risti
Revista Ibérica de Sistemas e Tecnologias de Informação
Iberian Journal of Information Systems and Technologies

Recebido/Submission: 15/03/2020
Aceitação/Acceptance: 17/05/2020

Análisis de las principales dificultades en la auditoría informática: una revisión sistemática de literatura

Daisy Imbaquingo[1,2], Javier Díaz[2], Tatyana Saltos[2], Silvia Arciniega[2], Jayli De la Torre[2], Jácome Jesús[2]

daisy.imbaquingoe@info.unlp.edu.ar,jdiaz@unlp.edu.ar, tksaltos@utn.edu.ec, srarciniega@utn.edu.ec, jddelatorrer@utn.edu.ec,jajacomeq@utn.edu.ec

[1] Universidad Nacional de La Plata, 1900, La Plata, Argentina.

[2] Universidad Técnica del Norte, Facultad de Ingeniería en Ciencias Aplicadas, 100105, Ibarra, Ecuador.

Pages: 427–440

Resumen: En la actualidad las organizaciones cuentan con una infraestructura de TI en la que se implantan sistemas de información y a su vez se desarrollan procesos que permiten automatizar otros que son manuales. El presente artículo tiene por objetivo realizar una revisión sistemática de la literatura a partir de la revisión de un número considerable de trabajos que permitan dar respuesta a las tres preguntas de investigación planteadas. Se determinó que las principales dificultades de la auditoría informática tienen que ver con los costos elevados de realizar una auditoría, en los resultados de esta que no satisfacen al usuario final y la posibilidad de generar resultados negativos. Por último, se señala la importancia de la auditoría en la seguridad de la información alojada en infraestructura propia del auditado y alojada en el Cloud.

Palabras-clave: auditoría de TI; problemas de auditoría de TI; tendencias de auditoría de TI.

Analysis of the main difficulties in Computer Auditing: Systematic literature review

Abstract: Currently organizations have an IT infrastructure where information systems are installed and at the same time processes are developed to allow the automatization of manual processes. The objective of this article is to make a literature systematic review starting with a considerable number of works which allow to give answers to three research questions asked. It was determined that the main difficulties of the computer audit are focused with the high costs to do an audit, the results of it that do not satisfy the final user and the possibility to generating negative results. Lastly, the importance of auditing in the security of the hosted information in the own infrastructure of the audited and hosted in the Cloud is pointed out.

Keywords: IT audit; IT audit problems; IT audit trends.

1. Introducción

Al hablar de auditoria se asocian a este proceso conceptos errados, tales como que el objetivo sea buscar errores en una organización y atacar a funcionarios o responsables. Si bien es cierto, la idea anterior tiene su verdad, la auditoría va más allá de los hallazgos y de identificar las anormalidades de los auditados, es así que el concepto de auditoría ha ido evolucionando con el paso del tiempo, y con él, las ramas que derivan de la misma también. Una de ellas es la llamada "Auditoría Informática" o también conocida como "Auditoría de TI". El área de la Auditoría de TI es relativamente nueva como explica Aditya & Ferdiana (2018), tuvo su auge en la década de los 60 cuando el empresario vinculó aspectos de la organización, estrategia de TI y los negocios, todo con el fin de cumplir los objetivos planteados en su organización. Con el paso del tiempo, la auditoría de TI se ha vuelto más compleja expone David (2015) debido al crecimiento de las tecnologías y a que las organizaciones buscan automatizar procesos. Las empresas en la actualidad están optando por el almacenamiento en Cloud mencionados, tales como señalan David (2015), Esther & Vasanthi (2019), Razaque Abdul (2017) lo que significa también que la auditoría de TI debe adaptarse a las nuevas tendencias.

Como su nombre lo indica, la Auditoría de TI es la encargada de auditar los procesos de TI en una organización relata Vasarhely Miklos (2018), encontrar fallos y hallazgos que ayuden al auditado a mejorar estos procesos y con ello llegar a sus objetivos, además Aditya & Ferdiana (2018) menciona que Auditoría de TI también es encargada de evaluar la seguridad de la información que maneja una empresa dentro y fuera de ella. Las vulnerabilidades en los sistemas web plantean serias amenazas a la seguridad y la privacidad, como violaciones de la privacidad de los datos, violaciones de la integridad de los datos y denegaciones de servicio, así señalan Thomé, Khin, & Bianculli (2018). Como bien se sabe, David (2015) revela que la información es uno de los bienes más preciados de cualquier organización, de ahí la importancia de resguardarla.

