos productos de las nuevas tendencias en tecnología, como ser:

- Social Commerce.
- Internet de las cosas.
- Drones/Robótica.
- Big Data.
- Nube.
- Vehículos autónomos/conectados.
- Ciberseguridad.
- Impresión 3D.
- Pago Móvil.
- Publicidad en Medios Sociales.

El enfoque basado en riesgos aplicado por el auditor debe ser capaz de identificar y analizar estos riesgos.

- **Problemas a los que se enfrenta el auditor**

Al desempeñar su trabajo, el auditor se encuentra con diferentes sistemas de administración de la información implementados las organizaciones, sobre todo automatizados, como los registros contables, sistemas de personal, gestión de inventarios, transferencias bancarias electrónicas, registros biométricos, y la aparición de activos de tecnología que soportan estos sistemas como ser los servidores, redes, centrales de comunicación, son solo algunos ejemplos. El auditor debe llegar a comprender su funcionamiento y no solo confiar "ciegamente" en los datos que arroja el "sistema" y enfocar su revisión solo en documentación física, ya que los riesgos podrían estar en el procesamiento "caja negra" de dicha información, caso contrario el auditor se enfrentaría a los siguientes problemas:

- Limitaciones en el diseño de pruebas de auditoría.
- Aumenta el riesgo de auditoria al no contar con un buen entendimiento del riesgo tecnológico.
- Enfoque de confianza en controles no sería posible al existir controles de tecnología de la información que no fueron probados.
- Imposibilidad de evaluar las bases de datos, redes, seguridad de la información y física.
- Mayor cantidad de horas para la ejecución de pruebas sustantivas (al no confiar en controles)
- Mayor presupuesto para la contratación de un especialista en ingeniería de sistemas.
- Descoordinación de objetivos de la auditoría entre el encargado de auditoría y el especialista (ingeniero de sistemas).
- El desconocimiento del uso TAACs, conlleva a que se insuman más horas en la revisión.
- Depender del muestreo de auditoría, siendo que con las herramientas se podría revisar la totalidad de la información.

En el caso de las unidades de auditoría interna con pocos recursos, se pueden citar los siguientes inconvenientes adicionales a los anteriores:

- Se cuenta con uno o dos auditores, la contratación de un auditor especializado significa un presupuesto adicional a la unidad.
- El auditor se ve en la necesidad de capacitarse, sin embargo no existen cursos disponibles en el mercado al nivel requerido.
- Afrontar una auditoria de sistemas, con el propósito de cumplir el Plan Anual de la Unidad de Auditoría Interna, conlleva a que se incurran en mayor cantidad de horas y que la auditoría sea muy superficial.

Los auditores externos que trabajan en firmas de auditoría, tienen los siguientes problemas:

- Dependencia del especialista.
- Descoordinación de objetivos entre el Gerente o Encargado de Auditoría con el especialista, ya que el especialista de formación es ingeniero de sistemas.
- Uso eficiente del trabajo del especialista (el especialista no tendría que estar haciendo trabajo que puede hacerlo otro auditor). Ejemplo: Cálculos manuales en Excel.
- Deficiente uso del enfoque de controles para la realización de pruebas sobre controles.

- **Entonces: ¿Qué conocimientos suficientes debe tener el auditor?**

Es necesario analizar cuáles serían los "conocimientos suficientes" debe tener el auditor de los riesgos, controles, técnicas de auditoría disponibles basadas en tecnología, y otras técnicas de análisis de datos, que le permitan al auditor, cuya responsabilidad fundamental no son las tecnologías de la información, desempeñar eficientemente el trabajo.

