

APLICACIÓN DE HERRAMIENTAS TECNOLÓGICAS PARA LA EVALUACIÓN DEL CONTROL INTERNO INFORMÁTICO

APPLICATION OF TECHNOLOGICAL TOOLS FOR THE EVALUATION OF INTERNAL COMPUTER CONTROL

Freddy Enrique Triana Litardo^{1*}

¹ Universidad Técnica Estatal de Quevedo. Ingeniero en sistemas; Magister en Conectividad y Redes de Ordenadores. ORCID: <https://orcid.org/0000-0002-3475-9774>. Correo: ftriana@uteq.edu.ec

Jefferson Xavier Bravo Salvatierra²

² Universidad Técnica Estatal de Quevedo. Ingeniero en Sistemas – Magister en Informática Empresarial. ORCID: <https://orcid.org/0000-0001-9566-3429>. Correo: jbravo@uteq.edu.ec

José Nolberto Macías Véliz³

³ Universidad Técnica Estatal de Quevedo. Licenciado en Sistemas Computacionales - Máster Universitario en Matemática y Computación. ORCID: <https://orcid.org/0000-0001-9312-7331>. Correo: jnmacias@uteq.edu.ec

* Autor para correspondencia: ftriana@uteq.edu.ec

Resumen

Las auditorías del control interno informático son una prioridad para las grandes, medianas y pequeñas empresas en Ecuador, por esta razón se han desarrollado técnicas y metodologías para gestionar las auditorías de Tecnologías de la Información (TI), con el fin de evitar la propagación de amenazas y riesgos dentro de las organizaciones. Este documento analiza el control interno informático en las instituciones ecuatorianas, y propone un procedimiento para la realización sistemática de auditorías internas para la evaluación del control interno informático, a partir de la utilización de herramientas tecnológicas. En la presente investigación se propone un procedimiento para la evaluación del control interno informático de las instituciones ecuatorianas, haciendo uso de herramientas tecnológicas. El procedimiento propuesto, consta de 4 actividades principales: Planeación, Respaldo, Ejecución y Reporte. Estas actividades han sido definidas para evaluar el control interno en las instituciones del Ecuador. Las actividades están previstas para ser realizada por un equipo de auditores internos. Se realizó una encuesta a 9 expertos en auditoría informática. El procedimiento propuesto fue evaluado por los auditores internos como Muy adecuado para ser implementado en las instituciones ecuatorianas.

Palabras clave: control interno informático; procedimiento; CAAT; herramientas tecnológicas; auditoría interna.

Abstract

Internal computer control audits are a priority for large, medium and small companies in Ecuador, for this reason techniques and methodologies have been developed to manage Information Technology (IT) audits, in order to prevent the spread of threats and risks within organizations. This document analyzes internal computer control in Ecuadorian institutions, and proposes a procedure for the systematic performance of internal audits for the evaluation of internal computer control, based on the use of technological tools. In the present investigation, a procedure is proposed for the evaluation of the internal computer control of the Ecuadorian institutions, making use of technological tools. The proposed procedure consists of 4 main activities: Planning, Support, Execution and Report. These activities have been defined to evaluate the internal control in the institutions of Ecuador. The activities are planned to be carried out by a team of internal auditors. A survey was conducted on 9 IT audit experts. The proposed procedure was evaluated by the internal auditors as Very suitable to be implemented in Ecuadorian institutions.

Keywords: *internal computer control; process; CAAT; Technological tools; internal audit.*

Fecha de recibido: 22/07/2022

Fecha de aceptado: 05/10/2022

Fecha de publicado: 06/10/2022

Introducción

Con el rápido desarrollo de la tecnología informática, la informatización global se ha convertido en la tendencia general del desarrollo humano. Los procesos institucionales son programados desde la computadora en red, lo cual ha brindado servicios de información convenientes y rápidos a los especialistas y directivos responsables de la organización de procesos y toma de decisiones (Boiko et al., 2019). Utilizar sistemas informáticos se ha convertido en una garantía importante para el desarrollo de las empresas. Sin embargo, debido a las características de la red informática, como la apertura, la interconexión y el control de acceso, el problema de la sistematización de la información institucional de la red informática se ha vuelto un tema de máxima prioridad, y el control de seguridad es particularmente importante (Berdik et al., 2021).

Con el advenimiento de la era de los grandes datos, el desarrollo de los procesos en red, el avance de la ciencia y la tecnología sin duda ha acelerado el proceso de información social. El procesamiento de información institucional y empresarial se ha convertido en la tendencia necesaria de estos tiempos (Li et al., 2021). El método tradicional de auditoría manual de las empresas, ha sido reemplazado gradualmente por la informatización de procesos, y entró oficialmente en la etapa de informatización. En el proceso de desarrollo empresarial, la información junto a los recursos humanos, son de los principales factores que se deben priorizar (Frauenstein & Flowerday, 2020). De la integridad y disponibilidad de la información almacenada

en los equipos de cómputo depende el éxito o el fracaso de las operaciones que se realizan a nivel empresarial (Rodríguez, Castro, et al., 2021). En este trabajo analiza los problemas existentes en el control interno informático, las habilidades y responsabilidades del auditor interno y propone las medidas preventivas correspondientes.

