

PONTIFICIA UNIVERSIDAD CATÓLICA DEL ECUADOR

FACULTAD DE CIENCIAS ADMINISTRATIVAS Y CONTABLES

**TRABAJO DE TITULACIÓN DE GRADO PREVIO A LA OBTENCIÓN DEL
TÍTULO DE LICENCIATURA EN CONTABILIDAD Y AUDITORÍA**

**PROPUESTA DE BUENAS PRÁCTICAS PARA LA APLICACIÓN DEL
MARCO DE REFERENCIA DE AUDITORÍA DE INFORMACIÓN Y
TECNOLOGÍA (ITAF) EN LOS SISTEMAS CONTABLES DE LAS EMPRESAS
DE OUTSOURCING CONTABLE EN EL AÑO 2021**

IVONNE DE LOS ANGELES COELLO CABRERA

DIRECTOR: DR. EFRAÍN ROBERTO BECERRA PAGUAY PHD. (C)

QUITO, MARZO 2023

DIRECTOR:

MGR. Dr. Efraín Roberto Becerra Paguay

INFORMANTES:

Mgtr.

DEDICATORIA

A mis padres: Iván Coello y Deysce Cabrera, por su apoyo incondicional en todo momento, por siempre brindarme su cariño y amor.

A mis hermanos: Jenny e Iván Gabriel por su cariño, consejos y apoyo incondicional en los momentos más difíciles.

A mi abuelita: Marcela Correa por estar siempre junto a mí con su cariño y sus consejos.

Y sobre todo a Dios por la salud, por siempre guiarme en cada momento de mi vida y darme fuerzas para enfrentar cada situación, obstáculo que se me presente.

Ivonne Coello

AGRADECIMIENTO

Al finalizar una etapa importante en vida, junto con el presente trabajo de titulación quiero expresar mis agradecimientos.

A Dios por permitirme finalizar una etapa más en mi vida.

A mi familia por todo el apoyo y esfuerzo brindado para poder culminar la universidad.

A mis profesores por todo el conocimiento impartido en clases.

A mi director de tesis, por su tiempo y guiarme siempre de la mejor manera para poder culminar este trabajo.

Y a todos quienes estuvieron junto a mí en la universidad apoyándome.

Ivonne Coello

Tabla de Contenidos

1. FUNDAMENTACIÓN TEÓRICO AUDITORÍA	1
1.1. Definición	1
1.2. Evolución de la auditoría	2
1.2.1. Antecedentes de la auditoría	2
1.2.2. Calificación de los tipos de auditorías	3
1.3. Sistemas informáticos y su evolución.....	5
1.3.1. Evolución de la función del sistema de información	6
1.4. Seguridad de la información	9
1.4.1. Control Interno.....	9
1.4.1.1. Método COSO-ERM	9
1.4.1.2. ISACA	10
1.4.1.3. COBIT	12
1.5. Auditoría de Sistemas	13
2. AUDITORÍA A LOS SISTEMAS INFORMÁTICOS EN LA INDUSTRIA CONTABLE	15
2.1. Legislación informática	15
2.1.1. ITAF.....	16
2.1.2. ISO 27000	17
2.1.3. Ley orgánica de protección de datos personales.....	19
2.2. Softwares más utilizados en los outsourcing contables	19
2.3. Causas que originan auditorías a los sistemas contables	19
2.4. Objetivos de las auditorías a los sistemas contables	21
2.5. Fases de la auditoría informática	22
3. PROPUESTA DE BUENAS PRÁCTICAS PARA LA TIC'S DENTRO DE LOS OUTSOURCING CONTABLES	24
3.1. Normativas relacionadas a la auditoria de sistemas.....	24

3.1.1. NIAS	24
3.1.2. Directrices ITAF	26
3.2. ITAF, y su aplicación en los outsourcing contables	35
3.3. Análisis de los sistemas	35
3.3.1. Objetivos del análisis de los sistemas contable	35
3.3.2. Sistemas Contables	36
3.4. Propuesta de buenas prácticas en el manejo de TI en los outsourcing contables	38
3.4.1. Criterios profesionales sobre la seguridad a sistemas contables.....	39
3.4.2. Perfil del Outsourcing Contable	50
3.4.3. Propuesta de buenas prácticas aplicado al área de servicio accounting	51
4. CONCLUSIONES Y RECOMENDACIONES	55
4.1. Conclusiones	55
4.2. Recomendaciones	56

Lista de Tablas

Tabla 1. Tipos de Auditoría	3
Tabla 2. Estándares	27

Lista de Figuras

Figura 1. Método COSO-ERM.....	10
Figura 2. Marco de referencia integrado de COBIT.....	12
Figura 3. ISO 27000	18

Resumen ejecutivo

Actualmente, con la globalización y actualización de la tecnología, las formas de ataque y daño utilizando las tecnologías de la información van de la mano, aumentando en gran medida el trabajo de los auditores para identificar los riesgos relacionados con las TIC. Sin embargo, no toda la responsabilidad recae en los auditores, ya que quienes utilizan diversas plataformas digitales para facilitar sus tareas también deben ayudar a minimizar el riesgo de ciberataques.

En la actualidad, existen gran cantidad de firmas contables en el Ecuador que brindan servicios de tercerización de servicios, por lo cual será importante identificar los servicios que las mismas brindan a entidades y/o organizaciones y lo importante que será la aplicación de buenas prácticas en los sistemas contables.

Abstract

Currently, with the globalization and updating of technology, the forms of attack and damage using information technologies go hand in hand, greatly increasing the work of auditors to identify risks related to ICT. However, not all of the responsibility falls on auditors, as those who use various digital platforms to facilitate their tasks must also help minimize the risk of cyberattacks.

Currently, there are many accounting firms in Ecuador that provide outsourcing services, so it will be important to identify the services that they provide to entities and/or organizations and how important the application of good practices will be in accounting systems.

1. FUNDAMENTACIÓN TEÓRICO AUDITORÍA

1.1. Definición

Como parte esencial del trabajo de titulación, se define el concepto de auditoría, que según Muñoz (2002) se define como, "...la revisión independiente de alguna o algunas actividades, funciones específicas, resultados u operaciones de una entidad administrativa, realizada por un profesional de la auditoría, con el propósito de evaluar su correcta realización y, con base en ese análisis, poder emitir una opinión autorizada sobre la razonabilidad de sus resultados y el cumplimiento de sus operaciones." (p. 11)

Adicional, se agregan definiciones de acuerdo con la auditoría:

Para Alcívar (2016) la actividad de auditar consiste en realizar un examen de los procesos y de la actividad económica de una organización para confirmar si se ajustan a lo fijado por las leyes o los buenos criterios (pág. 3).

Según Muñoz (2002) también se lo define como la supervisión de las cuentas de una empresa, hecha por decisión de un tribunal o a instancias de particular

Revisión de cuentas, examen y evaluación de la situación financiera y administrativa de una institución o empresa, realizados por especialistas ajenos a la misma (p. 11).

De acuerdo con Torres (2017) es un examen de las demostraciones y registros administrativos, en donde el auditor observa la exactitud, integridad y autenticidad de tales demostraciones, registros y documentos. (pág. 66)

Se puede concluir que la auditoría es una actividad, proceso que es llevado a cabo con el objetivo de evaluar la situación económica de una entidad para poder brindar pautas que ayuden a los administradores y socios a desarrollar estrategias que a corto, mediano y largo plazo represente actividades que como resultado sean de beneficio económico para la organización.

Es esencial, considerar que los conceptos anteriormente definidos serán de gran importancia para el desarrollo del presente trabajo de titulación.

1.2. Evolución de la auditoría

Según Muñoz (2002) indica que “En tiempos históricos, auditor era aquella persona a quien le leían los ingresos y gastos producidos por un establecimiento (de ahí su raíz latina del verbo *audire*, oír, escuchar), práctica muy utilizada por civilizaciones muy antiguas [...]” (p. 4)., de acuerdo a lo descrito por el autor la auditoría ha sido implementada desde inicios del siglo XX, y esto ha permitido que a lo largo de los años evolucione constantemente, en la actualidad la auditoría no solo tiene que ver con la información financiera de una empresa, si no que va más allá, es decir desde donde nace el registro y los controles que se tiene sobre el mismo.

1.2.1. Antecedentes de la auditoría

A medida que se desarrollaba el comercio, primero a través del intercambio de bienes a través de ciudades, estados y finalmente continentes, e impulsado por el aumento del tamaño y la cantidad del comercio, los primeros comerciantes necesitaban establecer mecanismos básicos de registro que les permitieran controlar su actividad comercial. Más tarde, a medida que los comerciantes crecieron y se reorganizaron en gremios y mercados locales, surgió la necesidad de una mejor documentación de sus actividades individuales y colectivas. Posteriormente, a medida que estos grupos crecieron, convirtiéndose en que se convirtieron en incipientes empresas, fue necesario establecer un mayor control para conocer sus actividades financieras, gracias a ese crecimiento se inició el registro de operaciones mercantiles a través de escribas, quienes al principio asentaban dichas operaciones en forma rudimentaria; posteriormente, con el nacimiento de la partida doble y el registro de operaciones financieras, surgió la llamada *teneduría de libros*. Conforme esta técnica evolucionó, se llegó a impulsar la contabilidad y el registro de operaciones en libros y pólizas. (Muñoz, 2002, p. 3)

En la actualidad, la contabilidad se lleva a cabo en sistemas de cómputo. A la par que esto evolucionaba, fue necesario que alguien evaluara que estos registros y resultados fueran correctos y veraces. Entonces se requirió también de alguien que verificara la veracidad

y confiabilidad de esas operaciones. En ese momento nació el acto de auditar (Muñoz, 2002, p. 3).

Es importante destacar que la auditoría ha tenido una evolución con el tiempo, desde el intercambio de bienes llamado trueque hasta el crecimiento de poblaciones que obligo buscar a las personas de aquel entonces mecanismos de control necesarios para el manejo de actividades comerciales que les permitiera llevar un correcto manejo de sus actividades financieras.

1.2.2. Calificación de los tipos de auditorías

Actualmente existen varias profesiones de auditoría, y según (Muñoz, 2002, pp. 12,13), la auditoria se puede categorizar de la siguiente manera:

Tabla 1. Tipos de Auditoría

Tipos de Auditoría	Categorización
Auditorías por su lugar de aplicación	Auditoría externa
	Auditoría interna
Auditorías por su área de aplicación	Auditoría financiera
	Auditoría administrative
	Auditoría operacional
	Auditoría integral
	Auditoría gubernamental
	Auditoría de Sistemas
	Auditoría al área médica
Auditorías especializadas en áreas específicas	Auditoría al desarrollo de obras y construcciones
	Auditoría fiscal
	Auditoría laboral
	Auditoría de proyectos de inversión
	Auditoría a la caja chica o caja mayor
	Auditoría del manejo de mercancías
	Auditoría Ambiental

	Auditoría de Sistemas
	Auditoría informática
	Auditoría con la computadora
	Auditoría sin la computadora
	Auditoría a la gestión informática
	Auditoría al sistema de cómputo
	Auditoría alrededor de la computadora
Auditoría de sistemas computacionales	Auditoría de la seguridad de sistemas computacionales
	Auditoría a los sistemas de redes
	Auditoría integral a los centros de cómputo
	Auditoría ISO-9000 a los sistemas computacionales
	Auditoría outsourcing
	Auditoría ergonómica de sistemas computacionales

Nota: Información tomada de (Muñoz, 2002), elaboración propia.