En línea a lo que el enfoque basado en riesgos establece, la revisión se enfoca en la evaluación de los procesos del negocio que es un conjunto de actividades interrelacionadas, transformando las entradas en salidas con ayuda de los recursos empleados (tal como personas, computadoras y aplicaciones) o intangibles (por ejemplo habilidades y experiencia). Así también, la existencia de controles de tecnología implementados en el

proceso como los generales de TI y los de aplicación. A continuación el esquema de un proceso:

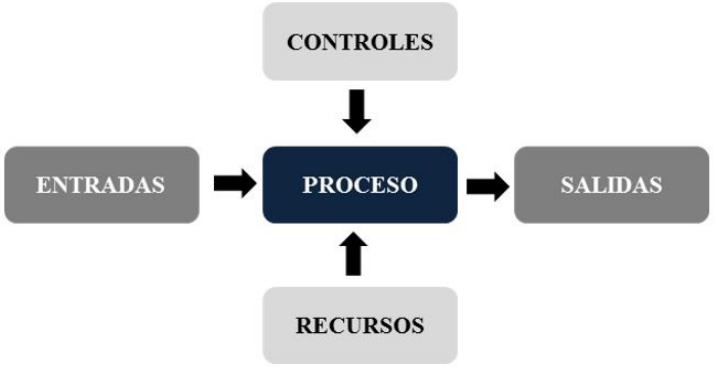

GRÁFICO 1. Esquema de un proceso de negocio
(Jorge Salazar Heredia (2016) Aptitudes del auditor interno respecto a las tecnologías de la información. www.auditool.org

Los controles generales son responsabilidad del departamento de TI, mientras que los controles de aplicación además de ser responsabilidad del departamento de TI son responsabilidad del negocio, ya que reflejan los controles del negocio y se basan en los requerimientos funcionales y de control atendidos por medio de servicios automatizados.

El siguiente gráfico muestra una descripción de estos dos tipos de controles según Arens, Elder y Beasley (2007) siendo que las áreas de aplicaciones y bases de datos, se encuentran en una posición de responsabilidad compartida entre el proceso del negocio y el departamento de Tecnología de Información: (p. 349)

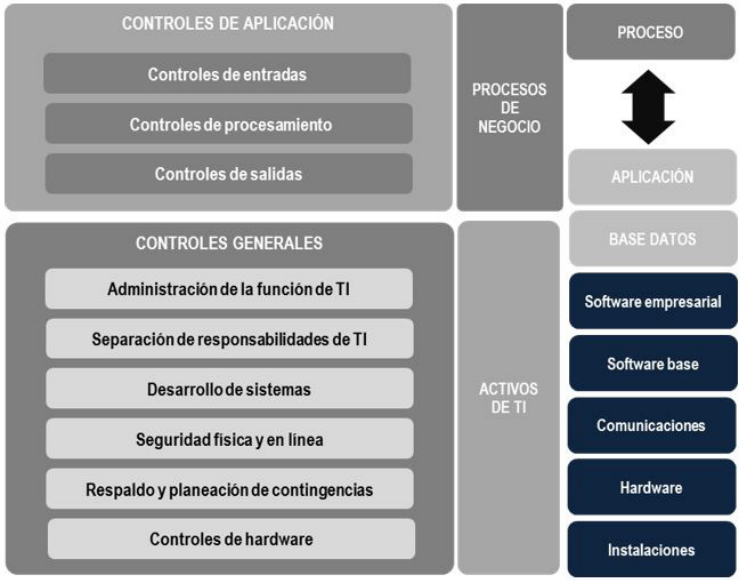

GRAFICO 2. Controles de tecnología y su relación con los procesos del negocio y el departamento de TI
(Fuente propia)

Por lo tanto, el auditor debe tener conocimiento de los controles de aplicación a un nivel de procesos de negocio (al nivel de usuario de la aplicación) y analizar la información contenida en las bases de datos, con la ayuda de herramientas que permitan el análisis de grandes volúmenes de información como Excel, Audito Command Language (ACL) o IDEA. Los controles generales, conforme a su complejidad, deben ser auditados por un auditor especialista, sin embargo esto no quiere decir que el auditor no cuente con estos conocimientos, ya que el auditor debe llegar también a comprender este tipo de controles.