Las auditorías del control interno informático son una prioridad para las grandes, medianas y pequeñas empresas en Ecuador, por esta razón se han desarrollado técnicas y metodologías para gestionar las auditorías de Tecnologías de la Información (TI), con el fin de evitar la propagación de amenazas y riesgos dentro de las organizaciones (Chang et al., 2019). Es la garantía básica para el funcionamiento normal del sistema de control interno de la red informática, reconocer los problemas de seguridad que puedan surgir y tomar las técnicas preventivas y contramedidas necesarias (Chang et al., 2020). Este documento analiza el control interno informático en las instituciones ecuatorianas, y propone un procedimiento para la realización sistemática de auditorías internas para la evaluación del control interno informático, a partir de la utilización de herramientas tecnológicas.

Materiales y métodos

Para el desarrollo del presente trabajo se investigaron las metodologías y buenas prácticas para gestionar auditorías para la evaluación del control interno informático, buscando las herramientas tecnológicas más alineadas a la recolección de evidencias, así como a la ejecución de las pruebas que se realizan a los controles en los sistemas de información. Lo anterior tiene como objetivo realizar una selección diagnóstica de las herramientas tecnológicas disponibles para la recolección de evidencia de auditoría de control interno informático, así como identificar las características de las aplicaciones utilizadas en la gestión de auditorías de TI, también llamadas Técnicas de Auditoría Asistida por Computadora (CAATS), con sus aspectos funcionales para categorizar su efectividad frente a las auditorías internas aplicadas. Este análisis sirve como base para proponer un procedimiento para la recolección de evidencias documentales en pruebas de cumplimiento en auditorías de control interno informático.

Control Interno Informático

El control es una función inherente a todos aquellos miembros de una organización que tienen a su cargo la ejecución de planes. De ahí que sea una función que no solo es responsabilidad de los niveles gerenciales superiores, sino de los niveles gerenciales bajo. Según la Organización Internacional de Entidades Fiscalizadoras Superiores, constituye una herramienta gerencial usada para brindar una seguridad razonable de que los objetivos gerenciales están siendo alcanzados. De acuerdo con Durán Ruiz, el control interno constituye una base de seguridad de cumplir con aspectos importantes dentro de la organización como son: la eficacia, la eficiencia, economía y legalidad (Durán Ruiz, 2018).

En la última década se ha notado un cambio de paradigma en el volumen de trabajo y datos en el mundo digital. A medida que aumentaba el volumen, la velocidad se convirtió en un desafío y el acceso rápido a los datos se convirtió en una necesidad. Grandes volúmenes de datos almacenados con las operaciones empresariales en dominios propios o de terceros, representa una amenaza para la seguridad e integridad de la

información institucional (Rodríguez, González, et al., 2021). El control interno informático es esencial para mantener de manera eficaz la tríada: Confidencialidad, Integridad y Autenticidad de la información.

El objetivo principal del control interno informático es monitorear y evaluar la seguridad del sistema y la información de auditoría. El sistema de control interno tiene como principio ayudar a las organizaciones a saber qué se requiere exactamente para proteger sus repositorios digitales y cuáles son las vulnerabilidades que permiten implementar una solución factible para la gestión de la seguridad (Buslepp et al., 2019). Así mismo abarca otros procesos cómo conocer sí se está generando y almacenando la información necesaria para dar trazabilidad, mantenimiento y veracidad a los procesos institucionales (Chen et al., 2020).

La auditoría para evaluar el control interno informático acumula, evalúa y prueba los datos de los sistemas de una organización y determina sí los sistemas protegen los datos, administran la integridad de los datos y se manejan de manera efectiva para lograr los objetivos comerciales de la organización. Las aplicaciones basadas en web están ampliamente expuestas y disponibles a través de Internet (Bryan, 2017).

La aplicación de herramientas tecnológicas para la evaluación del control interno informático involucra un proceso de identificación y extracción de evidencias digitales de un dispositivo digital que almacena información relevante de la institución y la preservación de la evidencia digital para mantener la transparencia de los procesos empresariales derivados de las operaciones que a diario se realizan en una empresa (Zhang et al., 2007). El campo del control interno informático necesita herramientas y técnicas para llevar a cabo la auditoría interna de evidencia digital y extraer artefactos importantes de ella en caso de violaciones cometidas desde un dispositivo. También apoya concejo directivo con un protocolo claro para llevar a cabo la investigación informática.

Fundamentos de Auditoría Interna

Los mecanismos de auditoría y control de los sistemas de información aseguran que un sistema de información está satisfaciendo los requisitos necesarios en diferentes áreas. La auditoría para la evaluación del control interno informático contribuye a la planificación, supervisión y toma de decisiones dentro de la organización (Pizzi et al., 2021). Hay varias definiciones para la auditoría informática, diversos autores concuerdan en que es un examen de los controles de gestión dentro de una tecnología de la información para recopilar y evaluar evidencia de los procesos de control dentro de la organización, lo que mejora el nivel de servicios proporcionados por la organización en general (Alzeban & Gwilliam, 2014).

