Sapienza Organizacional **ISSN:** 2443-4265 **E- ISSN:** 2443-4418 **Año** 9 **N°** 19 **Julio - Diciembre** 2022 **Pg.** 143-153

PROCESO DE LA AUDITORÍA Y TECNOLOGÍAS DE LA INFORMACIÓN

González, Maira

Licenciada en Contaduría Pública. Magíster en Ciencias Contables. Docente Agregado de la Facultad de Ciencias Económicas y Sociales de la Universidad de Carabobo.
E- mail: lobetomaira@gmail.com

Torres, Karla

Licenciada en Contaduría Pública. Doctora en Gerencia. Docente Titular de la Facultad de Ciencias Económicas y Sociales de la Universidad de Carabobo.
E-mail: katopo8@gmail.com.

Recibido: 15-15-2022
Revisado: 21-07-2022
Aceptado: 11-09-2022

RESUMEN

El experto contable en su ejercicio como auditor, debe tener competencias relacionadas con la tecnología de la información (TI), ya que las Normas Internacionales de Auditoría (NIA) establece la necesidad que el auditor obtenga un entendimiento de los riesgos y controles claves en TI, de este conocimiento se determinara el plan de auditoría. Dependiendo de la TI el auditor ejecutara su trabajo que requiere la evaluación de riesgo relacionada con TI, así como la evaluación sobre los controles automatizados para poder obtener evidencia de auditoría que permita una opinión sobre los estados financieros con seguridad razonable.

Palabras Clave: auditoría, controles, normas internacionales de auditoría, riesgos y tecnología de la información.

AUDIT PROCESS AND INFORMATION TECHNOLOGIES

ABSTRACT

The accounting expert in his exercise as an auditor must have skills related to information technology (IT), since the International Auditing Standards (NIA) establishes the need for the auditor to obtain an understanding of the risks and key controls in IT, from this knowledge the audit plan will be determined. Depending on the IT, the auditor will execute his work that requires the evaluation of risk related to IT, as well as the evaluation of automated controls in order to obtain audit evidence that allows an opinion on the financial statements with reasonable security.

Keywords: *auditing, controls, international auditing standards, risks and information technology.*

1. INTRODUCCIÓN

La auditoría de los estados financieros es un proceso sistematizado, llevado a cabo por el contador público en sus ejercicio independiente, que tiene como finalidad generar confianza en los usuarios de la información, sobre la razonabilidad o no de los estados financieros, en cuanto a si se encuentren libre de errores materiales, según las exigencias de un marco referencial que en Venezuela son las VEN NIF, brindando una seguridad razonable sobre la información que reflejan los estados financieros. La Norma Internacional de Auditoría (NIA) 200 (2009) establece en su párrafo 5 que: "Una seguridad razonable es un grado alto de seguridad. Se alcanza cuando el auditor ha obtenido evidencia de auditoría suficiente y adecuada para reducir el riesgo de auditoría".

El contador público en su ejercicio como auditor, frecuentemente obtiene evidencia de auditoría de la información que suministran los sistemas computarizados de las entidades, por tal motivo estos sistemas y la información que producen debe ser evaluada para determinar lo confiable y lo oportuno de los datos, así como de los efectos de esta información en la preparación de los estados financieros.

Para el logro del objetivo de la auditoria, se hace necesario que el auditor obtenga una comprensión de los sistemas de contabilidad y del control interno, que le permita la planeación de la auditoría. Las Normas Internacionales de Auditoría (NIA), establecen que en este proceso se debe obtener una compresión del diseño del sistema de contabilidad, del ambiente de control y de su operación.

La tecnología y la automatización de las entidades que son auditadas las hacen complejas y a la vez vulnerables antes acciones fraudulentas. El procesamiento electrónico de los datos ha permitidos que transacciones rutinarias contables y administrativas se realicen en formas más rápida y eficiente, además la tecnología impacta en la ejecución de muchos procedimientos de auditoría y ha llevado que el auditor use las computadoras para llevar a cabo su examen, trayendo como consecuencia debido a los adelantos tecnológicos que la evidencia de auditoría comprobatoria se obtenga principalmente en forma electrónica.

La naturaleza, oportunidad y alcance de los procedimientos de auditoría que se aplicaran están directamente influenciado por la complejidad de los sistemas de información, esto se debe a que los diferentes sistemas de información se encuentran en muchas entidades automatizados, por lo que auditor debe evaluar la seguridad que resguarda la integridad de la información.