Como se puede observar en la tabla anterior, la auditoría actualmente abarca diferentes campos y/o profesiones, y esto se debe a la globalización, requiriendo profesionales bien preparados para cubrir diferentes temas, como se dijo anteriormente, el auditor solía ser la persona encarga de revisar registros contables con el fin de tener un correcto control de las finanzas, sin embargo, se ha demostrado que va mucho más allá.

De acuerdo con Muñoz (2002), una auditoría informática o auditoría de sistemas de información es un examen técnico, profesional y exhaustivo de los sistemas informáticos, el software y la información que utiliza una empresa, ya sea personal, compartida y/o en red, y sus instalaciones, telecomunicaciones, mobiliario, periféricos y otros componentes. De la misma manera se revisa la administración informática, el uso de los recursos informáticos, las medidas de seguridad y los consumibles necesarios para el funcionamiento del centro de cómputo. El propósito básico es evaluar si el sistema se está utilizando adecuadamente para ingresar datos correctamente, procesar

información adecuadamente y difundir los resultados de manera oportuna en la agencia, incluida la evaluación del desempeño de funciones, actividades y operaciones que involucran a funcionarios, empleados y usuarios de servicios proporcionados por sistemas informáticos.

Adicional, es importante identificar que dentro de la auditoría de sistemas computacionales se encuentra la auditoría de outsourcing, para la cual Muñoz (2002) propone la siguiente definición:

Es la revisión exhaustiva, sistemática y especializada que se realiza para evaluar la calidad en el servicio de asesoría o procesamiento externo de información que proporciona una empresa a otra. Esto se lleva a cabo con el fin de revisar la confiabilidad, oportunidad, suficiencia y asesoría por parte de los prestadores de servicios de procesamiento de datos, así como el cumplimiento de las funciones y actividades que tienen encomendados los prestadores de servicios, usuarios y el personal en general. Dicha revisión se realiza también en los equipos y sistemas.
(p. 127)

1.3. Sistemas informáticos y su evolución

Los sistemas de información han ido evolucionando durante los últimos años hasta constituir los denominados sistemas de información estratégicos. Primeramente, los sistemas de información empresariales eran considerados como un instrumento simplificador de las distintas actividades de la empresa, una herramienta con la cual se facilitaban los tramites y reducía la burocracia.

Su finalidad era básicamente llevar la contabilidad y el procesamiento de los documentos que a nivel operativo. Posteriormente el desarrollo de la informática y las telecomunicaciones permitieron incrementar la eficacia en la realización de las tareas, ahorrar tiempo en el desarrollo de las actividades y almacenar la mayor cantidad de información en el menor espacio posible, lo cual aumentó en las organizaciones el interés en los sistemas de información. Con el transcurrir del tiempo las empresas fueron observando como las tecnologías y sistemas de información permitían a la empresa obtener mejores resultados que sus competidores, constituyéndose por sí mismas como una fuente de ventaja competitiva y una poderosa arma que permitía diferenciarse de sus

competidores y obtener mejores resultados que estos. De este modo los sistemas de información se constituyeron como una de las cuestiones estratégicas de la empresa, que ha de considerarse siempre en todo proceso de planificación empresarial. (Trasobares, pág. 4).

Los sistemas de información han evolucionado en las últimas décadas porque, como se mencionó en los párrafos anteriores, el desarrollo de los sistemas contables computarizados ha permitido a los auditores, consultores, etc. administrar, registrar y capturar el conocimiento sobre las actividades de una organización de una manera más flexible.

1.3.1. Evolución de la función del sistema de información

De acuerdo con el sitio web (tecnologias-informacion.com, 2018) la evolución de la función del sistema de información fue:

1950-1960 Procesamiento de datos electrónicos, sistema de procesamiento de transacciones

Durante este período, el papel de SI fue principalmente para realizar actividades como el procesamiento de transacciones, el mantenimiento de registros y la contabilidad. SI se utilizó principalmente para el procesamiento electrónico de datos.

EDP se describe como el uso de computadoras para registrar, clasificar, manipular y resumir datos. También se llama procesamiento de información o procesamiento de datos automático.

Sistema de procesamiento de transacciones (TPS) fue el primer sistema computarizado desarrollado para procesar datos comerciales. TPS estaba principalmente dirigido al personal administrativo de una organización. El TPS inicial utilizaba datos de procesamiento por lotes que se acumularon durante un período y todas las transacciones se procesaron posteriormente.

1960 -1970 Sistema de Información Gerencial

Management Information Systems (MSI) o Sistemas de información gerenciales. MSI procesa los datos en informes informativos útiles y proporciona a los gerentes las herramientas para organizar evaluar y administrar de manera eficiente los departamentos dentro de una organización. MSI entrega información en forma de pantallas e informes preespecificados para respaldar la toma de decisiones empresariales.

1970-1980 Sistemas de soporte de decisiones

En esta era, un avance importante fue la introducción de las computadoras personales (PC). Con la introducción de las PC, se produjo la distribución de la potencia informática o de procesamiento en toda la organización. La función de SI está fuertemente asociada con la administración en lugar de un enfoque técnico en una organización. El papel se centró en el "sistema interactivo basado en computadoras" para ayudar a los responsables de la toma de decisiones a resolver problemas.

Este nuevo rol de los sistemas de información para proporcionar soporte ad-hoc interactivo para el proceso de toma de decisiones a los gerentes y otros profesionales de negocios se denomina Sistemas de Soporte de Decisiones (DSS). DSS sirve el nivel de planificación, gestión y operaciones de una organización, por lo general, la alta dirección.

DSS usa datos de fuentes internas y / o externas. Las fuentes internas de datos pueden incluir datos de inventario, ventas, fabricación o financieros de la base de datos de una organización. Las fuentes externas podrían incluir precios, tasas de interés, población o tendencias. Los gerentes usan DSS para manipular los datos y ayudar con las decisiones. Los ejemplos de DSS son cifras de ingresos proyectadas basadas en suposiciones de ventas de nuevos productos, precios de productos y sistemas de análisis de riesgos.

1980-1990 Sistemas de información ejecutivo

Este período dio lugar a la informática departamental debido a que muchas organizaciones compran su propio hardware y software para satisfacer sus necesidades departamentales. En lugar de esperar el apoyo indirecto del departamento de servicio corporativo centralizado, los empleados podrían usar sus propios recursos para respaldar

sus requisitos laborales. Esta tendencia dio lugar a nuevos desafíos de incompatibilidad de datos, integridad y conectividad en diferentes departamentos.

1990-2000 Sistemas de gestión del conocimiento

Durante esta era, el rápido crecimiento de las intranets, extranets, internet y otras redes globales interconectadas cambiaron drásticamente las capacidades de SI en los negocios. Se hizo posible circular el conocimiento a diferentes partes del mundo independientemente del tiempo y el espacio.

Este período también vio una aparición de sistemas de planificación de recursos empresariales (ERP). ERP es una forma específica de organización de un sistema de información estratégica que incorpora todos los componentes de una organización, incluidas la fabricación, las ventas, la gestión de recursos, la planificación de recursos humanos y el marketing.

2000-2022 E-business

Internet y las tecnologías y aplicaciones relacionadas cambiaron la forma en que operan las empresas y las personas trabajan. Las funciones de los sistemas de información en este período siguen siendo las mismas que hace 50 años: mantenimiento de registros, gestión de informes, procesamiento de transacciones, gestión de soporte y procesos de gestión de la organización. Se usa para respaldar el proceso comercial, la toma de decisiones y las ventajas competitiva.

La diferencia es una mayor conectividad entre los componentes del sistema similares y diferentes. Existe una gran infraestructura de red, un mayor nivel de integración de funciones en todas las aplicaciones y potentes máquinas con mayor capacidad de almacenamiento. Muchas empresas usan tecnologías de Internet y procesos de negocio habilitados para la web para crear aplicaciones innovadoras de comercio electrónico. (Información, 2018).

1.4. Seguridad de la información

1.4.1. Control Interno

Según Aguirre (1996), el control interno puede definirse como un conjunto de procedimientos, políticas, directrices y planes de organización los cuales tiene por objeto asegurar una eficiencia, seguridad y orden en la gestión financiera, contable y administrativa de la empresa (salvaguardia de activos, fidelidad del proceso de información y registros, cumplimiento de políticas definidas, entre otros.)

La aplicación de control interno en las organizaciones tiene la finalidad de ser una guía que permitan cumplir con los objetivos empresariales, legales y a la vez prevenir de situaciones perjudiciales, entre otros.

En el año 1992 se publicó el Informe COSO, brindado una ayuda a los profesionales, puesto que describe todos los resultados que se obtuvieron durante la investigación del método.

El informe COSO brinda el enfoque de una estructura para comprender el control interno, que busca prevenir la pérdida de recursos, asegurar la elaboración de informes financieros y del cumplimiento de las leyes y regulaciones.

Dentro del control interno podemos encontrar cinco componentes fundamentales como son:

- Ambiente de control
- Evaluación de riesgos
- Actividades de control
- Información y comunicación
- Supervisión y seguimiento

1.4.1.1. Método COSO-ERM

Es un proceso estructurado, consistente y continuo implementado a través de toda la organización para identificar, evaluar, medir y reportar amenazas y oportunidades que

afectan el poder de alcanzar el logro de sus objetivos. La administración de riesgos corporativos se ocupa de los riesgos y oportunidades que afectan la creación de valor o su preservación.

El control interno se define como un proceso realizado por la gerencia y demás personal de la empresa con el fin de brindar una razonable seguridad sobre el logro de los objetivos en las siguientes categorías:

- Efectividad y eficacia de las operaciones
- Cumplimiento de las leyes y reglamentos aplicables
- Confiabilidad de la información financiera

Figura 1. Método COSO-ERM



Nota: Información tomada de (Martínez T. , 2017) Autor: COSO-ERM

1.4.1.2. ISACA

La Information Systems Audit and Control Association –Asociación de Auditoría y Control de Sistemas de Información– ISACA, comenzó en 1967. En 1969, el grupo se formalizó, incorporándose bajo el nombre de EDP Auditors Association –Asociación de Auditores de Procesamiento Electrónico de Datos. En 1976 la asociación formó una fundación de educación para llevar a cabo proyectos de investigación de gran escala para expandir los conocimientos y el valor del campo de gobernación y control de TI.

En las tres décadas transcurridas desde su creación, ISACA se ha convertido en una organización global que establece las pautas para los profesionales de gobernanza, control, seguridad y auditoría de información.

El aseguramiento de la información es la base sobre la que se construye la toma de decisiones de una organización. Sin aseguramiento, las empresas no tienen certidumbre de que la información sobre la que sustentan sus decisiones es confiable, segura y está disponible cuando se le necesita.

Definimos Aseguramiento de la Información como “la utilización de información y de diferentes actividades operativas, con el fin de proteger la información, los sistemas de información y las redes de forma que se preserve la disponibilidad, integridad, confidencialidad, autenticación y el no repudio, ante el riesgo de impacto de amenazas locales, o remotas a través de comunicaciones e Internet”.

Una tarea de aseguramiento puede darse a cualquier nivel, por lo que a continuación se describe brevemente las más importantes:

Aseguramiento de los Datos

Referente la información histórica o prospectiva, probabilística e indicadores de desempeño.

Aseguramiento de los Procesos

Basado principalmente en controles internos y procedimientos establecidos para la protección de intereses.

Aseguramiento del Comportamiento

Conformidad con normas, regulaciones o mejores prácticas.

