La necesidad de aplicar la auditoría preventiva en el Perú

Ampelio Ricardo Barrón Araoz
Juan Augusto Ferreyros Morón

Ensayo

RESUMEN

El objetivo principal de este artículo, fue priorizar toda actividad auditora que debe contener como enfoque central el tema de prevención de riesgos TIC (Tecnología de Información y Comunicaciones), que tenga como apoyo técnico el manejo de su información mediante computadoras, cualquiera sea su entorno organizacional. Al igual que un médico dirige el control preventivo en su paciente, que pueda inducirlo hacia la cura de su enfermedad. En nuestro caso, es fundamental el tema de comunicación constante con políticas organizacionales internas, con el fin de tener advertido al personal y utilizar la misma tecnología como aspecto de advertencia y lograr el compromiso de apoyo a la institución. En el proceso profesional de auditoría, muchas veces, la dirección de las empresas la solicita cuando ya se produjo el robo, el fraude o el sabotaje; es decir, post-acción. Hoy, en estos casos, es fundamental apoyarse en la propia tecnología para identificar, prevenir y accionar inmediatamente ante estos hechos delictivos, mediante un específico y profesional plan de auditoría de sistemas, que incluya técnicas de recojo de información de la situación actual, la identificación de puntos críticos o riesgos, tanto de procesos como de las actividades de cada proceso en riesgo a fin de identificar con exactitud el punto de quiebre que origina el problema, con análisis de sus causas, creando precedentes y evidencias que puedan sustentar informes técnicos de auditoria al/por computador. Así mismo, desarrollar un específico Plan de Continuidad priorizando la seguridad de la información, almacenada y gestionada en hardware y software, como en la data que manejan los propios usuarios. En este punto se toma como modelo el ISO17799, específicamente sobre la auditoría de sistemas.

Palabras clave: Prevención, auditoria de sistemas-TIC, Plan de Continuidad.

Abstract

The main objective of this article is to prioritize all auditing activity that should include as central focus the topic of ICT risk prevention (Information and Communication Technology), which has as technical support the management of its information through computers, whatever their organizational environment. Just as a physician directs the preventive control in his patient, which can induce him to cure his disease (not post-action). In our case, the issue of constant communication - with internal

organizational policies - is fundamental in order to warn staff and use the same technology as a deterrent, warning and achieve a commitment to support the institution. In the professional audit process, management often requests an audit when theft, fraud or sabotage has already occurred; that is, post-action. Today, in these cases, it is essential to rely on the technology itself to identify, prevent and immediately act on these criminal acts, through a specific and professional system audit plan, which includes techniques for collecting information on the current situation, identification Of critical points or risks, both of processes and of the activities of each process at risk in order to accurately identify the break point that originates the problem, analyzing its causes, creating precedents and evidences that can support technical audit reports To / by computer. Likewise, to develop a specific Continuity Plan prioritizing the security of information, stored and managed in hardware and software, as in the data that the users themselves. At this point, ISO17799 is taken as a model, specifically on systems auditing.

Key words: Prevention, audit of ICT systems, Continuity Plan.

Introducción

Esta investigación tiene como finalidad, direccionar a las TIC´s como una actual demanda dentro de un enfoque globalizado y cómo el auditor puede y debe capacitarse para un buen uso de las técnicas de prevención. De muy poco servirá a la organización contar con sofisticados y onerosos equipos TIC, cuando no hay forma de prevenir con técnicas conexas previas y concurrentes las formas de racionalizar y ordenar los procesos con el fin de ser menos dependientes de las propias computadoras. Las burocracias actuales, la excesiva tramitología y abundante papeleo (“desorden organizado”), hacen propicio el escenario de estos temas anti-éticos y -por consiguiente- la corrupción crece en forma exponencial, como ya se observa, incluso en las altas esferas políticas, aceptándose esto como una forma “ya natural” del actuar cotidiano en nuestro medio.

En consecuencia, el concepto que involucra la prevención se constituye en un excelente e ineludible factor de adelantarnos a hechos delincuenciales, que luego será difícil de detectar o restituir.