El presente documento de revisión sistemática pretende analizar los errores más comunes que tienen los auditores al realizar el proceso de Auditoría de TI o Auditoría Informática a través de la obtención de información de trabajos realizados en los cuales han surgido inconvenientes en este proceso. Los trabajos citados en este documento no solamente tienen que ver con la Auditoría de TI sino también con la Auditoría de manera general lo cual permitirá tener una visión más amplia del estado del arte de esta y realizar comparaciones entre sus distintas ramas con la Auditoría informática. A continuación, se enumeran las preguntas de investigación que serán respondidas más adelante en el documento:

- ¿Cuáles son las principales dificultades de la auditoría informática?
- ¿Cuáles son las principales capacidades, aptitudes o habilidades que debe tener un Auditor Informático?
- ¿Cuál es el papel de la Auditoría de TI con respecto a la seguridad de la información?

2. Metodología

La metodología usada para la redacción del presente documento de revisión sistemática de la literatura es la misma utilizada por Atymtayeva, Bortsova, & Inoue (2012) llamada

SLR. Cabe mencionar que el proceso de investigación se realizó en cuatro fases que se listan y describen detalladamente a continuación:

2.1. Búsqueda de documentos

Para realizar la búsqueda de los documentos en base al tema en desarrollo se usó la siguiente cadena de búsqueda en varias de las bases de datos científicas más usadas (Figura 1): ((“it audit” OR “computer audit” OR “information audit” OR “IS audit”) AND (“computer Audit issues” OR “it Audit issues” OR “audit issues”) AND (“Audit problems”)). Adicionalmente, se usaron algunas variantes para obtener, al menos, 15 documentos en cada base de datos bibliográfica. En total se obtuvieron 71 documentos relacionados al área en cuestión.

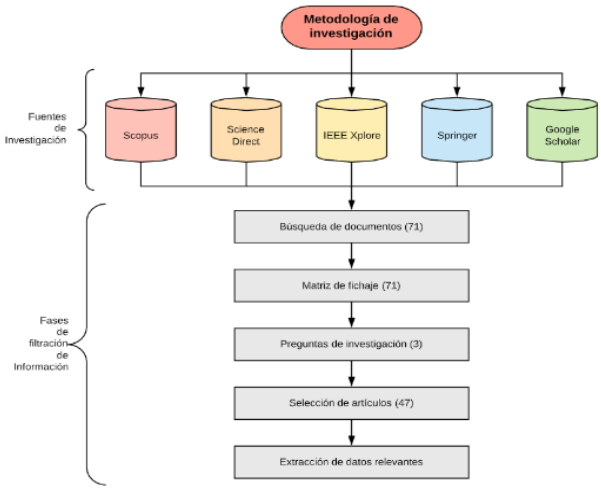

Figura 1 – Diagrama del protocolo utilizado en la SLR.

2.2. Preguntas de investigación

Para la redacción de los resultados de este documento se definieron tres preguntas de investigación (PI) sobre los problemas de la Auditoría informática, las cualidades de los auditores informáticos y el papel e importancia que desempeña la auditoría de la información en la seguridad de los datos. En la Tabla 2 se pueden observar a detalle las preguntas y la motivación que llevó a realizarlas. Para la búsqueda de información de relevancia para el presente trabajo se hizo uso de las bases de datos de Science Direct, Scopus, IEEE Explore, Springer y Google Scholar.

Número	Preguntas de investigación	Motivación
PI1	¿Cuáles son las principales dificultades de la auditoría informática?	Identificar los principales problemas para los auditores en la rama de la Auditoría Informática

Número	Preguntas de investigación	Motivación
PI2	¿Cuáles son las principales capacidades, aptitudes o habilidades que debe tener un Auditor Informático?	Identificar las cualidades que permiten a los auditores informáticos realizar su labor de la mejor manera posible.
PI3	¿Cuál es el papel de la Auditoría de TI con respecto a la seguridad de la información?	Identificar la importancia de la auditoría de TI en la seguridad de la información y el impacto que tiene en las organizaciones.

Tabla 1 – Preguntas de investigación (PI).

2.3. Selección de artículos

Para filtrar los documentos hallados en las bases de datos de investigación se aplicaron criterios de filtración. Los criterios considerados fueron: (i) relevancia del contenido, (ii) revisiones, (iii) estudios relacionados con la Auditoría Informática y temas afines. Además, un filtro adicional empleado al momento de realizar las búsquedas en las bases de datos bibliográficas fue de filtrar el contenido por "Ciencias e ingeniería", "Ciencias computacionales", "Seguridad de la información", "Auditoría y control interno", entre otras, todos estos escritos en inglés. En la segunda fase se tomó en cuenta el aporte a las preguntas de investigación descritas en el contenido del documento.

2.4. Extracción de datos relevantes

Al finalizar las dos fases de selección de los documentos se obtuvieron 48 trabajos. Para la extracción de las partes esenciales de los documentos se tomaron aquellos párrafos que ayudaron a responder las PI por lo que hubo que revisar en primera instancia, aquellos trabajos relacionados con la Auditoría Informática, Auditoría de TI y Problemas en la Auditoría de TI; pasando luego por aquellos relacionados con las características que definen a los buenos auditores en general y por supuesto a los auditores de TI; por último, se debió revisar la literatura relacionada con el papel de la Auditoría Informática en la seguridad de la información de las organizaciones en artículos que lo aplicaban a casos reales.