Aseguramiento del Sistema de Gestión

En la que los objetivos del negocio son establecidos para proteger a todos los involucrados: directivos y empleados. (Aguirre, 2022)

1.4.1.3. COBIT

COBIT, lanzado en 1996, es una herramienta de gobierno de TI que ha cambiado la forma en que trabajan los profesionales de TI.

De acuerdo con ISACA, COBIT es:

“Una herramienta que permite evaluar la calidad del soporte de TI actual de la organización, vinculando los distintos procesos del negocio con los recursos informáticos que los sustentan” (Aguirre, 2022).

COBIT establece un diagnóstico que permite definir las metas desde el punto de vista de seguridad y control que le serán de utilidad para la organización para cada uno de sus procesos, pudiendo entonces establecer un plan de acción para lograr estas mejoras, y posteriormente identificar los lineamientos para sustentar un proceso de monitoreo y mejora continua sobre las soluciones implementadas. (Aguirre, 2022).

Figura 2. Marco de referencia integrado de COBIT



Nota: Información rescatada de (Espinoza et al., 2017) Author: Javeriana

El sistema COBIT es empleado en todo el mundo por personas quienes tienen información. Están principal los procesos de negocio y la tecnología, son aquellos de quien depende la tecnología y la información confiable, fiable y los que proveen calidad, confiabilidad y control de tecnología de información. Este sistema se basa 5

principios y 7 habilitadores, COBIT5 utiliza prácticas de gobierno y gestión para describir las acciones que son ejemplo de mejores prácticas de su aplicación.

Principios de COBIT

- Satisfacer las necesidades del accionista
- Considerar la empresa de punta a punta
- Aplicar un único modelo de referencia integrado
- Posibilitar un enfoque holístico
- Separar gobierno de la gestión

Habilitadores de COBIT

- Principios, políticas y modelos de referencia
- Procesos
- Estructuras organizacionales
- Cultura, ética y comportamiento
- Información
- Servicios, infraestructura y aplicaciones
- Gente, habilidades y competencias

Las empresas cuentan con un capital activo muy valioso: la información y la tecnología. El éxito empresarial depende cada vez más de la comprensión de estos dos componentes. Las buenas prácticas centralizadas dentro de COBIT permiten a las empresas adaptarse a la tecnología de la información para lograr resultados óptimos. La información y la tecnología que la respalda son los activos más valiosos de muchas empresas, pero a menudo no se comprenden bien. Las empresas exitosas reconocen los beneficios de la tecnología de la información y la utilizan para crear valor para las partes interesadas. (Espinoza et al., 2017)

1.5. Auditoría de Sistemas

Según Muñoz (2002) la auditoría a los sistemas informáticos se define como:

La revisión técnica, especializada y exhaustiva que se realiza a los sistemas computacionales, software e información utilizados en una empresa, sean individuales, compartidos y/o de redes, así como a sus instalaciones, telecomunicaciones, mobiliario, equipos periféricos y demás componentes. Dicha revisión se realiza de igual manera a la gestión informática, el aprovechamiento de sus recursos, las medidas de seguridad y los bienes de consumo necesarios para el funcionamiento del centro de cómputo. El propósito fundamental es evaluar el uso adecuado de los sistemas para el correcto ingreso de los datos, el procesamiento adecuado de la información y la emisión oportuna de sus resultados en la institución, incluyendo la evaluación en el cumplimiento de las funciones, actividades y operaciones de funcionarios, empleados y usuarios involucrados con los servicios que proporcionan los sistemas computacionales a la empresa. (pág. 19)

Según la definición anterior, se puede decir que una auditoría de TI (también conocida como auditoría TSI) es una verificación técnica de todo el sistema informático de una empresa, comenzando con el software utilizado por la empresa y terminando con los consumibles relacionados con el uso de TSI. La importancia de esta auditoría es que debe realizarse con el objetivo de minimizar el potencial de mal uso de la información y/o datos, reduciendo así los riesgos que puedan estar asociados con los TSI. Esto puede estar en las etapas de planificación de una auditoría completa.

La realización de este tipo de auditoría requiere conocimientos, aunque no avanzados lo suficiente para comprender el funcionamiento de los TSI en una organización. El marco normativo a partir del cual nace ITAF son las Normas Internacionales de Auditoría (NIAS) ya que, esta normativa es exigida y recomendada por el International Accounting Standards Board (IASB) para realizar cualquier tipo de auditoría sin importar la focalización que pueda llegar a tener la ciencia de la auditoría.

La auditoría no solo está relacionada con las cifras de una empresa, si no por el contrario, junto a la globalización local y global, requiere que los profesionales responsables de las auditorías se especialicen en áreas más específicas, como la informática.

2. AUDITORÍA A LOS SISTEMAS INFORMÁTICOS EN LA INDUSTRIA CONTABLE

2.1. Legislación informática

ITAF y NIAS, son normativas internacionales que deben ser aplicadas en su totalidad para poder realizar una auditoría a sistemas de información, ya que aportan con conceptos y procedimientos en diferentes situaciones que pudiesen suscitarse dentro del ejercicio profesional. En cuanto a normativa local se refiere, la persona jurídica o natural deberá tomar enfocarse principalmente en la resolución No. SCVS-INC-DNCDN-2016-011, donde se encuentran detalladas diversas consideraciones para la realización de una auditoría externa.

Los requisitos para ejercer como auditor de sistemas de información no se encuentran normados, sin embargo, los requisitos para ser auditor externo si lo están, razón por la cual un perfil ideal para ejercer esta rama de la auditoría será una combinación de los requisitos formales para prestar servicios de auditoría externa, y los requisitos informales que pueden ser relevantes para la auditoría a los sistemas de información, en ejemplo de perfil ideal es como se muestra a continuación.

- Tener título de tercer nivel de auditor, contador público autorizado, economista, ingeniero comercial o ingeniero en contabilidad y auditoría, registrado en la Secretaría Nacional de Educación Superior, Ciencia, Tecnología e Innovación,
- Experiencia en auditorías externas/ internas realizadas a compañías y entes sujetos a control de la Superintendencia de Compañías, Valores y Seguros,
- Dominio de normas ITAF y NIA,
- Conocimiento y dominio de Softwares de auditorías informáticas,
- Experiencia en gestión de proyectos y análisis de riesgos.

2.1.1. ITAF

El marco de referencia de auditoría de tecnología de la información de ISACA (ITAF) en un marco de auditoría de TI integral que:

- Establece las normas que definen los requerimientos relacionados con los roles y responsabilidades, ética y conducta profesional esperada y conocimientos y competencias requeridas de los profesionales de auditoría y aseguramiento de TI.
- Define términos y conceptos específicos para la auditoría y aseguramiento de TI
- Proporciona orientación y técnicas para la planificación, la realización y los informes de las asignaciones de auditoría y aseguramiento TI

ITAF proporciona un recurso único para los profesionales de la auditoría y aseguramiento de TI para obtener una guía sobre el desempeño de auditorías y el desarrollo de informes de auditoría efectivos.

Los estándares de ITAF según ISACA (2020) se dividen en tres categorías:

- **Estándares generales (serie 1000)**- Detallar los principios de la profesión de aseguramiento de TI. Esto se aplica a los trabajos incluido entre otros, la ética, independencia, objetividad y el debido cuidado del profesional de auditoría y aseguramiento TI, así como el conocimiento, la competencia y la habilidad.
- **Estándares de desempeño (serie 1200)**- Abordar la realización del trabajo, como la planificación y supervisión, el alcance, la evaluación de riesgos, la movilización de recursos, la gestión del compromiso, la evidencia de auditoría y aseguramiento, y el ejercicio del juicio profesional y el debido cuidado.
- **Estándares de informes (serie 1400)**– Abordar los tipos de informes, los métodos de comunicación y la información comunicada. (pág. 267)

El marco normativo a partir del cual nace ITAF son las Normas Internacionales de Auditoría (NIAS) ya que, esta normativa es exigida y recomendada por el International

Accounting Standards Board (IASB) para realizar cualquier tipo de auditoría sin importar la focalización que pueda llegar a tener la ciencia de la auditoría.

De acuerdo con (IASB, s.f.) El objetivo principal del IASB, son los siguientes:

(a) desarrollar, buscando el interés público, un único conjunto de normas contables de carácter global que sean de alta calidad, comprensibles y de cumplimiento obligado, que requieran información de alta calidad, transparente y comparable en los estados financieros y en otros tipos de información financiera, para ayudar a los participantes en los mercados de capitales de todo el mundo, y a otros usuarios, a tomar decisiones económicas;

(b) promover el uso y la aplicación rigurosa de tales normas;

(c) cumplir con los objetivos asociados con (a) y (b), teniendo en cuenta, cuando sea necesario, las necesidades especiales de entidades pequeñas y medianas y de economías emergentes; y

(d) llevar a la convergencia entre las normas contables nacionales y las Normas Internacionales de Contabilidad y las Normas Internacionales de Información Financiera, hacia soluciones de alta calidad.

2.1.2. ISO 27000

La ISO 27000 ofrece una visión general de las normas y una introducción a los Sistemas de gestión de la seguridad de la información (SGSI). Uno de los aspectos más destacados es la implementación del SGSI, este consiste es un proceso cíclico continuo que pasas por las fases Plan-Do-Check-Act y vuelta a empezar.

Arranque o inicio del proyecto: en esta fase es necesario un compromiso por parte de la dirección de la empresa u organización, la realización de una buena planificación, así como la asignación de los responsables del proyecto.

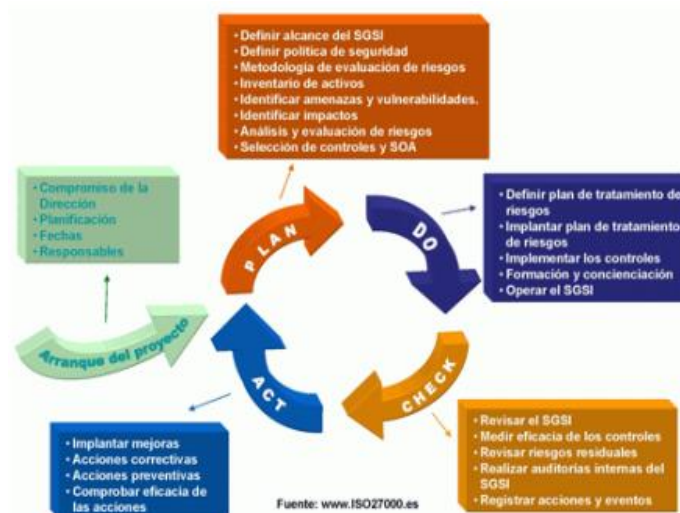
Planificación (Plan): en esta fase se deberían concretar aspectos como, de seguridad, la metodología y enfoque a utilizar para la evaluación de riesgos, el inventario de activos, la identificación de puntos débiles y la identificación de impactos (G. y otros, pág. 210).

Realización (Do): en esta fase se definiría e implementaría el plan de tratamiento de riesgos, se implementarían elementos de control, tareas de formación (G. y otros, pág. 210).

Revisión (Check): posterior a la fase de realización, se hace necesario revisar el proceso con el fin de medir la eficiencia de los controles y revisar otros riesgos (G. y otros, pág. 210).

Actuación (Act): en esta fase se implementarían mejoras y se adoptarían medidas correctoras y preventivas, con el fin de comprobar la eficacia de las acciones realizadas. (G. y otros, pág. 210)

Figura 3.ISO 27000



Nota: Tomado de (G. et al.) Autor: ISO 27000

2.1.3. Ley orgánica de protección de datos personales

El objeto y finalidad de la presente ley es garantizar el ejercicio del derecho a la protección de datos personales, que incluye el acceso y decisión sobre información y datos de este carácter, así como su correspondiente protección.