- **Habilidades y competencias requeridas por el auditor**

De acuerdo a la guía de estudio Gleim (2014), considera aquello que se refiere a "conocimientos suficientes", se han identificado las siguientes áreas que el auditor debe considerar conocer:

GRAFICO 3. Habilidades y competencias requeridas por el auditor
(Fuente propia)

Estas áreas implican conocer las siguientes temáticas:

- **Seguridad de TI.**

  - Seguridad física y seguridad de sistemas
  - Protección de la información
  - Autenticación y encriptación

- **Desarrollo de aplicaciones.**

  - Informática de usuario final
  - Control sobre los cambios de programa
  - Metodología de desarrollo de sistemas
  - Desarrollo de aplicaciones
  - Desarrollo de sistemas de información

- **Infraestructura del sistema**

  - Estaciones de trabajo
  - Bases de datos
  - Marcos de control de TI (eSAC, COBIT)
  - Áreas funcionales de operaciones de TI (operaciones de centro

de datos)
- Software de planificación de recursos empresariales (ERP) (SAP R/3)
- Datos, voz, y comunicaciones/conexiones de red (LAN, VAN, y WAN)
- Servidor
- Licencias de software
- Ordenador central
- Sistemas operativos
- Infraestructura de la Web

-Continuidad del negocio

- Planeación de contingencias de TI

Materiales y métodos

Para el análisis de las instituciones educativas en Bolivia, que enseñan materias del área de tecnología de la información, se ha utilizado el método basado en un análisis empírico Tamayo y Tamayo (1997), a una muestra representativa de los centros educativos públicos y privados de la enseñanza de la Auditoría, utilizando un cuestionario dirigido a directivos y búsqueda en las páginas web de estas instituciones. El análisis de los datos en la metodología de la investigación utilizada, ha sido un proceso de revisión de las encuestas y por lo tanto su registro en el presente trabajo de investigación.

Resultados

Formación profesional Instituciones de Educación Superior

Se debe inicialmente analizar cuál es la proporción de universidades públicas y privadas que cuentan dentro de sus ofertas académicas, la carrera de contaduría pública o auditoría, así mismo cuantas universidades cuentan con programas de formación complementaria a contadores generales para la obtención de dicha licenciatura, así podemos ver:

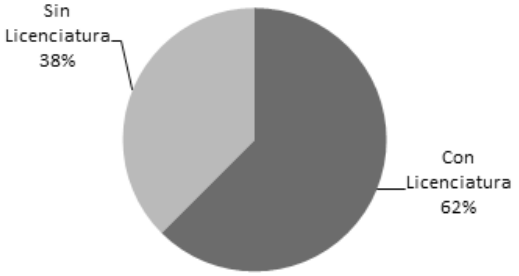

GRÁFICO 4. Universidades Públicas que cuentan con Licenciaturas en Contaduría Pública o Auditoría
(Fuente propia)

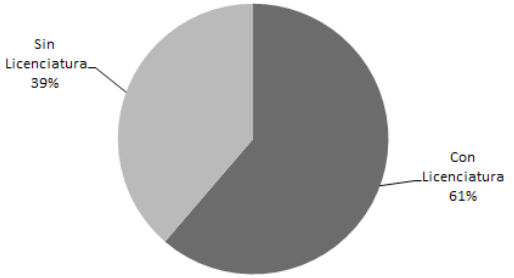

GRÁFICO 5. Universidades Privadas que cuentan con Licenciaturas en Contaduría Pública o Auditoría
(Fuente propia)

Se puede observar que el 62% (16 Instituciones) de las Universidades Públicas y el 61% (19 Instituciones) de las Universidades Privadas, tienen en sus ofertas académicas, la carrera de Licenciatura en Contaduría Pública o Auditoría, y solamente 3 Instituciones de las Universidades Privadas cuentan con un programa complementario de formación para los contadores generales. De estas universidades se han encuestado en la siguiente proporción:

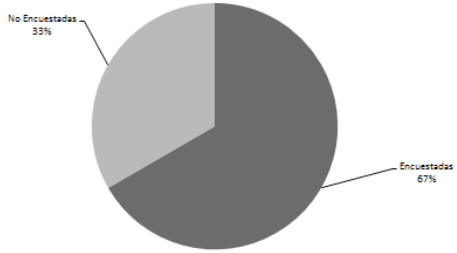

GRÁFICO 6. Universidades Públicas encuestadas
(Fuente: Propia)