Herramientas tecnológicas para realizar auditorías informáticas

Resulta prácticamente imposible completar un proceso de auditoría informática en condiciones humanas. Por lo tanto, los auditores internos que evalúan el control interno informático utilizan herramientas de auditoría de software para ayudar a realizar todas sus tareas de auditoría. Uno de estos tipos que respaldan a los auditores son las Herramientas de Auditoría Asistidas por Computadora (CAAT). Los CAAT se definen como aquellas herramientas y técnicas habilitadas por tecnología que aumentan la eficiencia de la realización de auditorías (Bierstaker et al., 2014). Los CAAT apoyan y ayudan a los auditores internos a completar el proceso de auditoría dentro de una organización. Permiten a las empresas realizar auditorías y controles continuos para ayudar a las actividades comerciales y mejorar la eficiencia de las tareas de la organización (Siew et al.,

2020). En la Figura 1 se definen algunas de las utilidades el empleo de los CAAT en la realización de auditorías informáticas.

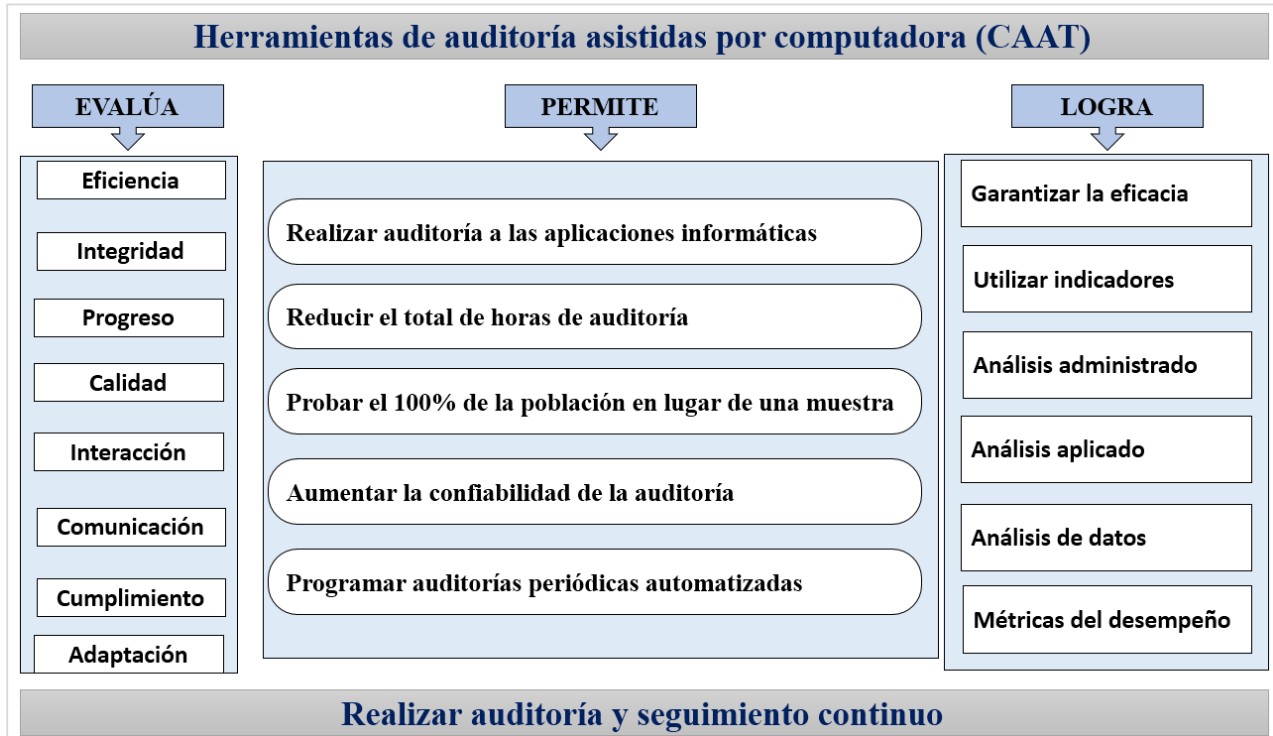


Figura 1. Utilidad de los CAAT en la realización de auditorías informáticas.

Fuente: Elaborado por los autores.

El objetivo de la auditoría es garantizar la eficacia de los controles internos, que están diseñados para facilitar las actividades de gestión de la empresa. Los auditores deben decidir el alcance de sus proyectos y desarrollar sus procesos CAAT con base en las políticas de auditoría. El desempeño de las CAAT se puede medir utilizando indicadores o métricas del desempeño del proyecto en equipo, como la eficiencia, la integridad, el cumplimiento o la adaptación al progreso del trabajo, la calidad de los resultados, la interacción y la comunicación. El uso de CAAT permite que las funciones de auditoría interna realicen análisis en profundidad de los datos digitales de las organizaciones (Liang et al., 2001).