3. Resultados

PI1 ¿Cuáles son las principales dificultades de la auditoría informática?

3.1. Costos exagerados

Hanibuchi (2019) afirma que al realizar sus auditorías a las calles de Japón utilizando la herramienta Google Street View generan costos muy elevados por ser herramientas de pago. Con el uso de la tecnología Hoffman Benjamin (2018) corrobora que existe aumento de las tarifas de auditorías. Kumar & Singh (2018) evidencian que existen pocos métodos de verificación de integridad remota que puedan servir en datos almacenados estáticos, pero no funcionan dinámicamente, estos métodos de verificación deben realizar empresas dedicadas a la integridad de los datos.

Bahri Leila (2018) propone un método de selección de auditoría mejorado que se basa en parámetros clave, como la reputación de los nodos y las tasas de malos comportamientos detectados en la red. Se realizó experimentos en un gráfico OSN real para estudiar el valor agregado de las estrategias de auditoría mejoradas propuestas. Los resultados muestran que el método mejora el rendimiento del sistema en más del 50% en comparación con las selecciones aleatorias. Se considera que este trabajo es de suma importancia para el desarrollo de soluciones de control de acceso, con un mecanismo de auditoría adecuado, eficiente y efectivo.

3.2. Falta de experiencia

Como afirma Pedrosa Isabel (2019) en previas investigaciones el grado de compromiso de la alta dirección y la influencia de los auditores legales es determinante para la adopción de CAATS. Además, Razaque Abdul (2017) señala que el papel de un tercer auditor externo podría ser una amenaza de seguridad potencial en sí misma y puede crear nuevas vulnerabilidades de seguridad para los datos del cliente. Huan Feiqi (2019) en su investigación indica que las tareas de auditoría repetitivas, estructuradas y laboriosas (como conciliaciones, interna pruebas de control y pruebas detalladas) son candidatos ideales para RPA (Robotic Process Automation), su aplicación a la auditoría se ha retrasado debido a preocupaciones sobre riesgo y regulación.

Según Siew Eu Gene (2019), los CAATT no se han utilizado en el mundo del desarrollo, sin embargo existe tres factores ambientales que son exclusivos del entorno de auditoría externa, estas son la complejidad del entorno AIS de los clientes, la presión competitiva de otras firmas de auditoría para adoptar los CAATT y el grado en que los organismos contables profesionales apoyan la adopción de los CAATT. El estudio realizado por Gepp Adrian (2018) se basa en la falta de progreso en la implementación de técnicas de big data en la práctica de auditoría sigue siendo sorprendente, dado que el uso temprano de técnicas de auditoría de muestreo aleatorio coloca a los auditores muy por delante de las prácticas de sus empresas cliente.

3.2.1. Reportes negativos

Alzahrani (2018) afirma que según la auditoría de seguridad interna realizada por un proveedor el 7 de septiembre de 2014, la red de la Universidad de Albaha tiene los siguientes problemas, en términos de seguridad: el departamento de TI necesita recursos más calificados, un solo ingeniero no puede manejar las operaciones diarias. El no tener un departamento de TI suficientemente equipado evidencia dificultades a la hora de realizar auditorías obteniendo resultados erróneos.

Hanibuchi (2019) presenta que uno de los mayores desafíos de la auditoria informática es la precisión en sus resultados, en este caso se presenta variedad de error en el estudio utilizando Google Street View al realizar auditorías sobre las calles de Japón, 830 segmentos fueron auditados física y virtualmente por auditores capacitados con resultados diferentes en pendientes. Manita Riadh (2020) expone su investigación La Nueva Ley sobre Regulación Económica (Ley Sarbanes-Oxley de 2002 en EE. UU.) que fortaleció los controles de los auditores, particularmente a través del PCAOB1 y los comités de auditoría. La calidad de la auditoría sigue siendo la principal preocupación

de los interesados, el usuario final no queda conforme con los resultados obtenidos por lo cual no pueden tomar decisiones que puedan ayudar en un futuro.

3.2.2. Comunicación ineficiente

Strous (1998) explica que los problemas particulares para un auditor son la creación de mensajes de información como los procesos que rigen dentro de un sistema no son directos con el auditado dentro y fuera de la organización y la creación de estos por parte del socio comercial. Thomé, Khin, & Bianculli (2018) revelan que no existe un auditor de seguridad para localizar vulnerabilidades en el código fuente, identificar sus causas y corregirlas, es así que no serían suficientes para soportar la auditoría de código que contienen información derivada de comportamientos observados del programa o trazas de ejecución. Pedrosa Isabel (2019) reflexiona sobre lo que se puede hacer para promover la TI entre los auditores, teniendo en cuenta el impacto de los CAAT en la eficacia y la eficiencia del trabajo de los auditores, lleva a la necesidad de aclarar las herramientas potenciales: esto puede indicar que las casas de software necesitan proponer software orientado por procedimiento/tarea y hacer que todo el software sea fácil de usar y comprender.