Inicialmente los sistemas de información de las entidades estaban dirigidos al almacenamiento y centralización de los datos y a la capacidad del cálculo de ciertas operaciones, pero posteriormente en los sistemas se implementaron controles internos automatizados, lo que los ha hecho más complejo y en algunos casos hasta el intercambio de la información incluyendo la de tipo comercial, dejando muy atrás el uso del papel como prueba documentaria de una transacción. Todo lo descrito anteriormente hace pensar la importancia que el experto contable que realiza la auditoría tenga conocimientos solidos sobre la evaluación de los sistemas de procesamiento electrónico de datos.

2.Identificación y evaluación de riesgo de auditoría en un ambiente de tecnología de la información

Las NIA, son las normas que incluyen los procedimientos que debe aplicar el auditor en la ejecución de su trabajo, permitiendo que el mismo se realice bajo estándares internacionales de calidad y con el claro objetivo de obtener la evidencia que permita opinar sobre la razonabilidad de los estados financieros. La existencia de las NIA unifica a nivel mundial el trabajo que realizan los auditores lo cual genera confiabilidad sobre la información auditada.

El enfoque de trabajo que se establecen las NIA hacen referencia a la evaluación los riesgos materiales que pueden afectar

las aseveraciones que hace la gerencia en la preparación de los estados financieros, identificar y evaluar los riesgos requieren que el auditor obtenga un conocimiento de la entidad y su entorno, así como de los sistemas contables y del control interno, el cual debe ser la respuesta a los riesgos de negocio que se hayan identificado.

Tal y como lo indica la NIA 315 (2019) "la sola evaluación de los riesgos, los procedimientos de valoración del riesgo por sí solos no proporcionan evidencia de auditoría suficiente y adecuada sobre la que basar la opinión de auditoría". Esto significa que además de evaluarse los riegos el auditor debe identificar los controles establecidos por la gerencia para mitigar el riesgo lo cual ayudará a determinar el alcance y procedimientos de auditoría con el que finalmente se obtendrá la evidencia necesaria para justificar la opinión del auditor.

Se puede pensar que las entidades que tienen un sistema de información integrado son más confiables en cuanto a la emisión de información financiera, pero en la realidad esto no es cierto, ya que la tecnología elimina el error humano al procesar información uniformemente y con mayor rapidez las operaciones, sin embargo, errores de programación pueden hacer que las transacciones se registren en forma errada, además existe el riesgo que al ser los procesos automatizados donde no se involucra el personal del cliente puede ser susceptibles a transacciones fraudulentas, lo que hace inferir que los sistemas pueden garantizar precisión de cálculo, rapidez en la información pero no en todos los casos la información que emiten y que se convertiría en los estados financieros pueda considerarse confiable.

Los sistemas de información que se encuentra altamente automatizados incluyen procedimientos para el registro, autorización, procesamiento, comunicación y documentación de las transacciones, los cual se traducen en diferentes riesgos para el auditor, como lo son: accesos no autorizados, fallas en los equipos, resguardo de información, documentación acorde con los requerimientos legales de país, entre otros aspectos. Para mitigar estos riesgos el auditor espera que existan controles automatizados y manuales, que permitan, detectar, corregir y monitorear en forma oportuna las transacciones.

Otro aspecto interesante en los sistemas de información es que sean tan complejos y no dejen la pista de auditoría, lo cual no sería conveniente ni para la entidad ni para los auditores, ya que las pistas de auditoria permiten el control de operaciones, reconstrucción de archivos, que pueden ocurrir por fallas de equipos, o fallas eléctricas, así como las necesidades de información que pueda tener cualquier tipo de revisor interno o externo a la entidad.

Algunos de los riesgos más frecuentes relacionados con los sistemas de información son los siguientes:

- Protección insuficiente del software y hardware, este aspecto se relaciona con fallas eléctricas, fallas en los equipos, sabotaje como lo es el secuestro de datas relacionada con información operativa y financiera.

- Errores sistemáticos que se originan por errores en la programación, en especial cuando los sistemas no han sido parametrizados para reconocer operaciones inusuales.

- Accesos no autorizados, esto ocurre cuando no se han establecido en forma apropiada restricciones de acceso a la información a través de contraseña e identificación de usuarios, trayendo como consecuencias acceso a información confidencial, e inclusive cambios en parametrización de sistemas, así como las autorizaciones a transacciones por niveles no apropiados.