Las Normas Internacionales para la Práctica Profesional de la Auditoría Interna, a través de la Norma 1220 de Auditoría Interna: Debido Cuidado Profesional, alienta a los auditores internos a utilizar herramientas basadas en tecnología durante la realización de trabajos de auditoría interna. Entre estas herramientas de base tecnológica, los autores de la presente investigación, recomiendan las CAAT listadas en la Tabla 1, para realizar auditorías internas para el control interno de las organizaciones (Zaiceanu et al., 2015).

Tabla 1. Características de las CAAT que respaldan al control interno informático.

CAAT	Configuración de Auditoría	Reportes	IU amigable	Sistema Operativo	Facilidad de uso
Onspring	Sí	Sí	Sí	Macintosh	Buena
ACL	Sí	Sí	Sí	Linux, Macintosh, Windows	Buena
IDEA	Sí	Sí	Sí	Windows	Buena
Xandria	Sí	Sí	Sí	Windows	Buena
Delphix	Sí	Sí	Sí	Linux	Buena
Active@	Sí	Sí	Sí	Windows	Buena
AuditBoard	Sí	Sí	Sí	Windows	Buena
Belarc Advisor	Sí	Sí	Sí	-	Buena
WinAudit	Sí	Sí	Sí	Windows	Buena
Janco	Sí	Sí	No	Windows	Buena
Ecomply	Sí	Sí	Sí	Windows	Buena
Cookie Assistant	Sí	Sí	Sí	Windows	Buena
Iubenda	Sí	Sí	Sí	Linux, Macintosh	Buena
BigID	Sí	Sí	Sí	Linux, Macintosh	Buena

Fuente: Elaborada por los autores.

Aunque las herramientas CAAT puedan tener múltiples utilidades, existen desafíos actuales para su implementación y utilización. Estudios empíricos y reportes técnicos (Debreceny et al., 2005; Jaber & Abu Wadi, 2018; Janvrin et al., 2008) han coincidido en los siguientes:

- Falta de compatibilidad de la aplicación en diferentes navegadores.
- Las interfaces de usuario necesitan adaptación sobre diferentes entornos.
- El módulo de reportes necesita actualizaciones y ajustes personalizados.
- El soporte en línea puede estar desactualizado y resultar incompetente.
- Actualizar el sistema puede ser defectuoso y costoso.
- Falta de foros de soporte y comunidad para los nuevos CAAT.
- La mayor curva de aprendizaje para funciones avanzadas.
- Los informes con gráficos multimedia e información tabular no se generan fácilmente.
- La necesidad de múltiples CAAT puede ser muy costosa.

En la literatura científica se identificaron algunos factores que los auditores deben tener en cuenta para la selección de la herramienta tecnológica más adecuada para realizar las tareas requeridas. Las CAAT tienen algunas características y factores básicos que afectan la decisión del auditor mientras busca una herramienta adecuada, a saber:

- **Facilidad de uso:** una medida de la facilidad de uso de la herramienta por parte de los usuarios previstos.
- **Extracción de datos:** incluye la capacidad de acceder a una amplia variedad de archivos de datos desde diferentes plataformas y de integrar datos con diferentes formatos.
- **Definición de atributos:** Capacidad para definir campos y seleccionar entre formatos estándar.
- **Análisis:** Funcionalidad basada en menús para procesar comandos de análisis.

- **Consultas:** Construcción de consultas y ajustes simplificados.
- **Multiplataforma:** Capacidad de ajustarse a la plataforma y sistema operativo utilizado en la organización.
- **Reportes:** Documentación de soporte e informes periódicos de auditoría.

Resultados y discusión

Procedimiento para la evaluación del control interno informático

En la presente investigación se propone un procedimiento para la evaluación del control interno informático de las instituciones ecuatorianas, haciendo uso de herramientas tecnológicas. La figura 2 muestra el procedimiento propuesto:

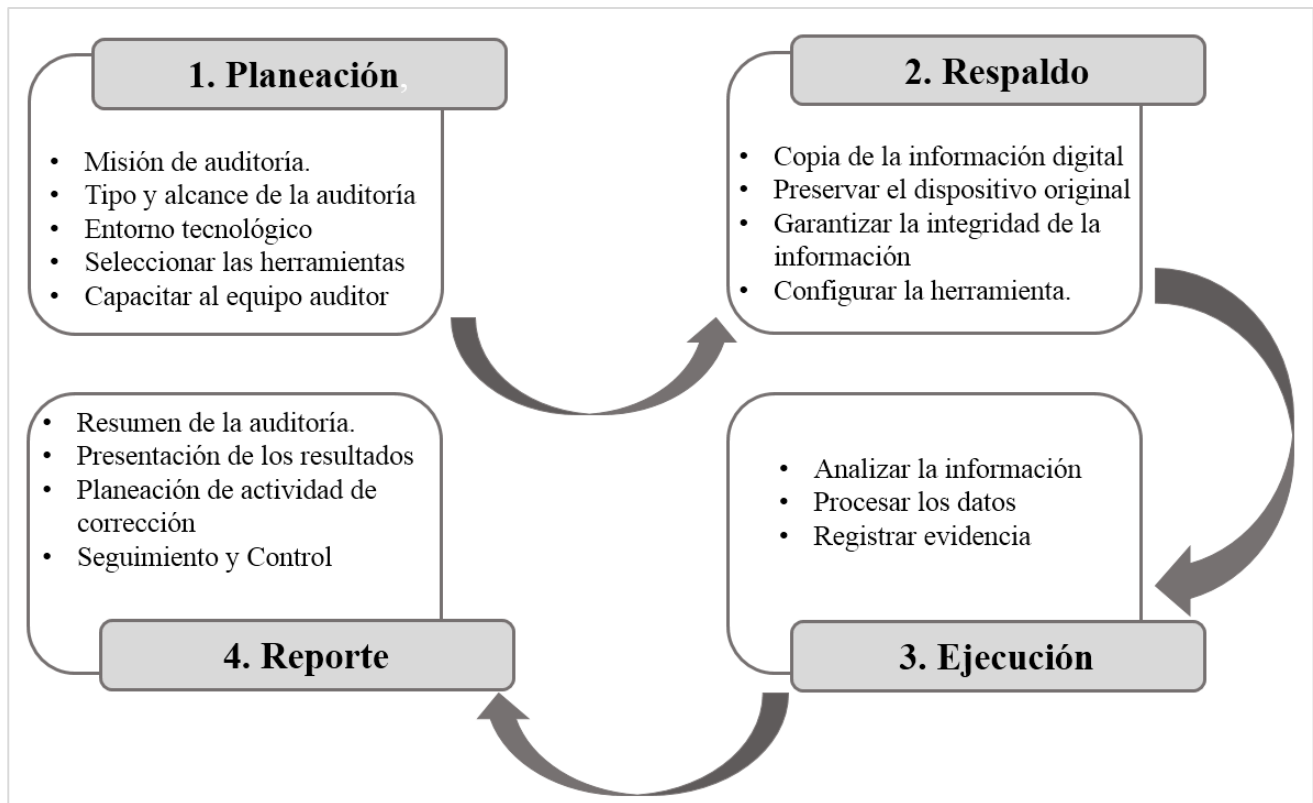


Figura 2. Procedimiento para la evaluación del control interno informático.

Fuente: Elaborado por los autores.

En la figura 2 se muestra el procedimiento propuesto, el cual consta de 4 actividades principales: Planeación, Respaldo, Ejecución y Reporte. Estas actividades han sido definidas para evaluar el control interno en las instituciones del Ecuador. Las actividades están previstas para ser realizada por un equipo de auditores internos. Para cada una de ellas se ha propuesto un conjunto de acciones, como sigue:

Actividad 1: Planeación

En esta actividad de determinar la misión de auditoría, y de definen los objetivos y las prioridades que la institución desea evaluar. Siendo necesario definir con antelación y por escrito el tipo de auditoría a realizar y el alcance que esta tendrá. Para realizar la planeación es muy importante considerar y evaluar el entorno tecnológico de la empresa, ya que serán auditados procesos informáticos que pueden estar o no conectados a la red.

Como parte de la actividad se deben seleccionar las herramientas adecuadas para automatizar el proceso de auditoría de manera tal que se abarque la mayor cantidad de procesos posibles con la integridad requerida. Una vez seleccionada las herramientas será necesario capacitar al equipo auditor en el uso de las herramientas seleccionadas.

Actividad 2: Respaldo

Esta actividad tiene mucha importancia, y debe ser cumplida con máximo apego al procedimiento. Se propone la realización de múltiples copias de seguridad, clones e imagen del software instalado y del total de información almacenada en el dispositivo digital que será auditado. Es responsabilidad del equipo auditor preservar el dispositivo original para evitar cualquier alteración en los datos.

Esta actividad incluye la identificación de los dispositivos digitales que serán auditados, siendo necesario registrar su número de serie, lugar físico en el que se encuentra almacenado, fecha en que comienza el proceso de auditoría, hora, usuarios del dispositivo, dispositivos externos conectados, y demás evidencias que se pueden recopilar.

Actividad 3: Ejecución

En esta actividad el auditor analiza y reconstruye los datos que pueden conducir a alguna conclusión importante para los interesados en la auditoría. Cada hallazgo se registra en documentos que se presentarán en las conclusiones de la auditoría integrados en un informe. En el proceso de registro de evidencia se prepara un documento de cadena de auditoría. Cada detalle de todo el hardware, software, usuarios con acceso a cada nivel de información, trazas, se registra en este documento con fecha y hora exactas. Se complementa con los gráficos y multimedias construidos con la CAAT utilizada.

Actividad 4: Reporte

En esta actividad se resume el proceso de auditoría y también la conclusión arribada de ella. Este documento está preparado en términos sumamente sencillos con las referencias claramente hechas, para que sea entendible por todos los participantes e interesados en el proceso de auditoría informática.