Tendencia de Auditoría	Nro. Artículos
Costos Exagerados	4
Falta de Experiencia	5
Reportes Negativos	4
Comunicación ineficiente	3
Total	16

Tabla 2 – Tendencias de dificultades en la Auditoría de TI.

PI2 ¿Cuáles son las principales capacidades, aptitudes o habilidades que debería tener un auditor?

3.3. Disponer amplios conocimientos

Lu Hui (2018) explica varios requisitos importantes para el sistema de auditoría de seguridad, no es difícil ver que el sistema de auditoría de seguridad no es solo un simple sistema de registro. Especialmente a medida que los ataques y la destrucción de la red se vuelven cada vez más serios, el sistema de auditoría de seguridad presenta requisitos más altos. Se debe guiar normas internacionales, de acuerdo con las condiciones del propio sistema, las dificultades de seguridad y los problemas que enfrentan las necesidades específicas para desarrollar nuestro sistema de auditoría de seguridad. Strous (1998) pone a consideración que el auditor debe tener conocimiento de legislación internacional sobre el estado legal de documentos comerciales electrónicos, retención de registros, acuerdos de intercambio de datos, etc. Huan Feiqi (2019) atestigua que el auditor debe tener el dominio contable, por lo que las principales firmas contables aplican RPA (Robotic Process Automation) para lograr ahorros de costos y aumentar la eficiencia

operativa en los servicios de asesoría e impuestos, además tener la capacidad de liderar a un grupo.

3.4. Imparcial sincero y honesto

Bylica Wojciech (2011) indica que el proceso de auditoría escalable propuesto da al auditor conocimiento sobre qué activos no están adecuadamente protegidos, y en qué forma particular la organización no puede realizar el procedimiento en una empresa. El proceso introducido permite centrarse en los problemas de seguridad más importantes el tiempo que incluye las prioridades de la organización.

David (2015) analiza que los auditores deben crear un informe de auditoría en el que se deben registrar todos los procedimientos que se realiza que contiene elementos de auditoría (interna, externa, TI) incluyen todos los SLA (Service Level Agreement), gobierno, ahorro de costos, almacenamiento de datos, problemas de riesgo y seguridad, y protección contra desastres en las operaciones de computación en la nube dentro de los sitios de proveedores de servicios y clientes de la industria. Básicamente, hay tres secciones que deben completarse, incluidos el objetivo, el procedimiento de auditoría y los resultados de la norma relevante.

Tendencia de Auditoría	Nro. Artículos
Disponer amplios conocimientos	3
Imparcial Sincero y honesto	2
Total	5

Tabla 3 – Tendencias de las habilidades de un auditor informático.

PI3 ¿Cuál es el papel de la auditoría de TI con respecto a la seguridad de la información?

La seguridad de la información de las organizaciones es de vital importancia para las mismas porque, como se sabe, "la información es poder". Es así que se puede evidenciar la importancia que tiene el realizar auditorías de la información que permitan saber el estado actual cómo las organizaciones manejan sus datos:

3.5. Las vulnerabilidades de los sistemas de información

Las vulnerabilidades y errores de los sistemas de información son a menudo explotados por usuarios malintencionados para inmiscuirse en éstos y comprometer la seguridad (por ejemplo, disponibilidad, integridad y confidencialidad) de los sistemas de información tal como señalan Nong, Xiangyang, & Qiang (2001). A demás Atymtayeva, Bortsova, & Inoue (2012) nos mencionan que "las amenazas que se presentan en los sistemas de información: Por lo general, el riesgo se calcula en función a la probabilidad de que la amenaza se ejerza contra la vulnerabilidad y el impacto resultante de un compromiso exitoso. En realidad, el impacto es el valor del daño al atributo de ciertos activos (disponibilidad, integridad, etc.) causado por la materialización de una o más

amenazas. La identificación y medición de riesgos es muy crucial en la auditoría de seguridad de la información, lo que también se menciona en este trabajo."

3.6. La auditoría de TI a la información de las organizaciones

La Auditoría Informática o de TI basa mucho sus técnicas y procesos en la visualización de datos de las organizaciones como exponen Aditya & Ferdiana (2018), a continuación, se define cuál es la importancia de realizar una auditoría a la información o a los datos que manejan interna y externamente las organizaciones. En algunos de los documentos encontrados, los auditores utilizan herramientas que explican en su investigación Swathy & Velvizhi (2014) en el que se menciona las "firmas de preservación de la estructura" las cuales son utilizadas como técnica para crear seguridad y autenticación de los datos en la nube. De modo que el verificador público realiza la auditoría sin necesidad de descargar los datos de quién lee desde la nube. Para admitir varias tareas de auditoría simultáneamente, el verificador realiza una auditoría por lotes. La auditoría de la información en la nube será un tema que trataremos más adelante. Al realizar un análisis Chang, Wu, & Chang (2008) muestran que existen aún problemas con las herramientas usadas para la extracción de datos de los sistemas de información en los cuales se alojan los datos de las organizaciones. Además, Aditya & Ferdiana (2018) proponen un esquema de comprensión novedosa a un sistema de auditoría que simula el método de DTT. Método que logra ser aplicado con éxito como indican Aditya & Ferdiana, (2018).