Finalmente, sí los robos o fraudes utilizando computadoras se han ejecutado en países desarrollados, supuestamente con todos los controles, como los mundialmente conocidos casos de Enron en Estados Unidos, Toshiba en Japón, “hackers” en el Capitolio, entre otros tantos que aún no han sido descubiertos y todos ellos con apoyo de expertos, de famosas sociedades de auditoría e incluso con el de poderosos personajes de los gobiernos perjudicados, ¿por qué no podrían estar ocurriendo ya en nuestros pobres países dónde los anti-valores se publican a diario?

“En líneas generales podríamos decir que las nuevas tecnologías de la información y comunicación son las que giran en torno a tres medios básicos: la informática, la microelectrónica y las telecomunicaciones; pero giran, no sólo de forma aislada, sino lo que es más significativo de manera interactiva e inter-conexionadas, lo que permite conseguir nuevas realidades comunicativas”. (Cabero, 1998: 198).

Las características que diferentes autores especifican como representativas de las TIC, recogidas por Cabero (1998), son:

Inmaterialidad
En líneas generales podemos decir que las TIC realizan la creación (aunque en algunos casos sin referentes reales, como pueden ser las simulaciones), el proceso y la comunicación TIC. Esta información es básicamente inmaterial y puede ser llevada de forma transparente e instantánea a lugares lejanos.

Interactividad
La interactividad es posiblemente la característica más importante de las TIC para su aplicación en el campo empresarial. Mediante las TIC se consigue un intercambio de información entre el usuario y el ordenador. Esta característica permite adaptar los recursos utilizados a las necesidades y características de los sujetos, en función de la interacción concreta del sujeto con el ordenador.

Interconexión
La interconexión hace referencia a la creación de nuevas posibilidades tecnológicas a partir de la conexión entre dos tecnologías. Por ejemplo, la telemática es la interconexión entre la informática y las tecnologías de comunicación, propiciando con ello, nuevos recursos como el correo electrónico, entre otros.

Instantaneidad
Las redes de comunicación y su integración con la informática, han posibilitado el uso de servicios que permiten la comunicación y transmisión de la información, entre lugares alejados físicamente, de una forma rápida.

Elevados parámetros de calidad de imagen y sonido
El proceso y transmisión de la información abarca todo tipo de información: textual, imagen y sonido, por lo que los avances han ido encaminados a conseguir transmisiones multimedia de gran calidad, lo cual ha sido facilitado por el proceso de digitalización.

Innovación
Las TIC están produciendo una innovación y cambio constante en todos los ámbitos sociales. Sin embargo, es de reseñar que estos cambios no siempre indican un rechazo a las tecnologías o medios anteriores; sino que en algunos casos se produce una especie de simbiosis con otros medios. Por ejemplo, el uso de la correspondencia personal se había reducido ampliamente con la aparición del teléfono, pero el uso y potencialidades del correo electrónico han logrado un resurgimiento de la correspondencia personal.

Tendencia hacia automatización
La propia complejidad empuja a la aparición de diferentes posibilidades y herramientas que permiten un manejo automático de la información en diversas actividades personales, profesionales y sociales. La necesidad de disponer de información estructurada hace que se desarrollen gestores personales o corporativos con distintos fines y de acuerdo con unos determinados principios.

Diversidad
La utilidad de las tecnologías puede ser muy diversa, desde la mera comunicación entre personas, hasta el proceso de la información para crear informaciones nuevas.
El objetivo principal de este trabajo de investigación, es determinar que la práctica de Auditoria preventiva a la empresa y al sector público disminuya la corrupción. Con aplicación de Auditoria preventiva se logrará la corrección de fraudes; asimismo la prevención de riesgos laborales disminuirá con la aplicación de este instrumento de control.

Seguridad de la información

La información es un activo que, como otros activos comerciales importantes, es esencial para el negocio de una organización y en consecuencia, necesita ser **protegido** adecuadamente. Esto es especialmente importante en el ambiente comercial cada vez más interconectado. Como resultado de esta creciente interconectividad, la información –ahora- está expuesta a un número cada vez mayor y una variedad más amplia de amenazas que propician la corrupción que hoy observamos –prácticamente- a todo nivel.

