UNIVERSIDAD NACIONAL DE LA PLATA

Facultad de INFORMÁTICA
UNIVERSIDAD NACIONAL DE LA PLATA

Secretaria de Postgrado

MÉTODO DE AUDITORÍA INFORMÁTICA BASADO EN SISTEMAS DE PROCESAMIENTO AVANZADO DE DATOS QUE PERMITA MINIMIZAR EL RIESGO DE CALIDAD DE LOS RESULTADOS

Tesis Doctoral – Doctorado en Ciencias Informáticas

Autor	Director
Daisy Elizabeth Imbaquingo Esparza	Javier Díaz

La Plata – Prov. Buenos Aires, 2023

DEDICATORIA

A mis padres Lucy y Hugo, de ustedes aprendí el verdadero significado del amor incondicional. Su ejemplo de entrega, sacrificio y constante apoyo me ha dado las herramientas necesarias para enfrentar todos los desafíos de la vida. Les dedico este trabajo por todo lo que han hecho por mí y por amarme sin reservas.

A mi esposo José, por ser mi compañero en esta maravillosa aventura de la vida. Tu amor incondicional y apoyo constante me hacen sentir bendecida todos los días.

A mis hijos José Guillermo, Melannie y Victoria por su amor infinito, por darme el ánimo y las fuerzas necesarias para seguir, son mi mayor orgullo y alegría. Sus sonrisas iluminan mi mundo y su amor me llena de felicidad.

Daisy Imbaquingo

AGRADECIMIENTO

A Dios por siempre estar conmigo con sus bendiciones y fortaleciéndome para cumplir este sueño tan anhelado.

A mi familia por el apoyo y empuje en los momentos difíciles.
A los auditores amigos, que contribuyeron con el aporte a este trabajo.

A la Facultad de Informática de la Universidad Nacional de la Plata por permitirme ampliar y mejorar mis conocimientos con cursos y en esta formación doctoral.

Al personal administrativo de la secretaría de posgrado de la Facultad de Informática de la Universidad Nacional de la Plata por su gentil ayuda y colaboración en todo momento.

A la Universidad Técnica del Norte por brindarme la oportunidad de completar mi formación académica, en especial al Dr. Miguel Naranjo- Rector de esta noble institución quien con su ejemplo y apoyo constante ha hecho realidad este sueño.

A mi director de Tesis Javier Díaz y a mi gran amigo Mario Ron, por dirigirme, orientarme y ayudarme en la realización de este trabajo doctoral.

A mis amigos Cosme, Erick, Brizeida y Lorena por su apoyo y consejos constantes.

RESUMEN

Las Instituciones de Educación Superior (IES) no disponen de un método o marco referencial que apoye al proceso de auditoría, que haga uso de técnicas estratégicas especializadas, ni permitan minimizar los riesgos de calidad y seguridad en los resultados obtenidos, a fin de que puedan aportar como un servicio agregado a los demás que se brindan dentro de estas instituciones y permitan la evaluación o acreditación institucional. Si bien a nivel de IES, existen estudios de propuestas de guías de auditoría informática aplicando metodologías, se conoce que ninguna de ellas contempla los servicios y los procesos específicos que se desarrollan dentro de estas instituciones, con el objetivo de controlar y garantizar la seguridad de los activos tecnológicos frente a las diferentes amenazas e incidentes, así como determinar las oportunidades de mejora. El objetivo de esta investigación es desarrollar un Método de Auditoría Informática para Instituciones de Educación Superior (MAIIES) como apoyo metodológico al proceso de auditoría informática en las IES. Este método incluye la fase de planeación, ejecución, comunicación de resultados, validación y seguimiento del ejercicio de auditoría con cuarenta y siete actividades agrupadas en cada fase. La investigación comprende dos fases. Para la primera fase, se realizó una extensa revisión bibliográfica, la identificación de factores y métricas de calidad y seguridad de la información en auditorías, análisis de marcos referenciales, estudio de la situación actual en las IES de Ecuador que pertenecen a la Corporación Ecuatoriana para el Desarrollo de la Investigación y la Academia (CEDIA). En la segunda fase, se propone el diseño y estandarización del MAIIES.

Palabras clave: Auditoría informática, Instituciones de Educación Superior, calidad, seguridad, estándar.