Consulta a expertos sobre el procedimiento propuesto

Una vez descrito el procedimiento, fue presentado a un conjunto de expertos en auditorías informáticas que aceptaron a formar parte del proceso de capacitación. Al finalizar se realizó una encuesta a 9 expertos, con formación profesional en auditoría interna, y con más de 5 años de experiencia en la auditoría informática. Los resultados fueron los siguientes:

Pregunta 1: ¿Qué utilidad le confiere a las CAAT propuestas en esta investigación?

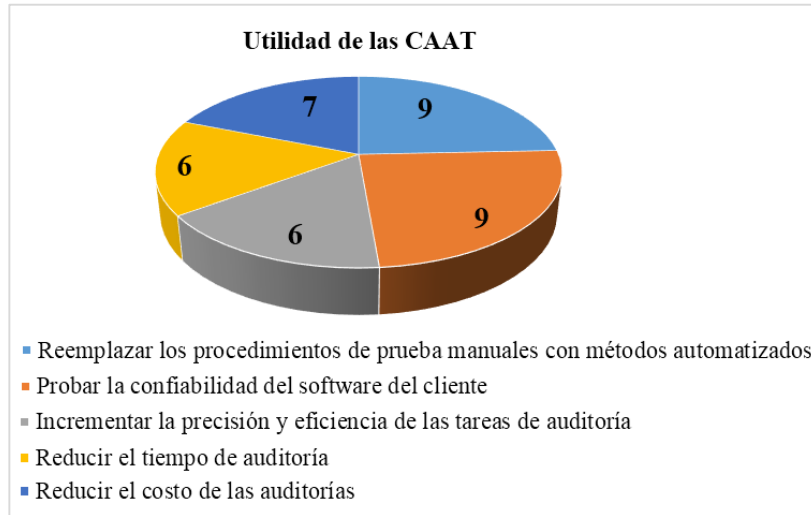


Figura 3. Utilidad expresada por los expertos en auditoría interna sobre el uso de las CAAT.

Fuente: Elaborado por los autores con información de la encuesta.

Pregunta 2: ¿Cuáles son los factores que usted tiene en cuenta para la selección de las CAAT en una auditoría informática?

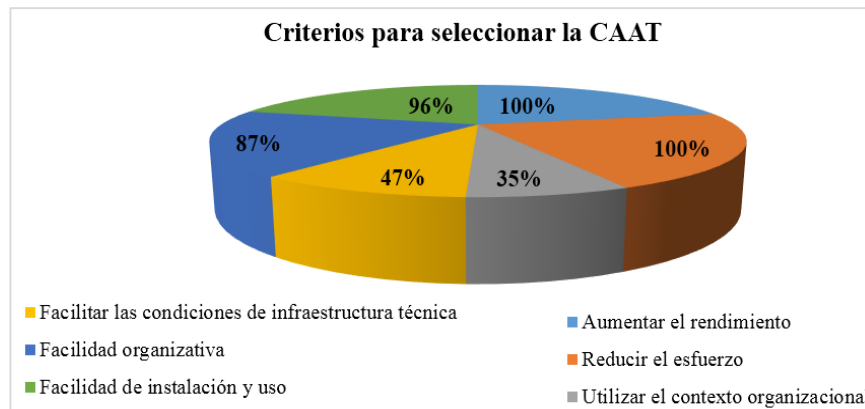


Figura 4. Criterios de selección del CAAT.

Fuente: Elaborado por los autores con información de la encuesta.

Pregunta 3: ¿Una vez analizado y experimentado el procedimiento propuesto, cómo valora su utilidad?

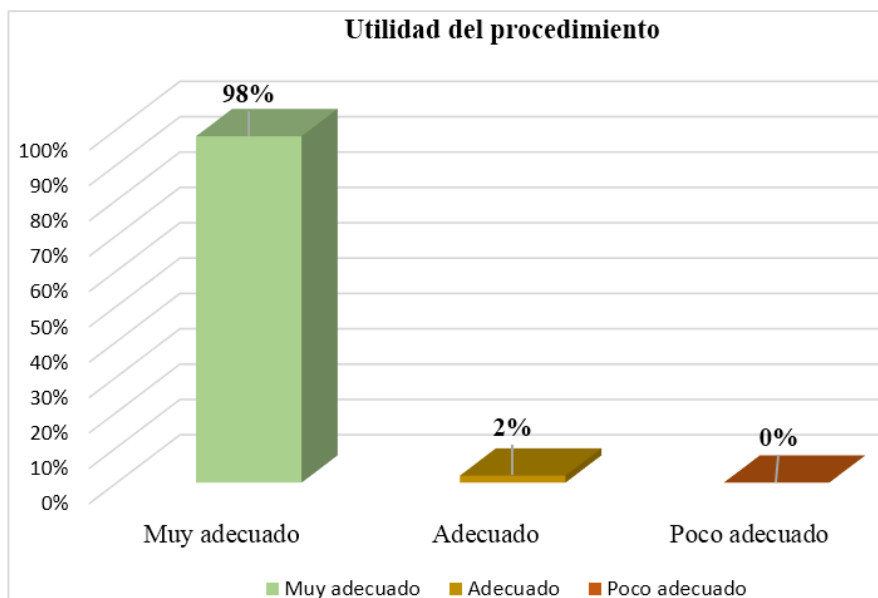


Figura 5. Valoración de los expertos sobre el procedimiento propuesto.
Fuente: Elaborado por los autores con información de la encuesta.