Para un auditor, es importante conocer la información acerca de los datos de los usuarios que usan un sistema de información con el fin de identificar si alguno de estos ha incurrido en alguna anomalía tal como explican Wang, Wu, & Deng (2017). Según Han, Lin, & Chen (2018) explican de un esquema que no tiene emparejamiento y permite que un auditor externo genere un metaconjunto de autenticación en nombre de los usuarios. Li, Yen, & Chuang (2016) en su investigación hablan de un dispositivo fuente que registra una entrada de los sistemas del usuario, los datos se transfieren a la base de datos simultáneamente. Cuando se agrega un registro, el servidor de la base de datos activa los programas basados en LZW (algoritmo de precisión sin pérdida) para ejecutar automáticamente las funciones de compresión y auditoría de datos. Por lo tanto, el proceso de datos recién agregados a los resultados de monitoreo fluye de manera oportuna y continua, lo que ayuda a que el trabajo del auditor fluya rápidamente. En resumen, la auditoría de la información se encarga de recabar los datos de las empresas con el fin de verificar si el flujo de los Sistemas de Información que maneja la misma contiene datos íntegros, verificables y sobre todo seguros frente a agentes que intentasen hacer uso indebido de estos.

3.7. La auditoría de TI a información alojada en *Cloud*

"La computación en la nube ha atraído mucha atención en esta década. Debido a los recursos ilimitados de la informática y el almacenamiento, cada vez más personas y las organizaciones prefieren seleccionar la computación en la nube para ayudar a almacenar los datos y procesamiento de los asuntos complejos." Explican (2018). Otro concepto casi análogo a la computación en la nube (respecto al almacenamiento de información) es el de outsourcing de bases de datos, que consiste en contratar alojamiento de terceros para

usar sus servicios de bases de datos. Xiang, Li, & Chen (2018) señalan que el outsourcing de bases de datos está ligado al desafío sobre la seguridad de los datos de los usuarios por lo tanto es importante proporcionar medidas de seguridad adecuadas para proteger los datos tercerizados de atacantes externos maliciosos. Y es aquí en donde actúa la auditoría informática, en verificar que la información almacenada en estos proveedores de servicio se encuentre segura.

Kumar & Singh (2018) proponen una arquitectura de seguridad de tres niveles para almacenar archivos multimedia que incluyen control de acceso, cifrado y verificación de firma de base de roles. Lo que puede considerarse como un protocolo de acceso a esa información y que ayudará un auditor a conocer los usuarios que interactúan con un sistema de información.

Otro problema es que los datos se pueden perder en la nube explican Esther & Vasanthi (2019). La pérdida de datos puede ocurrir en cualquier infraestructura, independientemente de las medidas confiables tomadas por los proveedores de servicios en la nube. Por otro lado, Pasquier, Singh, & Powles (2018) mencionan que los dispositivos IoT y sus sistemas de habilitación son, por su la naturaleza, un testigo constante de nuestra vida cotidiana. Estos almacenan información en la nube de sus usuarios, un trabajo a futuro puede ser el desarrollar metodologías de auditoría que permitan evaluar a estos dispositivos IoT y la información sobre los usuarios que éstos generan.

Por su parte, en la investigación de Wang, Hui, & Li (2013) se debe proteger la privacidad de la información de los auditados al tratarse de datos almacenados en la nube. En resumen en trabajos como los de (Nong, Xiangyang, & Qiang (2001), Wenying & Xiong (2018), Xiang, Li, & Chen (2018) y Esther & Vasanthi (2019) se mencionan casos de estudio en los cuales se aplican metodologías de autoría de TI que resultan exitosas. El éxito total de una auditoría en términos generales depende de la cooperación del auditado y de la subjetividad con la que responden las preguntas de auditoría o la validez de la información que entregan para este proceso. En la Tabla 3 se da un resumen de las tendencias de la Auditoría de TI aplicada a la información y los trabajos.