ABSTRACT

Higher Education Institutions (HEI) do not have a method or referential framework to support the audit process, which makes use of specialized strategic techniques, or to minimize the risks of quality and security in the results obtained, so that they can contribute as an added service to the others provided within these institutions and allow institutional evaluation or accreditation. Although at the HEI level, there are studies of proposals for IT audit guides applying methodologies, it is known that none of them contemplates the specific services and processes that are developed within these institutions, with the objective of controlling and guaranteeing the security of technological assets in the face of different threats and incidents, as well as determining opportunities for improvement. The objective of this research is to develop an IT Audit Method for Higher Education Institutions (MAIIES) as a methodological support to the IT audit process in HEIs. This method includes the phase of planning, execution, communication of results, validation and follow-up of the audit exercise with forty-seven activities grouped in each phase. The research comprises two phases. For the first phase, an extensive literature review was carried out, identifying factors and metrics of quality and information security in audits, analysis of reference frameworks, study of the current situation in the HEIs of Ecuador that belong to the Ecuadorian Corporation for the Development of Research and the Academy (CEDIA). In the second phase, the design and standardization of the MAIIES is proposed.

Key words: IT audit, Higher Education Institutions, quality, security, standard.

"Technology is a gift of God. After the gift of life, it is perhaps the greatest of God´s gifts. It is the mother of civilizations, of arts and of sciences."
Freeman Dyson (1961 – Proyecto Orion)

"De vez en cuando, una nueva tecnología, un antiguo problema y una gran idea se convierten en una innovación».
Dean Kamen. Creador del Segway y el iBOT

"Si piensas que la tecnología puede solucionar tus problemas de seguridad, está claro que ni entiendes los problemas ni entiendes la tecnología"
Bruce Schneier (2004)

"Si decides hacer solo las cosas que sabes que van a funcionar, dejarás un montón de oportunidades encima de la mesa".
Jeff Bezos, fundador y director ejecutivo de Amazon

ÍNDICE

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

GLOSARIO

BD	Big Data
BI	Bussines Intelligence
CACES	Consejo de Aseguramiento de la Calidad de la Educación Superior
CEDIA	Coorporación Ecuatoriana para el Desarrollo de la Investigación y la Academia
CES	Consejo de Educación Superior
CFA	Análisis Factorial Confirmatorio
CI	Ciencia de la Información
COBIT	Control Objetives for Information and Related Technology
CSIRT	Computer Incident Response Team
ECA	European Court of Auditors
EGSI	Esquema Gubernamental de Seguridad de la Información
ENISA	Agencia Europea de Seguridad de las Redes y de la Información
HITRUST	Health Information Trust Alliance
IA	Inteligencia Artificial
IAASB	International Auditing and Assurance Standards Board
IEC	International Electrotechnical Commission
IES	Instituciones de Educación Superior
IIA'S	Institute of Internal Auditors
INCIBE	Instituto Nacional de Ciberseguridad
INEN	Servicio Ecuatoriano de Normalización
INTOSAI	La Organización Internacional de Entidades Fiscalizadoras Superiores
ISACA	Information Systems Audit and Control Association
ISO	International Organization for Standardization
ISSAI	Normas Internacionales de las Entidades Fiscalizadoras Superiores
ITAF	Marco de Garantía de la Tecnología de la Información
ITIL	Information Technology Infrastructure Library

MAIIES	Método de Auditoría Informática para Instituciones de Educación Superior
NIST	National Institute of Standards and Technology
NSWG	New South Wales Government
NTE	Norma Técnica Ecuatoriana
PCAOB	Public Company Accounting Oversight Board
SENESCYT	Secretaría de Educación Superior, Ciencia, Tecnología e Innovación
SGSI	Sistema de Gestión de Seguridad de la Información
SI	Sistemas de Información
SIEM	Administración de eventos e información de seguridad

1. CAPÍTULO I

1.1. Introducción

El estudio de la información como parte de una determinada disciplina se inicia e impulsa en el siglo XX; es la Ciencia de la Información (CI). Una de las disciplinas que convierte al fenómeno informacional en objeto de indagación y punto medular de sus proposiciones cognoscitivas (Marín & Torres, 2005). A lo largo de la historia el término se ha presentado de diversas maneras dependiendo del uso dado abordándolo desde diferentes disciplinas y puntos de vista. Se afirma que:

El término información, aunque se empleó desde la antigüedad por los griegos y los romanos, adquirió una mayor relevancia y proliferó en la Edad Moderna, donde el avance de la ciencia y la aparición de tecnologías como la imprenta confluyeron para que la información resurgiera, sobre todo, en el ámbito científico (Marín & Torres, 2005).