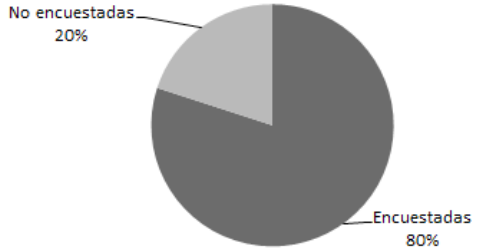

GRÁFICO 7. Universidades Privadas encuestadas
(Fuente: Propia)

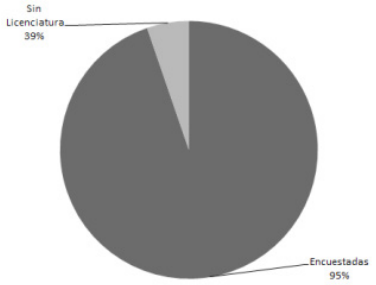

GRÁFICO 8. Universidades Privadas
(Fuente: Propia)

En este sentido, para que el auditor logre las habilidades y competencias requeridas, se debe comenzar desde la formación a nivel de pregrado. Del análisis del contenido curricular de cada una de los planes de estudio, respecto a las materias relacionadas con la tecnología de la información se pueden observar los siguientes resultados:

Tabla 1: Detalle de Universidades Públicas, Privadas y de Formación Complementaria para Contadores Generales para la licenciatura en Contaduría Pública (Fuente Propia)

UNIVERSIDADES PRIVADAS	
Universidad Católica Boliviana "San Pablo"	
8º Sem	Auditoría de ambientes computarizados
Universidad "La Salle"	
8º Sem	Auditoria de sistemas
Universidad Central	
1º Sem	Computación I
2º Sem	Computación II
4º Sem	Sistemas administrativos
8º Sem	Sistemas de información
Universidad Tecnologíca Boliviana UTB	
8º Sem	Sistemas de información gerencial
9º Sem	Diseño de sistemas contables y organizacionales
Universidad Franz Tamayo	
1º Sem	Informática I
2º Sem	Informática II
8º Sem	Auditoría de Sistemas Administrativos
9º Sem	Diseño de sistemas contables
Universidad Evangélica Boliviana	
1º Sem	Técnicas de estudio y computación
2º Sem	Informática y comunicación
7º Sem	Auditoría de sistemas
Universidad Privada Cumbre	
1º Sem	Informática empresarial
6º Sem	Taller de informática contable

Universidad Union Bolivariana	
6º Sem	Teoría de la computación
7º Sem	Diseño de sistemas contables
9º Sem	Gabinete de auditoría de sistemas
Universidad “Loyola”	
8º Sem	Auditoría de sistemas
Universidad Salesiana de Bolivia	
3º Sem	Informática
4º Sem	Base de datos I
7º Sem	Base de datos II
10º sem	Auditoría de sistemas
Universidad Provada de Santa Cruz	
5º Sem	Diseño e informatica contable
5º Sem	Informática empresarial
Universidad Tecnológica Privada de Santa Cruz	
4º Sem	Introducción a la informática
5º Sem	Informática aplicada
Universidad Provada de Oruro	
3º Sem	Infirmática I
4º Sem	Infirmática II
7º Sem	Infirmática contable
9º Sem	Auditoría de sistemas
Universidad Cristiana de Bolivia	
2º Sem	Infirmática
3º Sem	Infirmática aplicada
9º Sem	Auditoría de sistemas
Universidad de Aquino Bolivia	
1º Sem	Computación I

Universidad Adventistas de Bolivia	
3º Sem	Computación aplicada
6º Sem	Computación empresarial
Universidad Bolivia de Informática	
9º Sem	Auditoría de sistemas
Universidad "NUR"	
9º Sem	Auditoría de sistemas
UNIVERSIDADES PÚBLICAS	
Ununversidad Mayor de San Andrés	
2º Año	Diseño de sistemas contables
2º Año	Teoría computacional
Universidad Mayor de San Simón	
2º Sem	Sistemas administrativos
4º Sem	Informática I
5º Sem	Informática II
Universidad San Francisco Xavier	
5º Sem	Informática contable
8º Sem	Gabinete auditoría de sistemas
Universidad Autónoma "Tomas Frías"	
4º Sem	Análisis de Sistemas
5º Sem	Base de datos
9º Sem	Auditoría de sistemas
Universidad Autónoma Gabriel René Moreno	
2º Sem	Infirmática aplicada I
3º Sem	Infirmática aplicada II
7º Sem	Sistemas de información
9º Sem	Auditoría y control de sistemas de información