La información puede existir en muchas formas. Puede estar impresa o escrita en un papel, almacenada electrónicamente, transmitida por correo o utilizando medios electrónicos, mostrada en películas o hablada en una conversación. Cualquiera que sea la forma que tome la información, o medio por el cual sea almacenada o compartida, siempre debiera estar apropiadamente protegida.

La seguridad de la información es la protección de la información de un rango amplio de amenazas para poder asegurar la continuidad del negocio, minimizar el riesgo comercial y maximizar el retorno de las inversiones y las oportunidades comerciales.

La seguridad de la información se logra implementando un adecuado conjunto de controles; incluyendo políticas, procesos, procedimientos, estructuras organizacionales y funciones de software y hardware.

Se necesita establecer, implementar, monitorear, revisar y mejorar estos controles cuando sea necesario para asegurar que se cumplan los objetivos de seguridad y comerciales específicos. Esto se debiera realizar en equipo conjunto con otros procesos de gestión del negocio.

La información y los procesos, sistemas y redes de apoyo son activos comerciales importantes. Definir, lograr, mantener y mejorar la seguridad de la información puede ser esencial para mantener una ventaja competitiva, el flujo de caja, rentabilidad, observancia contable, legal, imagen comercial y controles con énfasis disuasivos.
Las organizaciones, sus sistemas y redes de información enfrentan amenazas de seguridad de un amplio rango de fuentes; incluyendo fraude por computadora, espionaje, sabotaje, vandalismo, fuego o inundación. Las causas de daño como

código malicioso, pirateo computarizado o negación de ataques de servicio se hacen cada vez más comunes, más ambiciosas y cada vez más sofisticadas.

La seguridad de la información es importante tanto para negocios del sector público como privado, y para proteger las infraestructuras críticas. La interconexión de redes públicas y privadas y el intercambio de fuentes de información incrementan la dificultad de lograr un control del acceso. La tendencia a la computación distribuida también ha debilitado la efectividad de un control central y especializado.

Muchos sistemas de información no han sido diseñados para ser seguros. La seguridad que se puede lograr a través de medios técnicos es limitada y debiera ser apoyada por la gestión y los procedimientos adecuados. Identificar qué controles establecer requiere de una planeación cuidadosa y prestar atención a los detalles.

La gestión de la seguridad de la información requiere, como mínimo, la participación de los accionistas, proveedores, terceros, clientes u otros grupos externos. También se puede requerir asesoría especializada de organizaciones externas.

Seguridad de la Información.- I.S.O. 17799 durante un examen de Auditoría de Sistemas –TIC

ISO (la Organización Internacional de Estandarización) e IEC (la Comisión Electrotécnica Internacional) forman el sistema especializado para la estandarización mundial. Los organismos internacionales miembros de ISO e IEC participan en el desarrollo de Estándares Internacionales a través de los comités establecidos por la organización respectiva para lidiar con áreas particulares de la actividad técnica.

ISO 17799 es una norma internacional que ofrece recomendaciones para realizar la gestión de la seguridad de la información dirigidas a los responsables de iniciar, implantar o mantener la seguridad de una organización.
ISO 17799 define la información como un activo que posee valor para la organización y requiere por tanto de una protección adecuada. El objetivo de la seguridad de la información es proteger adecuadamente este activo para asegurar la continuidad del negocio, minimizar los daños a la organización y maximizar el retorno de las inversiones y las oportunidades de negocio.
El ISO 17799 da la pauta en la definición sobre cuáles metodologías, políticas o criterios técnicos pueden ser aplicados en el régimen de manejo de la seguridad de la información.
El ISO 17799 favorece a la toma de decisiones sobre un marco de referencia de seguridad basado en ella proporciona beneficios a toda organización que lo implemente. Ya sea en su totalidad o en la parcialidad de sus postulaciones estipuladas.
Su elaboración y práctica integra mecanismos de control primordiales, que le permiten a las organizaciones demostrar que cuenta con el estado de la seguridad de la información pertinente; situación que resulta muy importante en aquellos

convenios o contratos con terceros que establecen como requisito contractual: la Declaración BS7799 u otras disposiciones de perfil similar que se acentúan mucho estos tiempos.