- Segregación de funciones o tareas, es el riesgo de que funciones que antes eran realizadas en forma segregadas cuando los procesos eran manuales, de que al ser automatizados se centralicen, es decir, que el mismo usuario realice actividades de autorización y registro contable, lo que

trae como consecuencia posibles errores intencionales o no sobre las transacciones que son registradas.

- Intervención manual inadecuada en los sistemas de información.

- Calificación del personal en el manejo de los sistemas, aunque la entidad mantenga sistema de información automatizados con poca complejidad, es vital que se cuente con personal interno o externo con conocimiento suficiente en la instalación, manejo y mantenimiento de los sistemas, dependiendo de la complejidad de los sistema las entidades pueden requieren de un departamento de sistema con todas las funciones propias de la tecnología de la información (TI), que incluiría a programadores, administradores de redes, responsables de archivos, administradores de base de datos, entre otros.

En una entidad se pueden presentar hechos o condiciones que indiquen la existencia de errores significativos relacionados con la tecnología de la información, como, por ejemplo: diferencias entre las estrategias de las TI y las estrategias del negocio, instalación de nuevos sistemas relacionados con la información financiera.

La NIA 315 "identificación y valoración de los riesgos de incorreción material", en su última revisión hace referencia a las TI y su influencia en la auditoría donde establece como prioritario la comprensión de parte del auditor de los sistemas de información incluyendo, las actividades de control y la comunicación. Para una mejor comprensión de los riesgos derivados de la TI es recomendable revisar los Anexos 5 y 6 de esta NIA.

La NIA 315 revisada en su anexo 5 denominado "Consideraciones para el conocimiento de la tecnología de la información", hace referencia que el sistema de control interno de las entidades tiene controles manuales y automatizados lo cual va a variar según la complejidad de la TI que sea evaluada por el auditor. Claro está, que los controles automatizados son más eficaces que los manuales, principalmente porque los controles automatizados no son fáciles de evitar y están menos expuestos a errores y equivocaciones.

El auditor debe obtener un conocimiento de los flujos de transacciones y el procesamiento de la información en el sistema de información, así como de la naturaleza y las características de las aplicaciones de TI que se utilizan. Las NIA le sugiere al auditor que debe clasificar la TI utilizada por la entidad en; software comercial no complejo, sistemas moderadamente complejos y sistemas de información complejos.

En el caso de las entidades que utilizan un software comercial, por lo tanto no tiene los códigos de fuentes que pudieran modificar los programas, el auditor deberá indagar en aspectos relacionados con: la reputación en el mercado sobre dicho software, el grado implantación del software ya que puede existir programas adicionales que no están siendo usados, las modificaciones que se ha hecho al software original por necesidades de la entidad, el acceso a la información relacionada con la preparación de los estados financieros y el volumen de datos usados.

Los sistemas moderadamente complejos presentan varias características entre ellas: introducción de datos moderados en forma automatizada, volumen moderado de datos almacenados, aplicaciones poco personalizadas, infraestructura pequeña o moderada, algunas aplicaciones tienen acceso a la web, entre otras características.

En los sistemas de información complejos el esfuerzo del auditor en el conocimiento de los sistemas información es mayor, ya que los sistemas de información financieros pueden estar integrados con sistemas operativos o empresariales, y en muchos casos la complejidad de estos sistemas es tal que se requiere un departamento dedicado a su administración e inclusive la utilización de proveedores externos para la realización de algunas tareas.

3. Evaluación de los controles internos en un ambiente de tecnología de la información (TI)

Una vez que el auditor identifica los riesgos significativos en un ambiente de TI deberá identificar los controles que mitigan estos riesgos, las NIA establecen una serie de criterios para la evaluación de los controles, como por ejemplo lo indicado en la Guía de aplicación y otras anotaciones explicativas de la NIA 315 (2018) señala: "La extensión y la naturaleza de los riesgos para el control interno varían según la naturaleza y las características del sistema de información de la entidad. La entidad responde a los riesgos que surgen de la utilización de las TI o de la utilización de elementos manuales en el control interno mediante el establecimiento de controles eficaces teniendo en cuenta las características del sistema de información de la entidad (A67)".