Universidad Autónoma Juan Misael Saracho	
2º Sem	Informática general
4º Sem	Diseño de sistemas contables
8º Sem	Auditoría de sistemas
Universidad Tecnica de Oruro	
2º Sem	Computación
6º Sem	Sistemas computarizados contables
7º Sem	Diseño de sistemas contables
9º Sem	Auditoria de sistemas
Universida Nacional siglo XX	
2º Año	Computación
3º Año	Sistemas computarizados contables
4º Año	Diseño de sistemas contables
5º Año	Auditoría de Sistemas
FORMACIÓN COMPLEMETARIA	
Universidad La Salle - PACC	
3º Sem	Auditoría de Sistemas
Universidad Central - Formación Complementaria	
3º Sem	Sistemas de información

Conclusiones

Actualmente una de las grandes debilidades, por no decir que es la mayor de todas, de los auditores que no tienen formación en ingeniería de sistemas y que seguramente de muchas otras profesiones que realizan las labores de fiscalización control y supervisión, es la carencia de entendimiento de las tecnologías de la información dentro de las organizaciones a un nivel de controles y riesgos de TI.

Las normas internacionales de auditoría establecen que el auditor debe contar con conocimientos suficientes, dentro lo que comprende el enfoque moderno de auditoria basada en riesgos, estos conocimientos se refieren principalmente a que el auditor debe contar con habilidades y competencias para el examen de los controles de aplicación que están directamente relacionados a los procesos del negocio, pero también llegar a comprender los controles generales de TI, ya que a través de la comprensión e identificación de los probables riesgos y de los controles clave en TI pueda planificar, dirigir, supervisar y revisar el trabajo.

Ante diversos fraudes de toda índole ocurridos a través del uso de la tecnología cada vez más sofisticada, se ha convertido en un gran reto para el auditor en el campo el cual se desempeña, exigiéndole a contar con mayores habilidades y competencias en este campo, para dar un valor agregado a las organizaciones inclusive en tiempo real y minimizando el riesgo de auditoría. Para lo cual se ha explicado a detalle los conocimientos mínimos y necesarios para afrontar este reto, así como analizar si la las instituciones de pregrado están formando adecuadamente a los auditores del siglo XXI.

Referencias

- Arens, Elder y Beasley (2007). Auditoría un Enfoque Integral. México: Prentice Hall.
- Gleim (2014). Curso preparación examen CIA (Certified Internal Auditor) Parte III. Estados Unidos:Gleim Publications.
- Instituto de Auditores Internos Global (2013). Marco para la Práctica Profesional de la Auditoría Interna. Estados Unidos: Bookstore IIA.
- International Federation of Accountants (IFAC). (2013). Normas Internacionales de Auditoría. Estados Unidos: Bookstore IFAC.
- Norma Internacional de Auditoría 620 “Uso del trabajo de un experto”. Junio 2005. Recuperado de www.auditories.org.bo/normativas/normas...auditorial/30_NIA_620
- Nahum Frett. (2016). Las nuevas 10 tendencias tecnológicas. Recuperado de: http://nahunfrett.blogspot.com/2016/01/10-tendencias-tecnologicas-seguir-en.

html?utm_source=feedburner&utm_medium=email&utm_campaign=Feed%3A+NahunFrett+%28Nahun+Frett%29. [10-01-2016].

- Ramón J. Pérez. (2015). Los 10 delitos informáticos más frecuentes. Recuperado de http://pro.giztab.com/2015/10/20/los-10-delitos-informaticos-mas-frecuentes/
- Salazar Heredia, J. (2016) Aptitudes del auditor interno respecto a las tecnologías de la información. Recuperado de: www.auditool.org.Tamayo y Tamayo, M. (1997). El proceso de la Investigación científica. México: Limusa.

Artículo recibido: 22-01-2016

Artículo aceptado: 29-02-2016