La ISO (*Internacional Organization for Standarization)* es una federación a nivel mundial de grupos nacionales de estándares de más de 100 países. La misión de la ISO es promover el desarrollo de la estandarización y actividades relacionadas con el propósito de facilitar el intercambio internacional de bienes y servicios mediante acuerdos internacionales y son publicados como Estándares Internacionales.

La sigla "ISO" es un juego de letras provenientes del griego "ISOS" cuya raíz del prefijo es "ISO-", que significa "igual", ya que las verdaderas siglas deberían ser "IOS", sin embargo, se utiliza "ISO" ya que es término apropiado para el objetivo de la normalización que persigue la organización y contiene las mismas iniciales de *"International Organization for Standarization".*

El objetivo de la norma ISO 17799 es proporcionar una base común para desarrollar normas de seguridad dentro de las organizaciones, un método de gestión eficaz de la seguridad y para establecer transacciones y relaciones, que se constituyen en pautas del pensamiento **preventivo** como eje central de la auditoría de sistemas.

La información y sus riesgos de seguridad

Los requerimientos de seguridad se identifican mediante una evaluación metódica de los riesgos de seguridad. El gasto en controles debiera ser equilibrado con el daño comercial probable resultado de fallas en la seguridad.
Los resultados de la evaluación del riesgo ayudarán a guiar y determinar la acción de gestión apropiada y las prioridades para manejar los riesgos de seguridad de la información, e implementar los controles seleccionados para protegerse contra dichos riesgos. La evaluación del riesgo se debiera repetir periódicamente para tratar cualquier cambio que podría influir en los resultados de la evaluación del riesgo.

Una vez que se han identificado los requerimientos y los riesgos de seguridad y se han tomado las decisiones para el tratamiento de los riesgos, se debieran seleccionar los controles apropiados y se debieran implementar para asegurar que los riesgos se reduzcan a un nivel aceptable. Los controles se pueden seleccionar a partir de este estándar o de otros conjuntos de controles, o se pueden diseñar controles nuevos para cumplir con necesidades específicas conforme sea apropiado.
La selección de los controles de seguridad depende de las decisiones organizacionales basadas en el criterio de aceptación del riesgo, opciones de tratamiento del riesgo y el enfoque general para la gestión del riesgo aplicado a la organización, y también debieran estar sujetas a todas las regulaciones y legislación nacionales e internacionales relevantes.

Se puede considerar un número de controles como un buen punto de inicio para la implementación de la seguridad de la información. Estos se basan en requerimientos legislativos esenciales o pueden ser considerados como una práctica común para la seguridad de la información.

Políticas de seguridad de la información

La política de la seguridad de la información debiera tener un dueño que tenga la responsabilidad gerencial aprobada para el desarrollo, revisión y evaluación de la política de seguridad. La revisión debiera incluir las oportunidades de evaluación para el mejoramiento de la política de seguridad de la información de la organización y el enfoque para manejar la seguridad de la información en respuesta a los cambios del ambiente organizacional, circunstancias comerciales, condiciones legales o ambiente técnico.

La revisión de la política de seguridad de la información debiera tomar en cuenta los resultados de las revisiones de la gerencia. Debieran existir procedimientos de revisión gerencial, equipo de trabajo, incluyendo un cronograma o el período de la revisión.

Problema

La Auditoría Financiera, se centra en la auditoría de Estados Financieros históricos, cuando el responsable de la gestión de un organismo privado o del sector público principalmente ya no está en el cargo; y al practicar la auditoría encuentran hallazgos importantes que compromete seriamente por mal uso de los recursos privados o de gobierno e incluso al llegar a manos de Poder Judicial, con pena privativa de libertad por muchos años, con lo cual absolutamente no se ha recuperado el recurso monetario mal usado. Con el propósito de prevenir y custodiar esos magros resultados en perjuicio económico de la empresa u organismo público, se plantea en este trabajo de investigación, adelantarnos con la política de control adecuado, mediante la aplicación de una auditoría preventiva.