Actualmente, el término información tiene una gran variedad de definiciones que no permite llegar a un criterio universal del vocablo en cuestión; sin embargo, se coincide en que el término proviene del verbo en latín "informato", que significa "dar forma, construir una idea o una noción". Los griegos y romanos en la antigüedad le concedieron al concepto un carácter dinámico (Marín & Torres, 2005) en donde se pretende construir la información para que tenga significado.

En este contexto, si en una organización existen recursos de información utilizados inadecuadamente, vinculando sus procesos y/o dificultades en la aplicación de políticas relacionadas, se recurre a la auditoría para evaluar la eficiencia y eficacia del uso de esa información organizacional y conseguir la mejora de los procesos utilizados por los empleados, así como lograr que los directivos conozcan las debilidades de la empresa para orientar mejor la planificación y asignar recursos (González & Ponjuán, 2014).

Por otra parte, conociendo que la auditoría informática permite la salvaguarda de activos en los sistemas informáticos, como actividad de suma importancia en la integridad de la información, que contribuye a alcanzar los objetivos organizacionales de forma eficiente; entre los activos se considera el

hardware, software, datos, programas entre otros, con lo cual el horizonte de cobertura de esta área se amplía sustancialmente. Al considerar estos elementos con el objeto de emitir una opinión razonable sobre su realidad, se puede caer en contradicciones o ambigüedades desde un punto de vista subjetivo del auditor" (Mesquida & Mas, 2015b). Con base a lo anterior, surge la necesidad de evaluar sistemas informáticos, la información generada en los mismos y todos los componentes relacionados (Imbaquingo, Diaz, Saltos, et al., 2020).

Actualmente, en Ecuador y en los demás países latinoamericanos, no se dispone de un marco referencial que apoye el proceso de auditoría informática en las Instituciones de Educación Superior (IES). Tampoco se cuenta con una metodología que contemple el uso técnicas estratégicas especializadas, así como de procesos, que permitan minimizar los riesgos de calidad y seguridad en los resultados de las auditorías informáticas.

En las IES se han presentado propuestas de guías de auditoría para la evaluación de seguridad de información aplicando metodologías como: COBIT, ISO, ITIL entre otras, sin embargo; ninguna de ellas contempla los servicios y los procesos específicos que se desarrollan dentro de estas instituciones, con el objetivo de controlar y garantizar la seguridad de los activos tecnológicos, frente a las diferentes amenazas e incidentes, así como determinar las oportunidades de mejora.

Por otra parte, los marcos de referencia y manuales de buenas prácticas se enfocan principalmente al ámbito empresarial, más que al ámbito de las organizaciones con fines sociales y educativos. De acuerdo con la bibliografía revisada, se ha detectado la necesidad de realizar auditorías informáticas periódicas. Cabe destacar que según (Cadena et al., 2019), solamente el 12% de universidades ecuatorianas realizan auditorías específicas y periódicas.

Dado lo anterior, con la presente investigación se pretende proponer el diseño de un método de auditoría informática, basado en la estandarización de procesos, que permita minimizar el riesgo de la calidad y seguridad de la información obtenida de IES del Ecuador; a fin de desarrollar un valor agregado que permita la evaluación o acreditación institucional reglamentaria en el país.

1.2. Aspectos generales de la Auditoría informática

La auditoría informática para (Imbaquingo, Diaz, Ron, et al., 2020) es un procedimiento técnico que se utiliza para verificar y corregir el desempeño, seguridad, efectividad y correcta divulgación de los resultados de todo el ambiente tecnológico e informático (hardware, software, comunicaciones, base de datos, etc.) de una organización.

Para desarrollar una auditoría informática es necesario cumplir con requisitos, tales como: hacer uso de una metodología predeterminada, disponer de una fecha de ejecución fija y contar con un auditor externo al servicio informático que lleve a cabo el proceso (Guindel, 2010).

Basado en lo anterior, el marco teórico es valioso para el diseño de un método de auditoría informática, basado en la estandarización de procesos, a los efectos que se pueda cumplir con el objetivo de obtener una auditoría de calidad.

Adicionalmente, es importante mencionar que la construcción de la información en estos últimos tiempos utiliza técnicas avanzadas para el tratamiento de los datos, como la Inteligencia de Negocios (Bussiness Intelligence BI), Inteligencia Artificial y Gestión de Grandes Volúmenes de datos (Big Data), tendencias tecnológicas actuales que permiten la extracción de información mediante la integración sinérgica de datos de diversas fuentes (Imbaquingo et al., 2016). La Inteligencia Artificial (IA) tiene aplicación en muchos aspectos a través de técnicas especiales como los sistemas basados en conocimiento y los sistemas basados en reglas, en los que se incorpora el conocimiento de los expertos que pueden ser auditores informáticos quienes determinan el procedimiento a seguir con sus reglas, para encontrar y evaluar las evidencias relacionadas con los objetivos de la auditoría de una manera más objetiva, mitigando los riesgos inherentes a la percepción del auditor (Imbaquingo et al., 2016).