2.2. Softwares más utilizados en los outsourcing contables

Existen diversos programas informáticos en el mercado enfocados a la gestión administrativa contable que son de gran ayuda para el ingreso de información de las empresas (Leandro, 2015).

En la actualidad se encuentran diferentes tipos de programas contables cada uno se diferencia por los productos que el mismo pueda ofrecer y dentro de ellos sus costos, adicional es importante mencionar que existen programas de escritorio y programas web. (Factory, s.f.)

Programas informáticos contables:

- Latinium
- Contifico
- Dátil
- Dora
- Perseo
- COI (Aspel)
- Helisa
- SAP Business One
- Siigo Pyme

2.3. Causas que originan auditorías a los sistemas contables

Las empresas poseen Sistemas de información para la gestión de su economía, es importante que estos funcionen correctamente y no sean manipulados, sometiéndose a un control estricto de evaluación de eficacia y eficiencia. (Martínez Y. A., 2012)

En relación con lo mencionado antes, la auditoria a los sistemas contables puede llevarse a cabo por diferentes aspectos, ya sean estos por control o por verificación de actividades y con ello evaluar el trabajo realizado por cada colaborador de la empresa, esto con el fin de evidenciar si existe un uso incorrecto o inadecuado del sistema, por lo cual este tipo de actividades ayudar a prevenir futuros eventos perjudiciales para la entidad.

Asimismo, según Muños R. existen diversas causas por las cuales se realizan auditoria a los sistemas contables, a continuación, se detallan algunas causas:

- Por solicitud expresa de procedencia interna
- Por solicitud expresa de procedencia externa
- Como consecuencia de emergencias y condiciones especiales
- Por riesgos y contingencias informáticas
- Como resultado de los planes de contingencia
- Por resultados obtenidos de otras auditorías
- Como parte del programa integral de auditoría

A continuación, detalla algunas causas mencionadas anteriormente:

A petición de accionistas, socios y dueños

Los dueños, accionistas de la empresa contrata a un tercero como un auditor externo con la finalidad de conocer cómo se utilizan los recursos de su empresa, para conocer el rendimiento de su patrimonio, si no existen fugas, malos usos o cualquier otro aspecto que interese a los dueños de la empresa, en el caso de la auditoria a los sistemas esta auditoría se encuentra enfocada a hacia el aprovechamiento de los recursos del área de sistematización de la empresa.

Por orden de la dirección general

Esta revisión puede realizarse por diversos motivos como una evaluación periódica del área de sistemas contables, con la finalidad de verificar el cumplimiento de actividades.

Por ordenamiento de las autoridades fiscales

Las autoridades fiscales solicitan (imponen) la realización de una auditoría que por lo general es de tipo externo, realizada por una empresa despacho o auditor independiente y casi siempre está enfocada a revisar la información de tipo impositivo que se procesa de los sistemas computacionales de la empresa.

De acuerdo con el párrafo anterior este tipo de auditorías tiene el objetivo de revisar la información y conocer a detalle si la misma tiene un correcto funcionamiento para el cálculo de impuestos o los resultados financieros.

Riesgos y contingencias del personal informático

Se origina por los posibles riesgos derivados de la actuación del factor humano del área de sistemas, ya sea del personal, asesores o consultores, ya sea porque pueden existir deficiencias y problemas de incumplimiento de las actividades.

2.4. Objetivos de las auditorías a los sistemas contables

El objetivo de realizar una auditoría a los sistemas contables puede darse por el hecho de una necesidad de la empresa cuyo fin sea el de evaluar diferentes áreas y los programas informáticos de las mismas.

Existen varios objetivos relacionados con la auditoría a los sistemas contables; sin embargo, los más importantes y concurrentes son los siguientes:

- Evaluar el cumplimiento de planes, programas, estándares, políticas, normas, lineamientos que regulan las funciones y actividades de las áreas y de los sistemas de procesamiento de información, así como de su personal y de sus usuarios. (Muñoz, 2002, pág. 205)
- Proporcionar información para el control de la totalidad de actividades de la empresa, pudiendo comprobar el cumplimiento de las metas establecidas por

la organización. Los sistemas de información abarcan a todos los departamentos de la empresa y a la gestión global de la organización.

- Adaptar las necesidades de información a la evolución de la empresa: conforme la empresa va creciendo y desarrollándose, surgen nuevas necesidades de información que han de ser satisfechas por el sistema de información, evolucionando este último adecuándose a las nuevas circunstancias del entorno. (Trasobares, pág. 2)

Con relación a las definiciones antes mencionadas, se podría concluir que el objetivo de las auditorías a los sistemas contables es establecer acciones que permitan un correcto manejo de la información en la empresa, y que con ello se cumplan las normas, políticas y procedimientos y de esta forma poder tener una confiabilidad sobre el procesamiento de datos y la emisión de balances contables.

2.5. Fases de la auditoría informática

La auditoría de un sistema informático requiere una serie ordenada de actividades y procedimientos específicos que deben desarrollarse previamente de forma secuencial, cronológica y manejable de acuerdo con fases, eventos y acciones necesarios para su ejecución.

Se creará de acuerdo con las necesidades específicas de la institución. Además, estos procedimientos deben adaptarse según el tipo de auditoría.

Llevar a cabo auditorías del sistema y adherirse estrictamente a los requisitos, técnicas y métodos de evaluación del dominio de sistematización. (Muñoz, 2002, p. 180)

1era etapa: Planeación de la auditoría de sistemas computacionales

P1. Identificar el origen de la auditoría

P2. Realizar una vista preliminar al área que será evaluada

P3. Establecer los objetivos de la auditoría

- P4. Determinar los puntos que será evaluados
- P5. Elaborar planes, programas y presupuestos para realizar la auditoría
- P6. Identificar y seleccionar los métodos, herramientas, instrumentos y procedimientos necesarios para la auditoría
- P7. Asignar los recursos y sistemas computacionales para la auditoría

2da etapa: Ejecución de la auditoria de sistemas computacionales

- E1. Realizar las acciones programadas para la auditoria
- E2. Aplicar los instrumentos y herramientas para la auditoria
- E3. Identificar y elaborar los documentos de desviaciones encontradas
- E4. Elaborar el dictamen preliminar y presentarlo a discusión
- E5. Integrar el legajo de papeles de trabajo de la auditoria

3era etapa: Dictamen de la auditoria de sistemas computacionales

- D1. Analizar la información y elaborar un informe de situaciones detectadas
- D2. Elaborar el dictamen final
- D3. Presentar el informe de auditoria (Muñoz, 2002, p. 185)

3. PROPUESTA DE BUENAS PRÁCTICAS PARA LA TIC'S DENTRO DE LOS OUTSOURCING CONTABLES

3.1. Normativas relacionadas a la auditoria de sistemas

3.1.1. NIAS

NIA 15

El propósito de la NIA 15 (Auditoría en un ambiente de sistemas de información por computadora), es establecer normas y proporcionar lineamientos sobre los procedimientos que deben seguirse cuando se realiza una auditoría en un ambiente de sistemas de información computarizada (SIC).

Un ambiente SIC existe cuando está involucrada una computadora de cualquier tipo o tamaño en el procesamiento por la entidad de información financiera de importancia para la auditoría, ya sea que dicha computadora sea operada por la entidad o por una tercera parte.

Para realizar una auditoría a sistemas informáticos el auditor deberá:

Habilidad y competencia

El auditor debería contar con suficiente conocimiento del SIC para planear, dirigir, supervisar y revisar el trabajo desarrollado.

La persona a cargo de realizar una auditoría debe tener una comprensión de los sistemas contables, su funcionamiento, controles internos y procesamientos de datos en transacciones, ya que esto le permitirá emplear pruebas de control a dicho sistema.

Planeación

El auditor deberá obtener una comprensión de los sistemas de contabilidad y de control interno, suficiente para planear la auditoría y desarrollar un enfoque. Dentro de esta comprensión se encuentran asuntos como la complejidad del procesamiento por computadora en cada operación de la contabilidad.

Evaluación del riesgo

El auditor deberá hacer una evaluación de los riesgos inherentes y de control para las aseveraciones importantes de los estados financieros. Los riesgos pueden resultar de deficiencias en actividades generales como el desarrollo y mantenimiento de programas, soporte de software, operaciones y control sobre el acceso a programas de utilería de privilegio especial.

Procedimientos de auditoría

El auditor deberá considerar el ambiente SIC al momento de diseñar los procedimientos de auditoría para reducir el riesgo a un nivel aceptablemente bajo. (Accountants et al., 2022)

NIA 16

La NIA 16 (Auditoría en un entorno de sistemas de información por computadora), la aplicación de procedimientos de auditoría puede requerir que el auditor considere técnicas que usen la computadora como una herramienta de auditoría. Estos diversos usos de la computadora son conocidos como Técnicas de Auditoría con Ayuda de Computadora (TAACs).

Esta norma describe dos de los tipos más comunes de TAACs; software de auditoría y datos de prueba usados para propósito de auditoría.

Software de auditoría

Consiste en programas de computadora usados por el auditor, como parte de sus procedimientos de auditoría, para procesar datos de importancia de auditoría del sistema de contabilidad de la entidad. Puede consistir en programas de paquete, programas escritos para un propósito, y programas de utilería.

Los programas en paquete son programas generalizados de computadora diseñados para desempeñar funciones de procesamiento de datos que incluyen leer archivos de computadora, seleccionar información, realizar cálculos, crear archivos de datos e imprimir informes en un formato específico por el auditor.

Datos de prueba

Las técnicas de datos de prueba se usan para conducir procedimientos de auditoría alimentado de datos por ejemplo una muestra de transacciones al sistema de computadora de una entidad, y comparando los resultados obtenidos con resultados predeterminados, como: transacciones de prueba seleccionadas de transacciones procesadas previamente o creadas por el auditor para probar características específicas de procesamiento del sistema de computadora de una entidad. Dichas transacciones son procesadas generalmente por separado del procesamiento normal de la entidad. (Accountants et al., 2022)

3.1.2. Directrices ITAF

El ITAF está dirigido aquellos profesionales de aseguramiento y auditoría de TI y están implicados en proporcionar aseguramiento sobre proceso de TI, componentes aplicados de TI, sistemas e infraestructura. La aplicación del marco de referencia es un prerrequisito para conducir la tarea de aseguramiento y auditoría de TI. Los estándares son obligatorios. Las directrices, herramientas y técnicas se diseñan para proporcionar asistencia no obligatoria a la hora de realizar tareas de aseguramiento. (ISACA, 2020)

Los estándares de ITAF se dividen en tres categorías:

Estándares generales (serie 1000): detallar los principios de la profesión de aseguramiento de TI. Estos principios se aplican a todos los trabajos, incluidos entre otros, la ética, independencia, objetividad y el debido cuidado profesional de auditoría y aseguramiento de TI, así como el conocimiento, la competencia y la habilidad.

Estándares de desempeño (serie 1200): abordar la realización del trabajo, como la planificación y supervisión, el alcance, la evaluación de riesgo, la movilización de recursos, la gestión del compromiso, la evidencia de auditoría y aseguramiento, y el ejercicio del juicio profesional y el debido cuidado.

Estándares de informes (serie 1400): abordar los tipos de informes, los medios de comunicación y la información comunicada.