La Auditoría Preventiva es un instrumento de gestión que persigue reflejar la imagen fiel del sistema de prevención de Riesgos Laborales de la empresa u organismo público, valorando su eficacia y detectando las deficiencias que puedan dar lugar a incumplimientos de la normativa vigente para permitir la adopción de decisiones dirigidas a su perfeccionamiento y mejora.

La prevención de riesgos laborales, como actuación a desarrollar en el seno de la empresa u organismo público, deberá integrase en el conjunto de sus actividades y decisiones, tanto en los procesos técnicos, en la organización del trabajo y en las condiciones que preste, como en la jerarquía de la organización, incluidos todos los niveles de la misma.

Auditoría Forense.- Es una técnica que tiene por objeto participar en la investigación de fraudes en actos conscientes y voluntarios en los cuales se eluden las normas legales.

Auditoría Forense Preventiva.- Está orientada a proporcionar evaluaciones o asesoramiento a diferentes organizaciones de características públicas y privadas respecto de su capacidad para disuadir, prevenir, detectar y proceder frente a diferentes acciones de fraude.

La auditoría financiera, es la función del Contador Público, por ser un profesional que conoce ampliamente la realidad de la empresa u organismo público, capaz de realizar las auditorías de cumplimiento, logística, tributaria, ambiental y otros que aparecerá más adelante dentro del campo de su ejercicio profesional.

Varios analistas, pensadores y conocedores de organismos empresariales y públicos han calificado que **el Contador Público es el médico de la empresa**, porque él vive la realidad del flujo de efectivo, en su tarea de registro de entradas y salidas del dinero, aún hoy, inmerso en escenarios informáticos.

El dinero es el combustible que mueve la rueda de los negocios; así como el aceite, la gasolina, el petróleo, el gas, entre otros, son combustibles que mueven el automóvil.

A fin de relievar la importancia del contador, **Lawrence J. Gitman, autor del libro de Principios de Administración Financiera, hace una analogía** entre el médico especializado en cardiología y el contador especialista en finanzas. Gitman dice: si el cardiólogo encuentra que el corazón podría estar funcionando bien; pero, si se presenta un coágulo en alguna parte del sistema circulatorio, puede colapsar la salud del paciente; de la misma manera, en una empresa cuyo estado de situación financiera arroja el resultado económico con alta utilidad, desde el punto de vista contable; pero, puede ocurrir que las ventas del año del 100% solo ingresó a Caja el 20%, y el 80% está en cuentas por cobrar. Esta situación puede llevar al colapso del negocio, por falta de liquidez para cumplir con sus compromisos adquiridos a corto plazo.

En la profesión médica hay nuevos paradigmas en la filosofía de este profesional; ahora ya no se preparan para curar enfermedades, sino para prevenir enfermedades. En los párrafos anteriores hemos puntualizado que el contador es el médico de la empresa y de los organismos públicos, y es quien realiza la auditoría financiera como función privativa de la profesión. Actualmente, el contador - auditor procesa su trabajo en base a los estados financieros históricos, que no tiene un valor agregado esperado, porque se trata de una información de gestión pasada, sin trascendencia. En ese período de tiempo las personas responsables de la gestión, -de repente- ya no continúan –hoy- en sus cargos.
La auditoría preventiva, básicamente, es control, es un instrumento de gestión que persigue reflejar la imagen fiel del sistema de prevención de riesgos laborales de la empresa. Prevenir genera acciones disuasivas con precauciones, para disuadir o medidas -por anticipado- para mitigar, evitar o remediar un mal.

Percepción de los contadores de la auditoría preventiva

Se ha aplicado la encuesta a 30 Contadores Públicos Auditores, el día lunes 14 de noviembre del 2016, en el Colegio de Contadores Públicos (escenario de la encuesta).

Los resultados fueron como sigue:

1. **¿Usted cree que la auditoría financiera histórica, no genera valor agregado esperado, por tratarse de una información de una gestión concluida con todos vicios y fraudes en la administración de recursos privados y públicos?**
   El 90% de los encuestados, respondieron totalmente estar de acuerdo en que la auditoría financiera histórica, no agrega valor agregado esperado, porque se trata de un examen practicado a la gestión ya realizada (período de gestión), en consecuencia cualquier resultado hallado no permite corregir, rectificar, prevenir los posibles errores o malversaciones de los recursos financieros.