Tendencia de Auditoría	Nro. Artículos
Auditoría de TI a las organizaciones	12
Auditoría de TI al cloud	6
Total	18

Tabla 4 – Tendencias de la Auditoría de TI en la información de las organizaciones

4. Discusión

Sobre las dificultades de la auditoria informática tenemos los principales puntos:

- Reportes Negativos: por la falta de una infraestructura adecuada los resultados no son 100% acertados, en la mayoría de los casos hace falta una tecnología robusta para tener seguridad al auditar con la ayuda de un computador.
- La ineficiente comunicación: al realizar un tipo de auditoria informática si bien

se tiene una comunicación con el auditado al no ser una auditoria presencial existe inconvenientes al intercambiar información durante la auditoria.
- Costos Exagerados: para realizar una auditoría informática se necesita equipos altamente costosos, así como de herramientas de software con licenciamiento que generan costos para el auditado.
- Falta de experiencia: cambiar la auditoria tradicional por una informática es complejo y como son herramientas nuevas se carece se información sobre la realización de una auditoria informática por la falta de experiencia al utilizar nuevos equipos y herramientas.

Tang Xing (2019) declara que relaciona la seguridad y los requisitos de eficiencia de las imágenes en la nube. Sin embargo, las soluciones existentes no tienen en cuenta las características de las imágenes en la nube y, por lo tanto, requieren enormes cómputos, comunicaciones y almacenamiento para generar, transferir y almacenar datos de autenticación. A demás, el resultado de la auditoría no se puede usar como evidencia para demostrar la culpabilidad del proveedor de servicios en la nube, ya que el verificador especificado por el cliente puede ocultar su mal comportamiento. En la Ilustración 1 se evidencia las dificultades presentes dentro de la auditoria informática desde el año 1998 hasta el año 2020 (Enero), teniendo 4 principales dificultades que varían en los diferentes años.

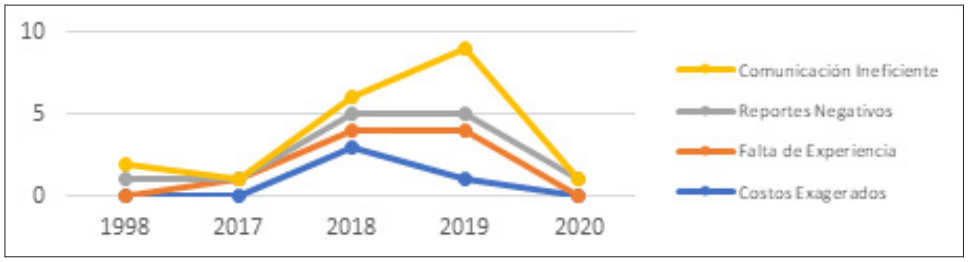

Figura 2 – Dificultades de la auditoría informática.

Las técnicas de los auditores son de gran importancia para evitar dificultades y fallas durante las auditorias informativas, los mismo que tienen que estar plenamente capacitados sobre qué es lo que se va a auditar, además Mary (2018) muestra cómo mejorar el proceso de gestión de piezas de repuesto en un operador de telecomunicaciones. Varias técnicas como: redes neuronales, proceso de jerarquía analítica y agentes de software se utilizan para implementar un prototipo de software que ha sido validado en un entorno operativo con una prueba de concepto, se aplicó una combinación de estas técnicas para administrar un inventario de repuestos y priorizar incidentes en un escenario tan complejo como la red de transmisión óptica de un importante operador de telecomunicaciones. La ayuda de la inteligencia artificial en los equipos facilita que un auditor pueda tomar decisiones dentro de un proceso de auditoria, tener la firmeza de decidir y estar seguro del procedimiento que se está realizando. En la Ilustración 2 se muestran las principales habilidades de un auditor a partir del año 1998 en donde

se evidencia la tendencia hacia el 2019 en disponer amplios conocimientos junto a la sinceridad presentados en los informes finales.

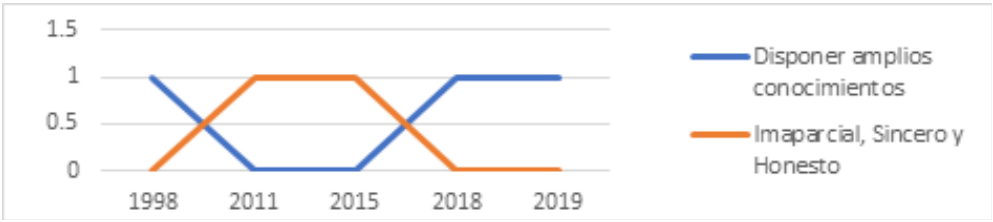

Figura 3 – Habilidades de un auditor.

Con respecto a la auditoría en el campo de la seguridad de la información es importante rescatar dos partes: La auditoría a datos alojados en Cloud; y la auditoría a datos alojados en SI (sistemas de información) de las organizaciones. En la Ilustración 3 se muestra que la Auditoría de la información que se encuentra en infraestructura propia de las organizaciones es la más común con el pasar del tiempo, sin embargo, a partir del 2018, la auditoría a datos almacenados en Cloud ha ido en constante crecimiento hasta estar casi a la par de la anterior.