Los estándares en ITAF contienen aspectos principales diseñados para ayudar al profesional de aseguramiento y auditoría de TI. Los estándares de ITAF se revisan periódicamente para una mejora continua y se corrigen como es necesario para seguir el ritmo de la evolución de la profesión de aseguramiento y auditoría de TI.

A continuación, se encuentra detallado los estándares de aseguramiento y auditoría TI.

Tabla 2. Estándares

ESTÁNDARES	
Estándares General	
1001 Estatuto de la función de auditoría	
1001.1.	La función de auditoría y aseguramiento de TI documentará la función de la auditoría de manera adecuada en un estatuto de la función de auditoría, indicando propósito, responsabilidad, autoridad y responsabilidad.
1001.2.	La función de aseguramiento y auditoría de TI tendrá que contar con un estatuto de auditoría acordado y formalmente aprobado por aquellos encargados de la gobernanza y de la supervisión de la función de auditoría, por ejemplo, el consejo directivo y/o el comité de auditoría.

1001.3.	La función de aseguramiento y auditoría de TI comunicará el estatuto de la función de auditoría, a los directivos ejecutivos/sénior. Además, elementos relevantes del estatuto de auditoría se compartirán con los grupos que se auditan a la entrada de reuniones y/o a través de cartas de compromiso.	— —
1001.4.	A través de la revisión del estatuto de auditoría de forma periódica, las responsabilidades de la función de aseguramiento y auditoría, como se refleja en el estatuto de auditoría, deben permanecer alineadas con la misión y las estrategias de la empresa. La revisión inmediata del estatuto de auditoría se garantiza si la misión o estrategias de la empresa cambian o si las responsabilidades de la función de auditoría cambian.	— —
1002 Independencia organizacional		
1002.1.	La función de auditoría y aseguramiento de TI debe estar libre de conflictos de interés y de la influencia indebida en todas las cuestiones relacionadas con las asignaciones de auditoría y aseguramiento. Cualquier impedimento a la independencia (de hecho, o apariencia) se identifica y comunica a las partes correspondientes.	— —
1002.2.	La función de aseguramiento y auditoría de TI debe tener una relación de informe funcional (por ejemplo, informar al consejo directivo) que apoya la capacidad de la función para permanecer libre de influencia indebida.	— —
1002.3.	La función de aseguramiento y auditoría de TI debería tener una relación de informe administrativo que soporta el desempeño libre de la función de sus responsabilidades (por ejemplo, ámbito de la asignación, campo de trabajo o informe).	— —
1003 Objetividad del auditor		
1003.1.	Los profesionales de aseguramiento y auditoría de TI deben ser objetivos, en todos los asuntos relacionados con las contrataciones de auditoría y aseguramiento.	— —
1400 Expectativa razonable		
1004.1.		—

Los profesionales de aseguramiento y auditoría de TI deben tener una expectativa razonable de que la asignación pueda ser completada de conformidad con los estándares de auditoría y aseguramiento de TI y, cuando sea necesario, con otras normas de la industria o leyes y reglamentos aplicables que darán lugar a una opinión o conclusión profesional.

Los profesionales de auditoría y aseguramiento de TI deben tener una expectativa razonable de que el alcance de la asignación permita llegar a una conclusión sobre la materia y de que se aborden las limitaciones de alcance.

Los profesionales de aseguramiento y auditoría de TI deben tener una expectativa razonable de que la dirección entienda sus obligaciones y responsabilidades con respecto a proporcionar la información adecuada, pertinente y oportuna necesaria para llevar a cabo la asignación.

1005 Debido cuidado profesional

Conforme con el Código de Ética Profesional de ISACA, los auditores ejercerán la diligencia debida y cuidado profesional. Mantendrán altos estándares de conducta y carácter y evitarán participar en actos que podrían desacreditarles a ellos o a la profesión.

1006 Competencia

Los profesionales de aseguramiento y auditoría de TI, junto con otras personas que ayudan en las actividades de auditoría y el aseguramiento, deben poseer la competencia adecuadas para realizar el trabajo requerido.

TI los profesionales de auditoría y aseguramiento de TI deben poseer el conocimiento adecuado sobre la materia para llevar a cabo sus roles en asignaciones de aseguramiento y auditoría de TI.

Los profesionales de auditoría y aseguramiento de TI deben mantener la competencia profesional a través de una adecuada formación profesional continua.

1007 Afirmaciones

Los profesionales de auditoría y aseguramiento de TI deben revisar las afirmaciones con las que la materia será evaluada para determinar que dichas afirmaciones sean capaces de ser auditadas y que las afirmaciones sean suficientes,

1700.1. válidas y relevantes

1800 Criterios

Los profesionales de aseguramiento y auditoría de TI deben seleccionar los criterios con los que se evaluará la materia, que sean objetivos, completos, relevantes, fiables, medibles, comprensibles, ampliamente reconocidos, autorizados y comprendidos por, o disponibles para, todos los lectores y usuarios del

1800.1. informe.

Los profesionales de aseguramiento y auditoría de TI deben considerar la aceptabilidad de los criterios y centrarse en criterios que están reconocidos, son autorizados y están públicamente

1800.2. disponibles.

Estándares de Desempeño

1201 Evaluación de riesgo en la planificación

La función de auditoría y aseguramiento de TI debe utilizar un enfoque de evaluación de riesgo adecuado (por ejemplo, basado en datos con factores cuantitativos y cualitativos) y una metodología de apoyo para desarrollar el plan de auditoría general de TI y determinar las prioridades para la asignación efectiva

1201.1. de los recursos de auditoría de TI.

Los profesionales de auditoría y aseguramiento de TI deben identificar y evaluar el riesgo relevante al área de revisión,

1201.2. cuando planifican actividades individuales.

Los profesionales de auditoría y aseguramiento de TI deben considerar el riesgo de la materia, el riesgo de la auditoría

1201.3. y la exposición relativa de la empresa al planificar actividades de auditoría

1202 Programación de auditorías

1202.1.

	La función de aseguramiento y auditoría de TI debe establecer un plan estratégico integral que resulte en calendarios de auditoría de corto y largo plazo. La planificación a corto plazo consiste en la realización de auditorías dentro del año, mientras que la planificación a largo plazo está constituida por auditorías basadas en temas relacionados con el riesgo dentro del entorno de tecnología de la información (TI) de la empresa que podrían realizarse en el futuro.	
1202.2.	La mayoría de los calendarios a corto plazo y largo plazo deberían acordarse con aquellos encargados de la gobernanza y supervisión (por ejemplo, comité de auditoría) y comunicarse dentro de la empresa.	— —
1202.3.	La función de aseguramiento y auditoría de TI debe modificar sus calendarios de auditoría a corto y largo plazo para que respondan a las necesidades organizativas (por ejemplo, eventos inesperados o iniciativas no planificadas).	— —
1203 Planificación de la asignación		
1203.1.	Los profesionales de aseguramiento y auditoría de TI deben planificar cada asignación de auditoría y aseguramiento de TI para abordar la naturaleza, el cronograma y el alcance de los procedimientos de auditoría que se deben llevar a cabo.	— —
1203.2.	Los profesionales de aseguramiento y auditoría de TI deben desarrollar y documentar un programa de auditoría de las asignaciones de auditoría y aseguramiento de TI que describa los procedimientos paso a paso y las instrucciones que deben usarse para completar la auditoría.	— —
1204 Desempeño y supervisión		
1204.1.	Los profesionales de auditoría y aseguramiento de TI deben llevar a cabo el trabajo en conformidad con el plan de auditoría de TI aprobado para cubrir el riesgo identificado y dentro del cronograma acordado.	— —
1204.2.	Los profesionales de auditoría y aseguramiento de TI deben proporcionar supervisión al personal de auditoría de TI	— —

	sobre quienes tienen responsabilidad de supervisión, para lograr los objetivos de la auditoría y cumplir con los estándares de auditoría profesional aplicables.	
1204.3.	Los profesionales de aseguramiento y auditoría de TI deben aceptar solo tareas que estén dentro de su conocimiento y habilidades o para las que tengan una expectativa razonable de adquirir las habilidades durante la asignación o lograr la tarea bajo supervisión.	
1204.4.	Los profesionales de auditoría y aseguramiento de TI deben obtener evidencia suficiente y apropiada para lograr los objetivos de la auditoría.	
1204.5.	Los profesionales de auditoría y aseguramiento de TI deben documentar el proceso de auditoría y describir el trabajo de auditoría y la evidencia de auditoría que respalda los hallazgos y las conclusiones.	
1204.6.	Los hallazgos y las conclusiones del profesional de aseguramiento y auditoría de TI deben estar respaldados por un análisis e interpretación apropiados de la causa raíz de esta evidencia.	
1204.7.	Los profesionales de auditoría y aseguramiento de TI deben brindar una opinión o conclusión de la auditoría apropiada e incluir cualquier limitación del alcance cuando no se obtenga la evidencia requerida mediante los procedimientos de prueba adicionales.	
1205 Evidencia		
1205.1.	Los profesionales de auditoría y aseguramiento de TI deben obtener evidencia suficiente y apropiada para extraer conclusiones razonables.	
1205.2.	Aplicando el escepticismo profesional, los profesionales de auditoría y garantía de TI evaluarán la suficiencia de las pruebas obtenidas para apoyar las conclusiones y alcanzar los objetivos de la asignación.	
1205.3.	Junto con otros papeles de trabajo, los profesionales de aseguramiento y auditoría de TI deben preservar la evidencia	

durante un periodo de tiempo que se corresponda con periodos de retención aprobados y formalmente definidos.

1206 Uso del trabajo de otros expertos

Los profesionales de auditoría y aseguramiento de TI deben considerar el uso del trabajo de otros expertos para la
1206.1. asignación, cuando sea apropiado.

Los profesionales de auditoría y aseguramiento de TI deben evaluar y aprobar la idoneidad de las calificaciones profesionales, competencias, experiencia relevante, recursos, independencia y procesos de control de calidad de otros expertos
1206.2. antes de la asignación.

Los profesionales de auditoría y aseguramiento de TI deben evaluar, revisar y valorar el trabajo de otros expertos como parte de la asignación, y documentar la conclusión sobre el uso y la
1206.3. confianza en su trabajo.

Los profesionales de auditoría y aseguramiento de TI deben determinar si el trabajo de otros expertos, que no forman parte del equipo de asignación, es adecuado y completo para concluir acerca de los objetivos de la asignación actual. Los
1206.4. profesionales deben también documentar la claramente la conclusión.

Los profesionales de auditoría y aseguramiento de TI deben determinar si se podrá depender del trabajo de otros expertos y se incorporará directamente o se hará referencia al mismo de
1206.5. manera separada en el informe.

Los profesionales de auditoría y aseguramiento de TI deben aplicar procedimientos adicionales de prueba para obtener evidencia suficiente y apropiada en los casos en que el trabajo de otros
1206.6. expertos no brinde evidencia suficiente y apropiada.

Los profesionales de auditoría y aseguramiento de TI deben brindar una opinión o conclusión de la auditoría e incluir cualquier limitación del alcance cuando no se obtenga la evidencia requerida mediante los procedimientos de prueba
1206.7. adicionales.