2. **En el Perú actual experimentamos hechos inauditos en el manejo de recursos del Estado, producto de esa acción dolosa, muchos funcionarios públicos actualmente purgan en las cárceles. ¿Cree Ud. que la auditoría preventiva, sería una solución para disuadir, prevenir, detectar y proceder frente a diferentes acciones de fraude?**
   La respuesta fue inobjetable, totalmente de acuerdo el 100%.

3. **¿Ud. como auditor, considera profesionalmente suficiente la forma cómo se audita, mediante la tecnología de información y comunicaciones (TIC)?**
   Respondieron el 70% en total de acuerdo, el 20% parcialmente de acuerdo y sólo el 10% respondieron en desacuerdo.

4. **¿Considera Ud. que es necesario contar con un auditor de sistemas en la Oficina de control Interno o auditoría interna a fin de prevenir los fraudes?**
   En esta pregunta, igualmente respondieron estar totalmente de acuerdo, por la forma rápida e inmediata de lograr la detección de fraudes y corrupciones.

5. **¿Considera Ud. que ya es momento que en el Perú exista normatividad legislativa, relativa a la manera de control de la gestión financiera mediante la auditoría preventiva?**
   Lo mismo, la respuesta fue categórica, el 100% está totalmente de acuerdo que se dicte una norma específica de aplicación de auditoría preventiva tanto en el sector privado como en el sector público.

Conclusiones

1. Las auditorías aplicadas sobre los estados financieros históricos, no generan valor agregado esperado, porque se ha procesado la información de gestión pasada, sin trascendencia. Se trata de períodos de gestión concluidas, ya no está en el cargo la persona o personas quienes deben responder por malos manejos, muchos salieron al exterior para eludir olímpicamente sus responsabilidades.

2. En las encuestas realizadas a los contadores públicos auditores, la mayoría está de acuerdo en aplicar la auditoría preventiva en todas las organizaciones, a fin de corregir, enmendar y prevenir los errores y riesgos que suelen incurrir los

responsables de la gestión en las empresas privadas como los funcionarios que ejercen cargos en el sector público.

3. La aplicación de auditoría preventiva, permite detectar y proceder frente a diferentes acciones de fraudes, conforme sostiene enfáticamente la auditoría forense preventiva.

4. En el Perú, experimentamos a cada momento, la corrupción de personas inescrupulosas, que están inmersos en fraudes y actos reñidos por la moral y ética. Es necesario recordar la sabia frase “en arca abierta hasta el justo peca”, eso es precisamente lo que pretende evitar la auditoría preventiva.

5. Los encuestados respondieron sobre la urgencia de contar con una norma legal que permita el control adecuado y oportuno de los estados financieros tanto del sector privado como de los organismos públicos.

Recomendaciones

1. Se deben organizar seminarios, bajo la coordinación del Colegio de Contadores Públicos de Lima y provincias, sobre la importancia de aplicación de la Auditoría Preventiva a nivel de empresas privadas y en las organizaciones del sector público más vulnerables, llámese Ministerios, Gobiernos Regionales, etcétera.

2. En las Universidades del Perú se debe incluir dentro del currículo de estudios, el curso de Auditoría Preventiva, como una forma de prevenir posibles fraudes en la gestión de negocios de empresas privadas y del sector público prioritariamente.

3. La Contraloría General de la República, en su misión de cautelar los recursos del Estado, debe programar y dictar cursos relacionados con la Auditoría Preventiva, como requisito obligatorio para la colegiación de contadores públicos de acuerdo a las normas legales vigentes.

4. Es necesario y urgente que la Contraloría General de la República y otros organismos públicos encargados de control financiero, tramiten ante las instancias correspondientes, que dicten normas referente a la Auditoría Preventiva para detectar y proceder frente a diferentes acciones de fraude y corrupción

.Fuentes de información

Lawrence J. Gitman; Chad J. Zutter (2012) Principios de Administración Financiera México: Pearson México
Ferreyros J.A (2009) Informática-SIG y Auditoría de Sistemas Lima: falta
Echenique J.A (2001). Auditoria en Informática. México: edit