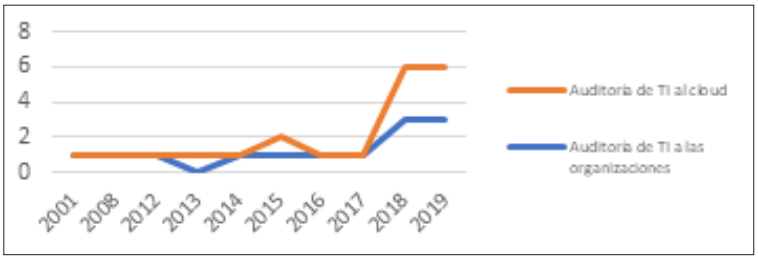

Figura 4 – Tendencias de auditoría de TI en la información.

El principal problema en este tipo de auditorías es la pérdida de información o de datos por problemas, en este caso, del cloud y de los proveedores de alojamiento de base de datos, lo que realmente imposibilita que el auditor genere un reporte de auditoría con hallazgos precisos y que puedan diagnosticar a detalle todas las anomalías que puedan presentarse en la información que la organización maneja. Por otro lado, al auditar los datos a sistemas de información con infraestructura propia del auditado se debe considerar las vulnerabilidades que estos poseen, ya que se encuentran expuestos a ataques maliciosos que pueden afectar de manera indeseable a una organización.

Afortunadamente en la actualidad las empresas que cuentan con un sistema informático, en su mayoría, llevan bitácoras (que registran interacciones de usuarios con el sistema) haciendo que así el auditor realice su trabajo sin basarse en suposiciones o incluso en la subjetividad, sino que, a partir de evidencias claras, pueda emitir su informe de hallazgos claro y preciso.

5. Conclusiones

Los artículos analizados en la redacción de este documento utilizaron técnicas de minería de datos para seleccionar su contenido en el ámbito de la Auditoría Informática. Como se evidenció, existen dificultades comunes en todos los casos de estudio en el apartado de la PI1, por ejemplo, los resultados que son erróneos que generan malestar al auditado, Lu Hui (2018) muestra sus pruebas al realizar estudio y análisis de calles en Japón con Google Street View genera resultados negativos, a esto se añade altos costos al utilizar herramientas tecnológicas para realizar una auditoría. La posición negativa de realizar auditorías informáticas se evidencia principalmente en los resultados que no satisfacen al usuario final.

Por otro lado, para poder garantizar que una auditoría informática se desarrolle de manera óptima, es necesario que auditores y auditados cooperen entre sí. Con respecto a los auditores, en la PI2 se analizaron las habilidades y actitudes que estos deberían poseer, como: experticia, exactitud y firmeza en resultados para tomar decisiones ante cualquier situación, ser discreto y una buena comunicación con el auditado siendo honesto sincero y parcial con los resultados, a fin de garantizar una auditoría de calidad. Como se observó en la discusión referente a la PI3, en la *Ilustración 3: Tendencias de Auditoría de TI en la información*, la auditoría a la información de las organizaciones tradicionalmente era realizada a la infraestructura instalada en las propias organizaciones y hasta la actualidad es lo que se continúa haciendo. Sin embargo, en los últimos años, Cloud Computing ha destacado en el almacenamiento de información de las organizaciones por lo que el área de la Auditoría de TI se ha adaptado a la información en estos servicios desde el 2014 aproximadamente, según muestra el número de investigaciones.

Finalmente, creemos que el uso de tecnologías emergentes como la minería de datos y algoritmos que permiten extraer información de auditoría a partir de sistemas informáticos y de sus usuarios, permitirá a los auditores informáticos eliminar la subjetividad, disminución de tiempo y costos en una auditoría.

Referencias

Aditya, B., & Ferdiana, R. (2018). Toward Modern IT Audit– Current Issues. *Proceedings - 2018 4th International Conference on Science and Technology, ICST 2018, 4*. doi:10.1109/ICSTC.2018.8528627

Atymtayeva, L., Bortsova, G., & Inoue, A. (2012). Methodology and Ontology of Expert System for Information Security Audit. *SCIS-ISIS 2012, 13*. doi:10.1109/SCIS-ISIS.2012.6505287

Bahri Leila, C. B. (2018). Enhanced Audit Strategies for Collaborative and Accountable Data Sharing in Social Networks. *IEEE CIC, 18*.

Bylica Wojciech, K. B. (2011). On Scalable Security Audit for Web Application According to ISO 27002. *Springer-Verlag Berlin Heidelberg, 160*.

Chang, S.-I., Wu, C.-C., & Chang, I.-C. (2008). The Development of a Computer Auditing System Sufficient for Sarbanes-Oxley Section 404— A Study on the Purchasing and Expenditure Cycle of the ERP System. *Information Systems Management, 25*. doi: 10.1080/10580530802151145

David, C. (2015). Cloud Computing Risk and Audit Issue. *Elsevier, 42*.