1207 Irregularidades y actos ilegales	
1207.1.	Los profesionales de aseguramiento y auditoría de TI deben considerar el riesgo de irregularidades y actos ilegales durante la asignación.
1207.2.	Los profesionales de aseguramiento y auditoría de TI deben documentar y comunicar, de manera oportuna, cualquier acto ilegal o irregularidad material a la parte correspondiente.
ÉSTANDARES DE INFORMES	
1401 Generación de informes	
1401.1.	Los profesionales de aseguramiento y auditoría de TI deben proporcionar un informe para comunicar los resultados al concluir la asignación.
1401.2.	Los profesionales de aseguramiento y auditoría de TI deben garantizar que los hallazgos en el informe de auditoría estén respaldados por evidencia suficiente y apropiada.
1402 Actividades de seguimiento	
1402.1.	Los profesionales de aseguramiento y auditoría de TI deberían controlar y reportar periódicamente a aquellos encargados de la gobernanza y supervisión del progreso de la dirección de la función de auditoría (por ejemplo, el consejo directivo y/o el comité de auditoría) sobre hallazgos y recomendaciones.
1402.2.	El progreso sobre el estado general de la implementación de los hallazgos de la auditoría debería reportarse regularmente al comité de auditoría, si está establecido.
1402.3.	Bien se determine que el riesgo relacionado con un hallazgo se ha aceptado y es superior al apetito de riesgo de la empresa, esta aceptación del riesgo debe comentarse con la dirección superior. La aceptación del riesgo (en particular, el fallo para resolver el riesgo) debe someterse a la atención del comité de auditoría (si está establecido) y/o el consejo directivo.

Nota: Tomado de (ISACA, 2020), elaboración propia.

3.2. ITAF, y su aplicación en los outsourcing contables

La aplicación del ITAF tiene el objetivo de aplicar procedimientos que permitan realizar el registro de la información de forma razonable y segura, esto debido a que los outsourcing contables son empresas que brinda servicios como asesoramiento de consultoría en diferentes áreas como nomina, tributarios, contables y/o financieros, entre otros.

La aplicación de normas de información financiera como la NIIF, temas tributarios, legales y de actualidad relacionados a leyes laborales exige que los outsourcing contables cuenten con personal experimentado que pueda asesorar, dirigir y desarrollar procesos sean administrativos y contables en las empresas que confiaron en su propuesta de servicio, además de contar con herramientas tecnológicas que ayuden de forma eficiente en el procesamiento de la información.

Por lo mencionado antes, es importante que el staff contable pueda seguir ciertas directrices, procedimientos y cumplimiento de normas, como la ISO27001 que habla sobre la seguridad de la información en las empresas, y que las mismas tienen como objetivo certificarse en el cumplimiento de esta ya que brinda una seguridad en los procesos que realiza la compañía con sus clientes.

De igual forma, la aplicación de ITAF en los outsourcing contables es una propuesta de control interno, ya que actualmente no existe un reglamento donde esto sea obligatorio para las entidades, sin embargo, las personas jurídicas que contratan el servicio de staff son en su gran mayoría empresas de diferentes regímenes tributarios como pueden ser régimen de microempresa actualmente régimen negocio popular, régimen general que dentro de ellos se encuentra los agentes de retenciones y los contribuyentes especiales.

3.3. Análisis de los sistemas

3.3.1. Objetivos del análisis de los sistemas contables

En el análisis del sistema contable es necesario verificar si la información procesada en el sistema se genera de acuerdo con los estándares establecidos por la empresa.

Una revisión de estos sistemas debe centrarse en lograr los siguientes objetivos:

Garantizar la integridad de los datos:

Garantizar que todas las transacciones sean registradas y generadas eficientemente en la base de datos; para ello, la organización necesita establecer controles en varios niveles para que los datos de entrada soporten las transacciones.

Garantizar el correcto registro y procesamiento de las transacciones:

Confirme que todas las transacciones se realicen de acuerdo con las leyes y regulaciones locales y los procedimientos internos de la empresa.

Proporcionar información financiera de forma fiable:

La información que genere el sistema contable debe ser veraz y oportuna, los informes deben ser seguros y confiables, y además deben estar debidamente presentados de acuerdo con las normas y principios contables.

Capacidad garantizada para presentar información. Es imperativo asegurar que la información contable se genere y proporcione en tiempo y forma para que las decisiones que tome la gerencia sean efectivas, eficientes.

3.3.2. Sistemas Contables

Es importante analizar los diferentes softwares contables que se mencionó anteriormente, esto con el fin de realizar un análisis con los objetivos que debería lograr los sistemas informáticos al momento de realizar una revisión.

Datil. - es un software de facturación que cuenta con una adaptabilidad para diferentes tipos de negocios, es importante destacar que esta plataforma cuenta como un proveedor autorizado de facturación electrónica.

Por otra parte, dátil es una plataforma que tiene una conexión directa con el Servicio de Rentas Internas (SRI) por lo cual existe una confiabilidad en el registro de datos en la plataforma, sin embargo, es importante mantener constantes controles.

El uso de la plataforma es en gran medida la facturación electrónica, sin embargo, en temas de control de sistemas informáticos es una plataforma que puede ser usadas por diferentes usuarios sin un control sobre el mismo, ya que adicional no cuenta con algún módulo de auditoría que permita identificar modificaciones o manipulación de la información como tal.

Latinium. - es un software para registros contables, emisión de balances, reportes de compras, anexo ATS, además que permite autorizar documentos electrónicos ante el SRI.

Este software garantiza el correcto registro de las diferentes transacciones, sin embargo, la persona que lo maneja debe entender el sistema para un correcto uso de este.

Adicional, latinium es un sistema contable que cuenta con diferentes controles, en primera instancia cada individuo debe contar con su propio usuario, además de que a este se le otorgan diferentes tipos de acceso de acuerdo con lo solicitado por parte de gerencia, también cuenta con módulo de control como es el de auditoría y el módulo de accesos en el cual se puede bloquear el reescribir información lo cual permite que la información contable se encuentre de alguna forma más segura.

SAP. – el sistema contable SAP es un sistema bastante conocido en el mercado y dentro de las diferentes organizaciones, este sistema que tiene diferentes funciones como la emisión de balances, registros contables, entre otros.

Este sistema contable a diferencia de los anteriormente mencionados cuenta con una gran variedad de módulos, como por ejemplo modulo bancos, reconciliación interna de facturación, módulo de socios de negocio, entre otros.

Al igual que otros sistemas se crean usuarios para el ingreso de la información los cuales tienen restricciones en ciertas configuraciones y módulos, se puede decir que el SAP es un sistema diferente a los otros mencionados ya que, por ejemplo, no se pueden realizar

modificaciones sobre la información ya ingresada lo cual permite que la información sea fiable y confiable.

Es importante destacar, que existen diversos sistemas contables en el mercado, sin embargo, se ha mencionado los tres sistemas que se ha podido identificar sus características principales.

Los sistemas contables como se ha detallado en diversas ocasiones son un activo fundamental para la compañía y por ello existen diferentes controles y normativas a seguir con el fin de poder mantener un orden y como resultado una garantía de la información.

A modo de conclusión, sobre la seguridad de los sistemas contables se puede identificar que como todos cuentan con un usuario y contraseña para acceder al mismo, no obstante, se evidencio que en los dos últimos sistemas existes un control un poco más fuerte esto debido a que el usuario que cuenta la personal debe ser personal, lo cual permiten a que personas internas puedan obtener información sobre los procesos realizados para cada usuario, pero este no se encuentra libre de vulnerabilidad ya sea porque existe intercambio de información de usuarios o por robo de información.

3.4. Propuesta de buenas prácticas en el manejo de TI en los outsourcing contables

En todas las empresas se puede encontrar un área TIC o Oficina de Tecnologías de la Información y las Comunicaciones, la cual se encarga de la gestión de los sistemas de información, gestión de procesos y procedimientos, redes de telecomunicaciones y todas las tecnologías vigentes en la organización. También son responsables de brindar un soporte adecuado y adecuado a los componentes técnicos como portales, micrositiros, intranet, sistemas de contabilidad y sistemas de beneficios, así como mantener a la organización en el camino correcto a través de la gestión de mejora continua, así como interna y externa.

Las organizaciones año a año planifican un presupuesto para proteger la información que la empresa adquiere, sea esta medidas de seguridad y protección como actualizaciones del sistema operativo, instalaciones de antivirus o configuraciones de dispositivos de seguridad como firewalls, ID, IP o cualquier cosa que ayude a proteger contra amenazas,

aunque siempre habrá una brecha de seguridad que comprometa la información de cualquier empresa, por lo que es recomendable educar, capacitar e informar a los trabajadores, clientes internos y externos, ya que son los eslabones más débiles de la cadena de seguridad.

Objetivos Generales y específicos

Objetivo General

Ofrecer al lector una guía de buenas prácticas para el manejo de TI de los sistemas informáticos.

Objetivos Específicos

- Disminuir el riesgo de errores de uso de sistemas contables
- Reducir el riesgo mediante el uso de TI para actividades que no sean el objetivo principal de la adquisición.

Alcance

La propuesta para el aseguramiento de buenas prácticas para los sistemas informáticos tiene como objetivo abordar alegaciones específicas relacionadas con el manejo de las TIC en la gestión, procedimiento o proceso dentro de una empresa a través de la prevención y evaluación de los diferentes “hardware” y “software”.

3.4.1. Criterios profesionales sobre la seguridad a sistemas contables

El outsourcing contable es la transferencia del control operacional de las organizaciones, el cual tiene un importante grado de autonomía para llevar a cabo ofreciendo a sus clientes resultados de calidad. La principal ventaja de un outsourcing es la reducción de costos en las empresas, ya que les permite enfocarse en la actividad principal del negocio.

Es importante que, la externalización de servicios contables cuente con:

- Staff experimentado
- Conocimiento de normas y leyes
- Servicios como Precios de Transferencia, Nomina, Tax, entre otros.
- Herramientas tecnológicas
- Manejo de sistemas contables operativos, entre otros.

Las preguntas que encuentran a continuación son relacionadas a la seguridad sobre los programas de TI (tecnología informática) dentro de una organización, ya que lo mismos son de gran importancia para la operatividad de estas, y por ello es recomendable capacitar al personal sobre buenas prácticas aplicadas a los sistemas o programas contables.

A continuación, se encontrarán las opiniones profesionales:

Nombre: Alejandra Acurio

- ¿Dentro de su trayectoria como profesional contable cual ha sido el programa o sistema contable que considera más le ha sido más útil en sus actividades?
Sap porque es un ERP en el cual se puede simplificar e integrar procesos que te permiten establecer indicadores para la toma de decisiones oportunas y tener una visión global de la compañía.
- ¿Cuál es su opinión al respecto del programa contable Latiniium o Sap?
Sap es un sistema completo que al ser manejado de manera adecuada es una herramienta que nos permite integrar las áreas de la empresa simplificando procesos que permitirá profundizar análisis y toma de decisiones de manera oportuna, eficaz y eficiente.
- ¿Considera usted que los programas contables que ha utilizado en sus diferentes actividades profesionales cuentan disponen de las seguridades óptimas para la protección de los datos y de la información tratada?Cuál es el programa que considera ofrece mejores garantías de seguridad informática contable.

- Los sistemas que he manejado si han tenido algunas vulnerabilidades en protección de información y en el manejo de usuarios para el acceso de informaciones y permisos de funcionamiento. Considero que Sap es un sistema que ofrece mayores garantías de seguridad.

Nombre: Daniela Vega

- ¿Dentro de su trayectoria como profesional contable cual ha sido el programa o sistema contable que considera más le ha sido más útil en sus actividades?

SAP

- ¿Cuál es su opinión al respecto del programa contable Latinium o Sap?