De lo descrito en el párrafo anterior se deprende que la intención de las NIA es que el auditor centre su atención en la evaluación de los controles que sean relevantes para mitigar los riesgos identificados en el proceso de auditoría, para ello, se debe tomar en cuenta que los controles que se vinculen con la integridad y la exactitud de la información, así como los relacionados con la salvaguarda de activos y las autorizaciones de operaciones tanto en el registro de compra como ventas de activos, autorizaciones de límites de créditos, de pagos, entre otras, son relevantes para el auditor ya que están directamente vinculados con la información financiera sobre la cual finalmente se emitirá una opinión.

Una vez que el auditor identifica los controles que considera relevantes, antes de probarlos debe realizar una evaluación de su diseño, es decir, si este control o su combinación con otros es capaz de mitigar el riesgo o los riesgos asociados, en el caso de considerar que el diseño es efectivo es que procederá a probarlo. Para la evaluación del diseño del control el auditor aplica técnicas de auditoria como la indagación y la inspección.

Tal y como lo indica las NIA 315 el auditor debe conocer las actividades de control establecidas en la entidad para responder a los riesgos vinculados con las TI. Las NIA indican que los controles sobre los sistemas de la tecnología de la información incluyen controles generales y controles de ampliación, ambos deben ser evaluados por el auditor.

En cuanto a los controles generales Arens (2007) dice: "los controles generales se relacionan con todos los aspectos de la función de TI, como la administración, adquisición de software y mantenimiento, seguridad en línea y física sobre el acceso de hardware, software e información relacionada, respaldo de la planeación en el supuesto de emergencias inesperadas y controles de hardware." (Pág. 348).

Los auditores evaluarán los controles generales ya que estos mantienen la integridad y la seguridad de la información y son los que mitigan riesgos relacionados con los accesos no autorizados, la confianza en los sistemas en el procesamiento electrónico de los datos, los cambios no autorizados en los sistemas, la pérdida de información, los respaldo y la seguridad general en los sistemas. Es práctica común de los auditores que la evaluación de los controles generales se realice al inicio de la auditoria, durante la etapa de la planificación, esto se debe a que los controles generales están diseñados para asegurar que los controles de aplicación sean efectivos.

Se hace necesario comprender que son las actividades de control de las aplicaciones según Whittington (2004) "Estas actividades se usan al procesar una aplicación. Se relacionan con la utilización de la tecnología de la información para iniciar, registrar, procesar y comunicar las transacciones u otros datos financieros." (Pág. 266). Estas actividades de control pueden ser preventivas o de detección y su objetivo principal es asegurar la integridad de la información financiera, son de relevancia para la auditoría ya que aseguran que las transacciones han ocurridos, están autorizadas y se han procesado en los sistemas de información de forma correcta.

Los controles generales se clasifican según su categoría en: Administración de la función TI, Segregación de funciones de TI, Desarrollo de sistemas, Seguridad física y en línea, Respaldos y plan de contingencia y los controles de hardware. Los auditores realizaran indagaciones sobre cada uno de estos controles documentándolos en algunos casos a través de cuestionarios, flujogramas de información o de manera descriptiva.

La administración de la función de la TI, se relaciona con la importancia que para la alta Gerencia tiene la tecnología de información esto se vincula con la supervisión y asignación de recursos por parte de la administración, en sistema complejos se crea un comité directivo de TI quienes hacen seguimiento de las necesidades tecnológicas de la entidad, sin embargo, en muchas entidades la función tecnológica se delega a empleados de bajo nivel o proveedores externos, lo que pudiera traer como consecuencias deficiencias en el manejo de los sistemas de información, lo ideal es que el jefe o encargado de la tecnología reporte directamente a la alta administración de la entidad.

La Segregación de funciones de TI, se refiere a la separación de tareas como por ejemplo separa responsabilidades de programación, de operaciones rutinarias de cómputo, así como la separación de las operaciones de control de datos.

Desarrollo de sistemas que son controles que se diseñan para reducir el riesgo de cambios no autorizados de software, esto incluye las políticas que establezca la entidad para el desarrollo de sistema o la compra de sistema a un proveedor, donde se incluirán los procedimientos en el caso de cambios de sistemas que asegure que el nuevo software sea compatible con el hardware existente.