Esther, D., & Vasanthi, N. (2019). LDAP: a lightweight deduplication and auditing protocol for secure data storage in cloud environment. *Cluster Computing*. doi:https://doi.org/10.1007/s10586-017-1382-6

Gepp Adrian, L. M. (2018). Big data techniques in auditing research and practice: Current trends and future opportunities. *Elsevier BV*.

Han, J., Lin, Y., & Chen, W. (2018). A Lightweight And privacy-preserving public cloud auditing scheme without bilinear pairings in smart cities. *Computer Standards and Interfaces, 62*. doi:doi:10.1016/j.csi.2018.08.004

Hanibuchi, N. I. (2019). Virtual audits of streetscapes by crowdworkers. *Elsevier BV, 79*.

Hoffman Benjamin, S. D. (2018). The impact of client information technology capability on audit pricing. *Elsevier Ltd., 29*.

Huan Feiqi, V. M. (2019). Applying robotic process automation (RPA) in auditing: A framework. *Elsevier Ltd., 35*.

Kumar, R., & Singh, G. (2018). ANALYSIS AND DESIGN OF AN OPTIMIZED SECURE. *Materials Today, 5*(1). doi: https://doi.org/10.1016/j.matpr.2017.11.180

Li, S.-H., Yen, D., & Chuang, Y.-P. (2016). A Real-Time Audit Mechanism Based on the Compression Technique. *ACM Transactions on Management Information Systems, 8*(2). doi:http://dx.doi.org/10.1145/2629569

Lu Hui, C. H. (2018). The Research on Security Audit for Information System Classified Protection. *Springer Nature Switzerland*.

M., A. (2018). Auditing Albaha University Network Security using in-house Developed Penetration Tool. *Institute of Physics Publishing, 978*.

Manita Riadh, E. N. (2020). The digital transformation of external audit and its impact on corporate governance. *Elsevier Ltd., 150*.

Mary, M. (2018). Optimizing the Spare Parts Management Process in a Communication Network. *Elsevier* .

Nong, Y., Xiangyang, L., & Qiang, C. (2001). Probabilistic Techniques for Intrusion Detection. *IEEE TRANSACTIONS ON SYSTEMS, 31*(4).

Pasquier, T., Singh, J., & Powles, J. (2018). Data provenance to audit compliance with privacy policy in the Internet of Things. *Personal and Ubiquitous Computing, 22*. doi:10.1007/s00779-017-1067-4

Pedrosa Isabel, C. C. (2019). Determinants adoption of computerassisted auditing tools (CAATs). *Springer-Verlag London Ltd*.

Razaque Abdul, R. S. (2017). Privacy preserving model: a new scheme for auditing cloud stakeholders. *Springer Berlin Heidelberg*.

Siew Eu Gene, R. K. (2019). Organizational and environmental influences in the adoption of computerassisted audit tools and techniques (CAATTs) by audit firms in Malaysia. *Elsevier Ltd*.

Strous, L. (1998). Audit of information System: The Need for Cooperation. *Springer, 15211*.

Swathy, K., & Velvizhi, N. (2014). Public Audit on Dynamic data preserving user identity and data freshness. *2014 Sixth International Conference on Advanced Computing (ICoAC)*. doi:10.1109/ICoAC.2014.7229741

Tang Xing, H. Y. (2019). Efficient Real-Time Integrity Auditing With Privacy-Preserving Arbitration for Images in Cloud Storage System. *IEEE Accesss Computer Science*.

Thomé, J., Khin, L., & Bianculli, D. (2018). Security Slicing for Auditing Common Injection Vulnerabilities. *Journal of Systems and Software*. doi:https://doi.org/10.1016/j.jss.2017.02.040

Vasarhely Miklos, H. F. (2018). "The Continuous Audit of Online Systems".

Wang, B., Hui, L., & Li, M. (2013). Privacy-Preserving Public Auditing for Shared Cloud Data Supporting Group Dynamics. *2013 IEEE International Conference on Communications (ICC)*. doi:10.1109/ICC.2013.6654808

Wang, Y., Wu, Q., & Deng, R. (2017). Identity-Based Data Outsourcing with Comprehensive Auditing in Clouds. *IEEE Transactions on Information Forensics and Security, 12*(4). doi:10.1109/TIFS.2016.2646913

Wenying, Z., & Xiong, L. (2018). Secure sustainable storage auditing protocol (SSSAP) with efficient key updates for cloud computing. *Sustainable Computing: Informatics and Systems*. doi:https://doi.org/doi:10.1016/j.suscom.2018.03.002

Xiang, T., Li, X., & Chen, F. (2018). Achieving verifiable, dynamic and efficient auditing for outsourced. *Journal of Parallel and Distributed Computing*. doi:https://doi.org/10.1016/j.jpdc.2017.10.004