SAP excelente pero ciertos problemas para configurar reportes específicos. Problemas generales con la implementación del anexo locales como ATS – Latinium ciertas falencias en reportes simples como detalles de cxc o cxp

- ¿Considera usted que los programas contables que ha utilizado en sus diferentes actividades profesionales cuentan disponen de las seguridades óptimas para la protección de los datos y de la información tratada?Cuál es el programa que considera ofrece mejores garantías de seguridad informática contable.

SAP

Nombre: Angie Gallardo

- ¿Dentro de su trayectoria como profesional contable cual ha sido el programa o sistema contable que considera más le ha sido más útil en sus actividades?

SAP Business One

- ¿Cuál es su opinión al respecto del programa contable Latiniun o Sap?

Sap, es un programa muy completo, cuenta con todos los módulos y reportes necesarios para la correcta visibilidad de información, precisa, clara y completa de cada aspecto de la operación.

- ¿Considera usted que los programas contables que ha utilizado en sus diferentes actividades profesionales cuentan disponen de las seguridades óptimas para la protección de los datos y de la información tratada? Cuál es el programa que considera ofrece mejores garantías de seguridad informática contable.

A lo largo de mi vida profesional he tenido la oportunidad de manejar diversos Sistemas Contables, los mismos que en ocasiones sufren deficiencias en la seguridad de la información y confiabilidad.

Sap, por otro lado, cuenta con todas las seguridades en sus módulos y reportes necesarios para la correcta recopilación de datos de manera automatizada, segura y confidencial.

Nombre: Diego Vinueza

- ¿Dentro de su trayectoria como profesional contable cual ha sido el programa o sistema contable que considera más le ha sido más útil en sus actividades?

Considero que un sistema contable estaría completo si es parte de un ERP, debido a que tiene comunicación directa con los módulos de la organización desde el reconocimiento de horas extras de manera automática en nómina hasta alertas para declaración de impuestos. Por experiencia los programas que más se adaptan a las necesidades de las empresas son los desarrollados por las mismas. Un ejemplo de lo antes mencionado es la Compañía Kruger corporation, la misma que utiliza el sistema Kruger

- ¿Cuál es su opinión al respecto del programa contable Latinium o Sap?

Latinium, es muy amigable en cuanto a su uso, pero no es robusto en sus módulos y seguridades. Por lo general es observado por las auditorias informáticas que se le hacen. SAP, depende del desarrollo en cada compañía y los costos de desarrollo son elevados. No es muy amigable en su uso.

- ¿Considera usted que los programas contables que ha utilizado en sus diferentes actividades profesionales cuentan disponen de las seguridades óptimas para la protección de los datos y de la información tratada?Cuál es el programa que considera ofrece mejores garantías de seguridad informática contable.

Actualmente en mi trabajo las seguridades de protección de datos y de información se la realiza conforme la ISO 27001 que permite el aseguramiento, la confidencialidad e integridad de los datos y de la información, así como de los sistemas que la procesan.

Nombre: Ricardo Cisneros

- ¿Dentro de su trayectoria como profesional contable cual ha sido el programa o sistema contable que considera más le ha sido más útil en sus actividades?

En mi trayectoria como profesional he manejado varios sistemas contables para el control de los registros y presentación de estados financieros. El programa que me ha sido de mayor utilidad, dentro de mi vida profesional, ha sido el sistema NETSUITE de Oracle.

- ¿Cuál es su opinión al respecto del programa contable Latinium o Sap?

El sistema Latinium mantiene una configuración útil para los módulos de control de compras, ventas, inventarios, impuestos, Activos fijos entre otros, sin embargo, debido a la actualización de los sistemas contables, existen nuevas herramientas online, que permiten el uso de una red de servidores remotos conectados a internet para almacenar, administrar y procesar datos, desde cualquier punto de acceso a la red. Esto sin lugar a duda, es una ventaja competitiva de cualquier sistema contable, permitiendo ingresar a la información contable y financiera de las empresas, desde cualquier punto o dispositivo de acceso a Internet, con el fin de tomar decisiones de manera oportuna.

- ¿Considera usted que los programas contables que ha utilizado en sus diferentes actividades profesionales cuentan disponen de las seguridades óptimas para la protección de los datos y de la información tratada?Cuál es el programa que considera ofrece mejores garantías de seguridad informática contable.

Cada sistema contable mantiene su nivel de seguridad, sin embargo, existen sistemas de seguridad de información basado en procesos y jerarquías de aprobación que permiten que la información, materia prima de los Estados financieros, sea segura y confiable. Un ejemplo claro de esto es el sistema contable SAP.

Nombre: Mara Zamora

- ¿Dentro de su trayectoria como profesional contable cual ha sido el programa o sistema contable que considera más le ha sido más útil en sus actividades?

Los sistemas contables Latinium, MBA3 y SAP.

- ¿Cuál es su opinión al respecto del programa contable Latinium o Sap?

Los 2 me parecen buenos sistemas de acuerdo con la operatividad del negocio, Latinium creo que es más amigable con el usuario por lo cual el manejo de él a mi criterio es de preferencia, en cambio en SAP al estar enlazado a varias rutas en varios casos no es amigable y deben hacerse varios desarrollos para poder obtener más bondades del mismo.

- ¿Considera usted que los programas contables que ha utilizado en sus diferentes actividades profesionales cuentan disponen de las seguridades óptimas para la protección de los datos y de la información tratada?Cuál es el programa que considera ofrece mejores garantías de seguridad informática contable.

Si, en su mayoría si. SAP por las limitaciones de accesos.

Nombre: Leonardo Murillo

- ¿Dentro de su trayectoria como profesional contable cual ha sido el programa o sistema contable que considera más le ha sido más útil en sus actividades?

HubSpot, es un desarrollador y comercializador de productos de software que ofrece una suite completa de herramientas de contables, es de fácil acceso y amigable con el entendimiento para los usuarios que son empresas de todo tamaño.

El software CRM contable que ofrece es un programa de gestión informática que ayuda a los contadores, contables y áreas afines a recopilar y organizar los datos de los clientes para agilizar intercambios de documentos, actualizaciones de ventas y otras tareas clave.

- ¿Cuál es su opinión al respecto del programa contable Latinium o Sap?

Latinium me parece muy elemental debido a que sus bases son hechas en Excel y no tiene muchos controles en los análisis financieros en cuanto a la formulación y restricción de datos.

- ¿Considera usted que los programas contables que ha utilizado en sus diferentes actividades profesionales cuentan disponen de las seguridades óptimas para la protección de los datos y de la información tratada?Cuál es el programa que considera ofrece mejores garantías de seguridad informática contable.

En cuanto a seguridad HubSpot me parece seguro por ser tener sus bases internacionales y con muchos certificados que respaldan la seguridad de sus clientes. Poseen servidores de máxima seguridad.

Nombre: José Luis Perero

•¿Dentro de su trayectoria como profesional contable cual ha sido el programa o sistema contable que considera más le ha sido más útil en sus actividades?

Sap Business One, de acuerdo a la parametrización es una amplia herramienta de datos para armar dashboards y procesos se control en temas contables y de manejo de información, con ello se puede analizar decisiones.

•¿Cuál es su opinión al respecto del programa contable Latinium o Sap?

La base de datos latinium no integra procesos de seguridad en cuanto a correcciones y trazabilidad de errores, SAP lleva un proceso de auditorías de datos con hora y fecha que permite ubicar el responsable y el porqué de los cambios o modificaciones en cada registro, adicional integra controles de información mínima para crear asientos o registros contables.

•¿Considera usted que los programas contables que ha utilizado en sus diferentes actividades profesionales cuentan disponen de las seguridades óptimas para la protección de los datos y de la información tratada?Cuál es el programa que considera ofrece mejores garantías de seguridad informática contable.

Si, considero que llevar la información en nube y que se integre a nuevos sistemas contables en un caso de transiciones de sistemas contribuye a manejar de manera eficiente la información, adicional de bloquear toda modificación en la estructura del asiento o registro y tener accesos de seguridad que apliquen permisión por niveles se permitirá medir de manera fiable la información.

Nombre: Andrés Santamaria

•¿Dentro de su trayectoria como profesional contable cual ha sido el programa o sistema contable que considera más le ha sido más útil en sus actividades?

- SAP
- SAP HANA
- SAP B1
- POWER BI
- ALTERYX

•¿Cuál es su opinión al respecto del programa contable Latinium o Sap?

Es uno de los mejores ERP en el mercado actualmente

•¿Considera usted que los programas contables que ha utilizado en sus diferentes actividades profesionales cuentan disponen de las seguridades óptimas para la protección de los datos y de la información tratada?Cuál es el programa que considera ofrece mejores garantías de seguridad informática contable.

SAP ofrece la capacidad de conectarse con servidores privados tanto físicos como digitales en los cuales se puede implementar mecanismos de seguridad implementados con otros softwares especializados para la seguridad informática.

Nombre: Mayra Badillo

•¿Dentro de su trayectoria como profesional contable cual ha sido el programa o sistema contable que considera más le ha sido más útil en sus actividades?

Sap Business One, ya que dependiendo de la parametrización inicial que tenga el programa o el que se le quiera dar al mismo, el software en cuestión puede llegar a ser de gran utilidad para los negocios y/o empresas que adquieran el mismo.

•¿Cuál es su opinión al respecto del programa contable Latinium o Sap?

Latinium es un gran software contable, ya que brinda diferentes módulos que pueden ser utilizados con el fin de detallar la información contable, sin embargo, no considero que el sistema sea el mas seguro en cuanto a seguridad de la información. SAP por el otro lado cuenta con diferentes módulos contables que pueden llegar a ser engorrosos para el usuario, pero a diferencia de Latinium, Sap cuenta con mayor seguridad de la información ya que, no permite la modificación de la misma.

•¿Considera usted que los programas contables que ha utilizado en sus diferentes actividades profesionales cuentan disponen de las seguridades óptimas para la protección de los datos y de la información tratada?Cuál es el programa que considera ofrece mejores garantías de seguridad informática contable.

Considero que los programas contables y los softwares en general cuentan con un nivel de seguridad relativamente alto, en mi experiencia profesional Sap es el mejor software con el cual se puede manejar un negocio y/o empresa.

3.4.2. Perfil del Outsourcing Contable

El outsourcing contable es la subcontratación de procesos contables administrativos que implica el uso de firmas externas especializadas para brindar servicios en áreas que no son procesos críticos de la organización.

Es importante que los outsourcing contables puedan obtener certificaciones como la ISO27001 y la ISO27005, ya que dentro de estas dos normas se espera realizar un proceso sistemático que sea documentado y conocido a nivel de toda la organización. El certificarse para las organizaciones ayuda a que las organizaciones puedan determinar procesos, normas y procedimientos que ayuden a proteger la información de esta.

Debe realizarse seguimientos mediante auditorias anuales o semestrales que tengan como objetivo la mejora continua. Adicional, es importante que las organizaciones implementen sistemas de seguridad a la información.

Por otro lado, es importante que se sensibilice el usuario sobre los riesgos de seguridad informática. Además, contar con procesos debidamente estructurados para el uso y correcto manejo de los diversos sistemas contables.

Obtener certificaciones de seguridad a la información dictadas por la ISO.

Disponer de un departamento de seguridad informática encargados sobre la ciberseguridad de la organización para brindar soportes adecuados al mismo. Las personas encargadas de la ciberseguridad puede ser un experto en auditoria o a su vez contar con profesionales contables, que cuente con los siguientes requisitos:

- Principios y Valores Morales y Éticos
- Seguridad en sí mismo
- Capacidad Estratégica, Analítica y Crítica
- Buena Presentación y Arreglo Personal
- Independiente

En general, el profesional debe de contar con principios y valores como es la honestidad, ética y curiosidad; además de contar con una gran capacidad analítica y una buena presentación.