Seguridad física y en línea, estos controles incluyen los controles físicos de los equipos de computación a través del acceso restringido tanto al hardware como al software, así como los respaldos que deben realizarse de la información, entre los controles físico están todas las normas que se establecen para que los equipos funciones en condiciones ópticas relacionados con aspecto de frio o de humedad que eventualmente pueden afectarlos. Los controles en línea los cuales reducen la posibilidad de cambios no autorizados en las aplicaciones y archivos de datos.

Respaldos y plan de contingencia, cada entidad debe contar con un plan de contingencia para responder a los riesgos relacionados con fallas eléctricas, humedad, daños causados por agua, así como sabotajes sobre los sistemas. Este plan debe estar por escrito e incluir las políticas de respaldos interno y externos de los datos y software.

Controles de hardware, estos controles son establecidos por los fabricantes de equipos de cómputo y la entidad debe hacer seguimiento de ellos con el fin de detectar y prevenir fallas en forma oportuna.

Los controles de aplicación se pueden clasificar en controles de entrada, de procesamiento y de salida. Los controles de entradas buscan una seguridad razonable que los datos de entrada están autorizados e incorporados de forma exacta en el sistema. Los controles de procesamiento garantizan que el procesamiento de los datos está conforme con la aplicación, identificando de manera oportuna, en el caso de ser necesario, errores y duplicidad. Los controles de salida son los que aseguran la exactitud del resultado de procesamiento de datos.

Finalmente, el auditor debe saber que mientras más dependa una entidad de sus sistemas de información basados en tecnología, será más probable que los procedimientos sustantivos que diseñe el auditor por sí solos no puedan proporcionar suficiente evidencia, por lo que se debe probar la eficiencia de los controles atomizados que hayan sido identificados.

La evaluación de los controles generales es realizada por los auditores antes de evaluar los controles de aplicación, ya que si se concluye que los controles generales son ineficientes se infiere que existen potenciales errores en los controles de aplicación, por el contrario cuando se confía en los controles

generales se considera que existe una mayor probabilidad que los controles de aplicación sean eficaces, lo que pudiera traer como consecuencia una reducción en las pruebas de control y sustantivas haciendo más eficiente el proceso de auditoría.

Los auditores para obtener información sobre los controles generales y de aplicación suelen realizar entrevistas con el personal directamente involucrado con la administración de los sistemas y con los usuarios claves, se revisan la documentación del sistema que se obtienen de los manuales de usuarios, así como se aplican cuestionarios que deben ser respondido por el equipo de TI.

El auditor una vez que conoce el sistema de control de la entidad, será capaz de identificar si se encuentra ante un entorno de tecnología de información sencillo o de alta complejidad, por ejemplo en aquellos sistemas de información donde los documentos de origen como órdenes de compra, facturas, reportes de nómina, así como la información emitida por el sistema de contabilidad libros de diarios y mayores analíticos le van a permitir al auditor comparar los registros producidos por la computadores con los documentos de origen, en estos casos el impacto de la TI es menor y no se realizaran pruebas de controles de cómputo, en este caso el auditor realizara pruebas a controles manuales así como pruebas sustantivas de mayor alcance, lo que le permitirá reducir los riesgos de auditoría y emitir una opinión.

En otros casos parte significativa de la evidencia de auditoría es digital, como por ejemplo las facturas electrónicas además la información interna de finanzas, de recursos humanos, operacional o de planificación, cuyos elementos nacen en un sistema de información y se transmiten electrónicamente. En estos casos se realizan pruebas a los controles de aplicación ya que aplicar solo pruebas sustantivas se consideran que no es la mejor alternativa.

En Venezuela se ha observado que entidades que en años anteriores tenían sistemas de información de moderada o alta complejidad, inclusive sistemas que habían sido diseñados según las necesidades de la entidad, emigraron a software comerciales relativamente simples, que incluyen un módulo administrativo utilizado en la facturación y manejo de proveedores y sus pagos y un módulo contable para la emisión del balance de comprobación y posterior preparación de estados financieros, esto debido principalmente a la reducción significativas de operaciones y a los altos costos de mantenimiento de los sistemas de información. Por lo que los auditores tal y como lo exige la NIA 315, debe realizar una evaluación de los riesgos relacionados con la TI, y evaluara los controles generales, aunque probablemente decida realizar pruebas de controles manuales y sustentación de saldo para obtener la evidencia de auditoría.