Pregunta 4: ¿Una vez analizado y experimentado el procedimiento propuesto, lo utilizaría usted en una auditoría profesional dentro de la organización que representa?

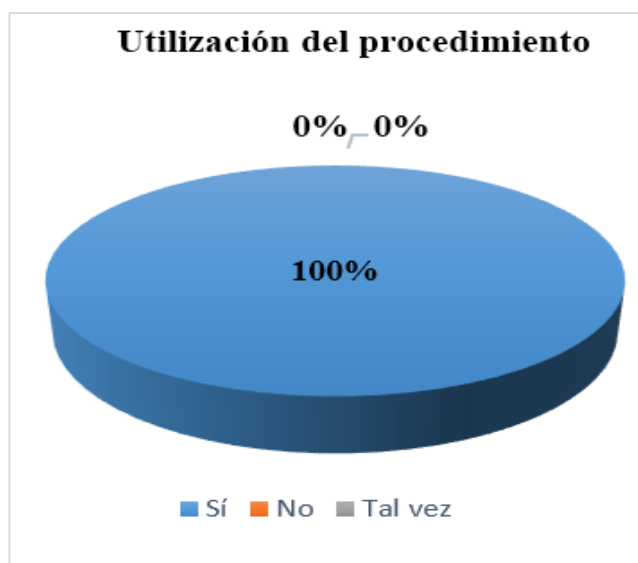


Figura 6. Interés en utilizar el procedimiento propuesto.
Fuente: Elaborado por los autores con información de la encuesta.

Las CAAT se pueden categorizar ampliamente para cubrir varios dominios tales como: análisis de datos, evaluación de seguridad, sistemas operativos, sistema de gestión de bases de datos y herramientas de prueba de software y código. La categorización de estas herramientas ayuda a las instituciones a satisfacer sus requisitos de auditoría. Pueden realizar procedimientos de auditoría fiables y ofrecer resultados de auditoría rápidos y precisos. Por lo tanto, la necesidad de CAAT es cada vez mayor, ya que permiten a los auditores ejecutar sus tareas de revisión y monitoreo de manera efectiva y completa.

Conclusiones

Las organizaciones de hoy operan y compiten en la era de la información. La información se ha convertido en un recurso clave para la mayoría de las organizaciones, economías y sociedades. Debido al desarrollo de la industria de TI, se considera vital para todas las organizaciones, ya sean lucrativas o no lucrativas, realizar auditorías internas sistemáticas para evaluar el control interno informático.

Supervisar los ataques y peligros de los que está sujeta la organización de datos de las asociaciones es cada vez más problemático, debido al desarrollo característico de los ataques, peligros y vulnerabilidades, avanzados por los avances de la innovación. El compromiso fundamental de este trabajo es comprender y administrar las herramientas de seguridad de los sistemas, para las vulnerabilidades del sistema y las aplicaciones. Este trabajo describe diferentes métodos y herramientas de auditoría de aplicaciones y sistemas. Los auditores de aplicaciones y sistemas continúan trabajando con las diferentes herramientas disponibles de escaneo y auditoría para proteger los datos. Se requiere una auditoría del sistema para proteger el sistema de vulnerabilidades.

El procedimiento propuesto, consta de 4 actividades principales: Planeación, Respaldo, Ejecución y Reporte. El procedimiento fue evaluado por los auditores internos expertos como Muy adecuado para ser implementado en las instituciones ecuatorianas.

Referencias

- Alzeban, A., & Gwilliam, D. (2014). Factors affecting the internal audit effectiveness: A survey of the Saudi public sector. *Journal of International Accounting, Auditing and Taxation*, 23(2), 74-86. <https://www.sciencedirect.com/science/article/pii/S1061951814000214>
- Berdik, D., Otoum, S., Schmidt, N., Porter, D., & Jararweh, Y. (2021). A survey on blockchain for information systems management and security. *Information Processing & Management*, 58(1), 102397. <https://www.sciencedirect.com/science/article/pii/S030645732030892X>
- Bierstaker, J., Janvrin, D., & Lowe, D. J. (2014). What factors influence auditors' use of computer-assisted audit techniques? *Advances in Accounting*, 30(1), 67-74. <https://www.sciencedirect.com/science/article/pii/S0882611013000631>
- Boiko, A., Shendryk, V., & Boiko, O. (2019). Information systems for supply chain management: uncertainties, risks and cyber security. *Procedia Computer Science*, 149, 65-70. <https://www.sciencedirect.com/science/article/pii/S1877050919301152>