En cuanto a conocimiento se refiere el o los profesionales encargados deberán conocer y de manera preferible dominar distintos programas que son usados dentro de las organizaciones. Además, el profesional deberá tener conocimiento y experticia en normativa referente a la auditoría externa, auditoría a sistemas informáticos, y normativa local relacionada con esta prestación de servicios.

En términos generales la persona encargada de ciberseguridad deberá contar de preferencia con los siguientes conocimientos:

Dominio de la normativa ITAF, NIAS, NIC, NIFF, Normativas Locales, además de conocimiento en IASB y IESBA.

ITAF, NIC, NIAS y NIFF son normativas internacionales que deben ser aplicadas en su totalidad para poder realizar una auditoría a sistemas de información, ya que aportan con conceptos y procedimientos en diferentes situaciones que pudiesen suscitarse dentro del ejercicio profesional.

3.4.3. Propuesta de buenas prácticas aplicado al área de servicio accounting

Para poder establecer buenas prácticas, es importante identificar el objetivo y aquellas actividades que realiza el área de accounting, el cual podría ser relacionado al mantener y efectuar libros contables de las diferentes compañías con la correcta aplicación de las normas vigentes en el Ecuador y a su vez políticas contables para la emisión de estados financieros sean estos mensuales o anuales.

Actualmente el área de servicio de accounting cuenta con diversas funciones, sin embargo, la mayoría de las actividades que realiza necesitan de un sistema contable que les permita realizar:

- Registros contables de la información

- Revisión de los documentos o datos ingresados en el sistema
- contabilización de reembolsos
- Registro de transacciones de acuerdo con las políticas contables
- Organizar un archivo físico y digital de la información
- Registros contables de nomina
- Depreciaciones de activos fijos
- Registro y contabilización de pagos
- Emisión o autorización de documentos como facturas de venta y liquidaciones
- Emisión de notas de crédito
- Emisión de retenciones
- Conciliación de transacciones efectuadas
- Descarga de diferentes reportes
- Emisión de ATS (Anexo Transaccional Simplificado)
- Elaboración de impuestos y declaraciones

De acuerdo con las actividades anteriormente se propone implementar los siguientes controles y/o actividades para efectuar de manera correcta los servicios:

- Según el sistema contable que utilice la organización se deberá establecer actividades y procedimientos a cada integrante de la organización o área de accounting, adicional deberá contara con un usuario independiente, el mismo dependiendo del nivel de experiencia contara con diferentes accesos en el sistema contable y/o accesos limitados.
- De acuerdo con lo mencionado en el párrafo anterior, será importante acordar cuáles serán las funciones por cumplir dentro de la organización, esto dependerá mucho su nivel de conocimiento y puesto para el que se le haya contratado dentro de la empresa, el mismo puede ser pasante, asistente, semi-senior, senior, supervisor y gerente, será importante determinar las actividades que desarrolla cada persona a su cargo.

- Los usuarios deberán tener un conocimiento previo del manejo del sistema, en cuanto a los módulos de cada sistema, esto será fundamental, ya que un entendimiento previo permitirá que el usuario pueda ser eficiente en el manejo del sistema contable, por lo cual se recomienda que la organización cuente con capacitaciones para el entendimiento del sistema.
- Los usuarios no podrán compartir sus claves y contraseñas, ya que los mismos deberán ser de uso personal, por lo cual no debe de ser compartido con terceros, incluso dentro de la organización.
- Se recomienda no ingresar a páginas web o sitios web que no sean de uso de trabajo. Además, se recomienda que la organización pueda limitar accesos a páginas web que puedan generar virus.
- La información proporcionada por el cliente deberá ser manejada con confidencialidad y a su vez archivada en la red de la empresa, en el caso de ser digital y en carpetas si la misma es física.
- La o las personas que cuenten con un usuario y contraseña deberán tener una conexión de red privada virtual (VPN), que permita tener acceso a la red de información de documentos electrónicos e internet.
- En caso de realizar trabajo virtual o realizar actividades fuera de la organización se recomienda evitar la conexión a redes públicas de internet wifi, ya que existe una brecha de seguridad.
- Se recomienda que ante un desconocimiento del sistema por parte de colaboradores estos no manipulen los diferentes módulos, ya que el uso incorrecto de información puede ocasionar errores materiales para la organización.
- Se recomienda que, al finalizar cierres mensuales dentro del sistema contable, este sea bloqueado una vez se haya realizado el cierre con el fin de evitar posibles modificaciones.

- Es importante que el sistema contable cuente con un módulo de auditoría que permita identificar los cambios realizados por los diferentes usuarios, y que este además cuente con fecha y hora de las modificaciones para reconocer responsables.

- Se recomienda que al finalizar el mes se maneje un detalle de los usuarios, de acuerdo con los registros realizados y cambios que se hayan hecho en los mismo, esto con el fin de brindar un control periódico.

- Se recomienda que al momento que un usuario requiera tener acceso a módulos del sistema contable, esto se maneje con aprobaciones previas de un superior.

4. CONCLUSIONES Y RECOMENDACIONES

4.1. Conclusiones

La auditoría de sistemas de información tiene como objetivo comprobar y revisar que la información que se maneja a través de diferentes medios informáticos tenga una estabilidad básica para reducir la posibilidad de peligro de fuga, mala implementación de la información y/o dependencia excesiva de las TIC.

Dado el carácter confidencial de los trabajos que realizan los auditores externos para las empresas, es difícil encontrar información referente a los sistemas informáticos de diversas organizaciones, por lo que se optó por realizar preguntas relacionados a los sistemas contables Latinium y SAP de acuerdo con su experiencia profesionales

La mayoría de los profesionales encuestados llegaron a la conclusión de que uno de los sistemas contables más favorables es el sistema SAP, ya que el mismo cuenta con diferentes protecciones a nivel de módulos que permite que la información de una organización se mantenga de forma segura y además que el sistema en mención ayuda al buen funcionamiento de diversas áreas de recursos humanos comerciales, contables o corporativas. Además, en base a los criterios profesionales se puede identificar que uno de los mejores sistemas contables es aquel que la misma organización lo localice de acuerdo con sus necesidades como empresa.

También se puede concluir que una auditoría de sistemas informáticos reduce el riesgo de sufrir interferencias no deseadas con las TIC, pero no lo elimina, porque siempre existe la posibilidad de experimentar interferencias no deseadas

4.2. Recomendaciones

Realizar auditorías internas periódicas con el fin de descubrir oportunamente los riesgos relacionados con los sistemas de información de la empresa y tomar medidas de contingencia en caso de que ocurran dichos incidentes.

Invertir en seguridad informática es la opción más lógica e idealmente reduce cualquier tipo de ciberataque que pueda surgir.

La creación de un comité de auditoría o un departamento de auditoría interna ayudará en gran medida a evitar ignorar los temas cibernéticos, ya que mantener un control adecuado sobre las TIC dentro de la organización facilitará lograr o lograr una mayor rentabilidad en el mercado, reduciendo costos como el laboral y evitando quedar atrapados en una situación insostenible. cargo gastos necesarios.

Hoy en día, con el desarrollo de la tecnología, es difícil mantenerse a la vanguardia, pero es recomendable mantenerse en constante capacitación en temas tecnológicos de nuevos programas que habiliten las tareas diarias o actualizar el software existente. para obtener el mayor beneficio de ellos.

Referencias bibliográficas:

- Accountants, I. F., Committee, I. A., & (IMCP), I. M. (2022). *NIA15: Auditoría en un Ambiente de Sistemas de Información por Computadora*. NIA15: Auditoría en un Ambiente de Sistemas de Información por Computadora: file:///C:/Users/coelloi/Downloads/NIA%2015_%20Auditor%C3%ADa%20en%20un%20Ambiente%20de%20Sistemas%20de%20Sec.%20401%20Informaci%C3%B3n%20por%20Computadora.pdf
- Accountants, I. F., Committee, I. A., & Públicos, I. M. (2022). *NIA 16: Técnicas de Auditoría con Ayuda de Computadora*. NIA 16: Técnicas de Auditoría con Ayuda de Computadora: file:///C:/Users/coelloi/Downloads/NIA%2016%20_%20T%C3%A9cnicas%20de%20Auditor%C3%ADa%20con%20Ayuda%20de%20Computadora%20Sec.%201009%20(Reemplazada)%20T%C3%A9cnicas%20de%20Auditor%C3%ADa%20con%20Ayuda%20de%20Computadora%20(Reemplazada)%20NIA%2016.pdf
- Aguirre, Y. (2022). *Propuesta de implantación del área de auditoría en informática en un órgano legislativo*. <https://olea.org/~yuri/propuesta-implantacion-auditoria-informatica-organo-legislativo/index.html>
- Alcívar, Brito, & Guerrero. (2016). Auditoría en las Empresas. *Revista Académica: Contribución a la Economía*, 3.
- Espinoza, J. J., Abad, C. R., Castillo, L. F., & Villavicencio, O. E. (2017). Sistema cobit en los procesos de auditorías de los sistemas informáticos. *REVISTA CIENCIA E INVESTIGACIÓN*, 3.
- Factory, S. (s.f.). *PC.Gerente*. Programa Contable: <https://pcgerente.com/programas-contables-mas-utilizados-en-ecuador/>
- G., G. E., Romero, R. M., R., D. J., & P, R. O. (s.f.). *Seguridad Informática*. Madrid: Macmilian Iberia S.A.
- IASB. (s.f.). *NICNIFF*. Qué es el IASB: <https://www.nicniif.org/home/iasb/que-es-el-iasb.html#:~:text=La%20Junta%20de%20Normas%20Internacionales,Normas%20Internacionales%20de%20Informaci%C3%B3n%20Financiera>.
- Información, T. (2018). *Evolución de los Sistemas de Información*. <https://www.tecnologias-informacion.com/evolucionssystemas.html>
- ISACA. (2020). Marco de referencia de auditoría de información y tecnología. 7-8. ITAF.

- Leandro. (7 de Abril de 2015). *Programas de Contabilidad*. Los programas de contabilidad más usados: <https://programascontabilidad.com/comparativas-de-sofware/cuales-son-los-programas-de-contabilidad-mas-usados/>
- Martínez, T. (25 de Enero de 2017). *Red Global de Conocimientos en Auditoría y Control Interno*. Auditool: <https://www.auditool.org/blog/control-interno/4906-lo-nuevo-de-coso-erm>
- Martínez, Y. A. (2012). Auditoría con Informática a Sistemas Contables . *Revista de arquitectura e Ingeniería*, 5.
- Mauricio Torres Maldonado, J. S. (2017). *Auditoría Integral* . Quito: Mengraf.
- Muñoz, C. (2002). *Auditoría en Sistemas Computacionales*. México: Pearson Educación.
- tecnologias-informacion.com. (2018). *Tecnologías Información*. <https://www.tecnologias-informacion.com/evolucionsistemas.html>.
- Trasobares, A. H. (s.f.). *Los Sistemas de Información: Evolución y Desarrollo*. [file:///C:/Users/coelloi/Downloads/Dialnet-LosSistemasDeInformacion-793097%20\(1\).pdf](file:///C:/Users/coelloi/Downloads/Dialnet-LosSistemasDeInformacion-793097%20(1).pdf)