4.Las Tecnologías emergentes y el enfoque del auditor

La continua innovación tecnológica que se ha experimentado en las últimas décadas ha afectado el mundo en todos sus ámbitos y claro esta ha influenciado las entidades y por lo tanto el trabajo del auditor. Las llamadas tecnologías emergentes que son tecnologías en vías de desarrollo, es decir, que aún están creciendo y que se esperan un mayor impacto en la humanidad, también deben ser evaluadas por el auditor ya que están afectando las operaciones que se registran en los estados financieros.

Si hablamos de internet, la conectividad de hoy día en la era digital, donde casi cualquier dispositivo, como los celulares, puede conectarse al internet y poder realizar pedidos y pagos desde cualquier lugar sin importar ni el tiempo ni la distancia, afecta el alcance del trabajo del auditor que requiere de nuevas experticias para poder evaluar el diseño y la operatividad de los sistemas.

Una de las consecuencias inmediata de la era digital y las bondades de la conectividad, es que esta tecnología ha mejorado la comunicación entre los auditores y sus clientes, cada vez esta relación se hace más interactiva, un ejemplo de esto es el desarrollo de plataformas tecnológicas

por parte de grandes firmas de auditoría, para recibir y enviar información, dejando atrás en muchos casos el usos de correos electrónicos y permitiendo un seguimiento del avance de la auditoria no solo para el equipo de trabajo sino también para la entidad auditada.

La presencia de la inteligencia artificial en el manejo de procesos de negocio que permiten hacer proyecciones de inventario, manejo de efectivo, tendencias del mercado, entre otros aspectos y que son usados por la alta gerencia para la toma de decisiones, e inclusive pueden ser usado para la realización de estimaciones contables, ya que esta tecnología puede identificar correlaciones de datas que antes no era posible, introduce nuevos riegos de negocio, que de acuerdo con las NIA, deben ser entendidos por el auditor, en especial su impacto en las transacciones que se registran en la contabilidad y la confianza que generan los reportes de esta proyecciones sobre los cuales la gerencia toma decisiones, el auditor evaluara los riesgos y el ambiente de control diseñado por la entidad para formarse una opinión sobre la razonabilidad de estos registros que afecta las preparación de los estados financieros.

Otra tecnología emergente que está afectado a las entidades y más aún podría modificar la forma en que se hace la auditorias se refiere a las técnicas de almacenamiento y tratamiento masivo de datos o Big Data, esta tecnología permitirá a corto plazo el tratamiento masivo de datos por parte del auditor, lo que llevará, probablemente a las grandes firmar a obtener todo el sistema de información de un cliente para posteriormente realizar la auditoría, trayendo como consecuencia inmediata que la auditoría sea más eficiente ya que entre otras consideraciones, el auditor automáticamente podría revisar el 100% de las operaciones en cualquier momento, determinando los errores de forma oportuna, por supuesto, esto está en desarrollo y se presentan grandes dificultades, como por ejemplo: la no autorización de la data por parte de la entidad auditada, la inversión tecnológica y entrenamiento que deberán hacer las firmas de auditores, significando una gran transformación en la profesión del auditor, lo que sí está claro es que la tecnología ya está en proceso lo demás será parte de la evolución que ha experimentado el proceso de la auditoría desde la llegada de la TI.

La tecnología Blockchain según Bautista, F. (2.021) “es un protocolo informático que se traduce en una serie de registros descentralizados e inmutables en la red, capaces de registrar toda una serie de transacciones - eventos-, quedando dichas transacciones registradas y protegidas por la inalterabilidad del sistema”. Lo que se traduce en una base de datos que comparte varios computadores y tiene aplicación en la contabilidad y en el proceso de auditoría, la aplicación más conocida ha sido en uso de monedas digitales, pero el sector financiero ha estado interesado en esta tecnología para disminuir su dependencia de intermediario en transacciones de dinero, para el proceso de auditoria esta tecnología puede enfocarse a obtener transacciones contables en tiempo real y automatizar y hacer más efectivo el trabajo del auditor.

Con las tecnología emergentes se ve a corto o mediano plazo un cambio en el rol del auditor, actualmente existen especialistas en informática que forman parte del equipo de auditoría y como expertos se encargan de la evaluación de los riegos tecnológicos de las entidades más complejas, sin embargo, el desarrollo de la tecnología está llevando a que se requiere un auditor integral por supuesto con sólidos conocimientos contables, así como de estándares de auditoría, pero a la vez que sea capaz de entender y usar herramientas informáticas para la ejecución del trabajo.