- Bryan, D. B. (2017). Organized labor, audit quality, and internal control. *Advances in Accounting*, 36, 11-26. <https://www.sciencedirect.com/science/article/pii/S0882611016301079>
- Buslepp, W., Legoria, J., Rosa, R., & Shaw, D. (2019). Misclassification of audit-related fees as a measure of internal control quality. *Advances in Accounting*, 46, 100425. <https://www.sciencedirect.com/science/article/pii/S0882611018301962>
- Chang, S.-I., Chang, L.-M., & Liao, J.-C. (2020). Risk factors of enterprise internal control under the internet of things governance: A qualitative research approach. *Information & Management*, 57(6), 103335. <https://www.sciencedirect.com/science/article/pii/S037872062030272X>
- Chang, Y.-T., Chen, H., Cheng, R. K., & Chi, W. (2019). The impact of internal audit attributes on the effectiveness of internal control over operations and compliance. *Journal of Contemporary Accounting & Economics*, 15(1), 1-19. <https://www.sciencedirect.com/science/article/pii/S1815566918301589>
- Chen, H., Yang, D., Zhang, J. H., & Zhou, H. (2020). Internal controls, risk management, and cash holdings. *Journal of Corporate Finance*, 64, 101695. <https://www.sciencedirect.com/science/article/pii/S0929119920301395>
- Debreceny, R., Lee, S. L., Neo, W., & Toh, J. S. (2005). Employing generalized audit software in the financial services sector: Challenges and opportunities. *Managerial Auditing Journal*. <https://www.emerald.com/insight/content/doi/10.1108/02686900510606092/full/html>
- Durán Ruiz, A. M. (2018). El nuevo enfoque de riesgo en el control interno de la administración pública venezolana. *Sapientia Organizacional*, 5(9), 81-104. <https://www.redalyc.org/journal/5530/553056570005/553056570005.pdf>
- Frauenstein, E. D., & Flowerday, S. (2020). Susceptibility to phishing on social network sites: A personality information processing model. *Computers & Security*, 94, 101862. <https://www.sciencedirect.com/science/article/pii/S0167404820301346>
- Jaber, R. J., & Abu Wadi, R. M. (2018). Auditors' usage of computer-assisted audit techniques (caats): Challenges and opportunities. Conference on e-Business, e-Services and e-Society,
- Janvrin, D., Lowe, D. J., & Bierstaker, J. (2008). Auditor acceptance of computer-assisted audit techniques. *Iowa State University, Arizona State University and Villanova University*, 4. http://www.mtc.gov/uploadedfiles/multistate_tax_commission/audit_program/resource/auditoracceptance.pdf
- Li, H., Wu, Y., Cao, D., & Wang, Y. (2021). Organizational mindfulness towards digital transformation as a prerequisite of information processing capability to achieve market agility. *Journal of Business Research*, 122, 700-712. <https://www.sciencedirect.com/science/article/pii/S0148296319306241>
- Liang, D., Lin, F., & Wu, S. (2001). Electronically auditing EDP systems: With the support of emerging information technologies. *International Journal of Accounting Information Systems*, 2(2), 130-147. <https://www.sciencedirect.com/science/article/pii/S1467089501000148>
- Pizzi, S., Venturelli, A., Variale, M., & Macario, G. P. (2021). Assessing the impacts of digital transformation on internal auditing: A bibliometric analysis. *Technology in Society*, 67, 101738. <https://www.sciencedirect.com/science/article/pii/S0160791X2100213X>
- Rodríguez, A. R., Castro, V. F. R., González, A. d. C. R., Baque, N. A. C., & Tarragó, J. C. P. (2021). Aplicaciones de la Inteligencia Artificial en técnicas de minería de procesos. *Serie Científica de la*

- Universidad de las Ciencias Informáticas*, 14(7), 136-155.
<https://publicaciones.uci.cu/index.php/serie/article/view/920>
- Rodríguez, A. R., González, A. d. C. R., Tarragó, J. C. P., & Gálvez, D. L. D. (2021). Implementación de algoritmos de Inteligencia Artificial en la predicción de nuevos conocimientos mediante enseñanza constructivista. *Serie Científica de la Universidad de las Ciencias Informáticas*, 14(3), 131-141.
<https://publicaciones.uci.cu/index.php/serie/article/view/762>
- Siew, E.-G., Rosli, K., & Yeow, P. H. (2020). Organizational and environmental influences in the adoption of computer-assisted audit tools and techniques (CAATTs) by audit firms in Malaysia. *International Journal of Accounting Information Systems*, 36, 100445.
<https://www.sciencedirect.com/science/article/pii/S1467089518300411>
- Zaiceanu, A. M., Hlaciuc, E., & Lucan, A. N. C. (2015). Methods for risk identification and assessment in financial auditing. *Procedia economics and finance*, 32, 595-602.
<https://www.sciencedirect.com/science/article/pii/S2212567115014379>
- Zhang, Y., Zhou, J., & Zhou, N. (2007). Audit committee quality, auditor independence, and internal control weaknesses. *Journal of accounting and public policy*, 26(3), 300-327.
<https://www.sciencedirect.com/science/article/pii/S0278425407000208>