5. REFLEXIONES FINALES

En el siglo XXI las entidades están cada vez más digitalizadas y conectadas, lo que ha traído como consecuencia una gran dependencia en la tecnología, por lo tanto, el auditor

es responsable del entendimiento relacionado con el entorno de la TI, así como de los controles generales y de aplicación que mantenga la entidad que se está auditando.

El objetivo de una auditoría no cambia bajo un ambiente de sistemas de información computarizada sea sencillo o de alta complejidad, sin embargo, la automatización que ofrecen los sistemas tanto en el ingreso de la información como en procesamiento, almacenamiento y comunicación de la información contable tienen consecuencias de alto impacto sobre los estados financieros. Las NIA, requieren que el auditor obtenga suficiente conocimiento del sistema de información, lo que permitirá diseñar el plan de auditoría, en que se deberá considerar si se necesitan conocimientos específicos para la realización del trabajo, en especial en ambiente complejos en los que se pueda requerir dentro del equipo de auditoria la asistencia de especialistas en sistemas información computarizados.

Las NIA establecen que el auditor debe identificar los riesgos relacionados con los sistemas de información automatizados, además se deben identificar los controles que van a mitigar estos riesgos, el primer paso es evaluar el diseño de los controles establecidos, en el caso de que a juicio del auditor estén adecuadamente diseñado se procederán a probar los controles y posteriormente se informaran los hallazgos y desviaciones encontradas. Si el auditor concluye que el control es ineficiente esto impactara, la naturaleza y alcance de los procedimientos de auditoría, obteniendo la evidencia de auditoría a través de procedimientos sustantivos.

Tomando en cuenta que los avances tecnológicos son continuos y van a gran velocidad en todos los aspectos que influyen las entidades auditadas, se evidencia la necesidad de que el auditor desarrolle competencias en el área de informática que le permita responder a tecnologías emergentes, ya que se hace necesario para que el auditor pueda evaluar los riegos potenciales asociados a la TI, y así seguir brindando a la sociedad en general una seguridad razonable, al momento de emir su opinión adaptada a los nuevos retos tecnológicos.

8. REFERENCIAS

Arens, A., & Randal J. (2007). *Auditoría un enfoque integral*. México, Prentice Hall.

Baque, E., & Chiquito, G. (2019). Control interno como proceso fundamental de los sistemas computarizados de auditoría. *Revista Científica Mundo de la Investigación y del Conocimiento*. Vol. 3 núm. 1 enero, ISSN: 2588-073X, 2019, pp. 1225-1242.

Bautista, F. (2021). Blockchain y la auditoría interna/externa Disponible en https://www.crowe.com/ve/insights/blockchain-y-la-auditoria-interna-externa [Consulta: 2022, septiembre 26].

Espinoza, W. (2016). La tecnología de la información como herramienta contraccionista para el auditor financiero híbrido. *Revista de difusión cultural y científica de la Universidad La Salle en Bolivia* Disponible en http://www.scielo.org.bo/scielo.php?script=sci_arttext&pid=S2071-081X2016000100002 [Consulta: 2022, septiembre 11].

Grisanti Belandria, A. (2009) *Lecciones de Auditoría III*. Caracas- Venezuela. Vadell Hermanos Editores.

Norma Internacional de Auditoria 200 (2009). Objetivos Globales del Auditor Independiente y realización de la auditoría de conformidad con las normas internacionales de auditoría.

Norma Internacional de Auditoria 315 (revisada en 2019). Identificación y Valoración de Riesgos de Incorreción Material.

Pérez, I. (2022). Tecnología y auditoría; principales retos. Disponible en: https://www.icjce.es/tecnologia-auditoria-principales-retos[Consulta: 2022, septiembre 24].

Rodríguez, I. (2022). El auditor y los controles generales de la tecnología de la información. Disponible en: https://www.auditool.org/blog/auditoria-externa/8775-el-auditor-y-los-controles-generales-de-tecnologia-de-la-informacion [Consulta: 2022, septiembre 21].

Saade, G. (2010) *El procesamiento electrónico de datos*. Trabajo de Seminario. Universidad Nacional de Tucumán. Facultada de Ciencias Económicas.

Whittington r., & Pany K. (2004). *Principios de Auditoría*. México. Mc Graw Hill