Con base en el estudio de lo recopilado en el marco teórico, se consolida la fuente para el informe final del estado del arte de la problemática elegida. Como proceso de consolidación y desarrollo del método de auditoría informática orientado a la calidad y seguridad de la información de las IES planteado, se lleva a cabo la revisión bibliográfica aplicada, incluyendo artículos de

publicaciones especializadas, trabajos presentados en congresos e investigaciones llevadas a cabo por organismos internacionales; además, de sitios web de autores, organizaciones e institutos de investigación vinculados con la temática. En consecuencia, con base en el estudio de lo recopilado en el marco teórico, se consolida la fuente para el informe final del estado del arte de la problemática elegida.

1.3. Objetivos

1.3.1 Objetivo general

La presente tesis doctoral tiene como objetivo diseñar un método de auditoría informática, basado en la estandarización de procesos, que permita minimizar el riesgo de la calidad y seguridad de la información obtenida de IES. Este soporte debe ser adecuado y fácil de implementar para cualquier institución educativa que posea un departamento tecnológico con al menos un recurso informático que contenga información y procesos auditables. Para cumplir con el objetivo general, se ha trabajado con siete objetivos específicos que se detallan a continuación.

1.3.2 Objetivos específicos

Basado en la sección 1.2 es posible afirmar que las auditorías informáticas que se vienen aplicando en IES en la Zona 1 del Ecuador, no han contribuido a solucionar la problemática de la alta dirección de éstas. Los sistemas de control interno de las universidades no son eficientes y eficaces porque sus mecanismos no han sido incorporados en la administración de estas instituciones y por ende no forman parte de la esencia de estas, lo que afecta en la ineficacia de la administración de las universidades y en los servicios que la comunidad universitaria ofrece

La falta de definición del entorno de control, la inadecuada definición de riesgos tecnológicos, la falta de información y de una adecuada supervisión del control interno exige el contar con un nuevo modelo que pueda influir en una óptima administración de las IES.

Considerando que en las IES se desarrolla gestión de sistemas de información, tanto en la parte estratégica como operativa, los módulos o

sistemas cumplen un rol protagónico como ejes principales de la gestión convirtiéndose de esta forma en un requerimiento esencial para cualquier organización, en especial en las IES cuyo proceso crítico está relacionado con la gestión académica al servicio de los estudiantes.

Al no existir un método moderno de auditoría cada profesional impone su criterio personal generando problemas de calidad y seguridad de la información, y peor aun cuando se deben considerar técnicas avanzadas de datos para minimizar el riesgo inherente de la auditoría, que tiene que ver con la subjetividad de la apreciación de la realidad por parte de los auditores, claro que esta subjetividad ha sido abordada con otros elementos como los estándares o conformando equipos de trabajo, pero se debe dejar paso al análisis objetivo de los datos y el uso algunas técnicas avanzadas de datos para recopilar información y de esta forma asegurar los resultados, para el cumplimiento de este trabajo se integran objetivos específicos que se pueden expresar en un conjunto de preguntas de investigación:

- Describir la calidad de los resultados que obtienen los auditores en las instituciones de educación superior de la Zona 1 de Ecuador, durante los procesos de auditoría informática. ***¿Qué es calidad en auditorías? ¿Cuáles son los factores que impactan en la calidad de los resultados de auditoría? ¿Cuáles son las métricas para evaluar calidad de auditorías informáticas?***
- Determinar el nivel de seguridad con el que cuenta la información obtenida por los auditores en las instituciones de educación superior de la Zona 1 de Ecuador, durante los procesos de auditoría. ***¿Cuáles son los estándares internacionales de la seguridad de la información? ¿Cuáles son las métricas para evaluar la seguridad en las IES?***
- Diagnosticar el grado de estandarización del procedimiento de auditoría que llevan a cabo los auditores en las instituciones de educación superior, para obtener la información. ***¿Cuáles son los marcos referenciales y metodologías más reconocidos en auditoría informática? ¿Cuáles son las fases en un proceso de auditoría informática? ¿Cuáles son las actividades para desarrollar un proceso de auditoría informática?***

- Analizar las alternativas de auditoría informática existentes, en términos de los criterios de estandarización de la auditoría. ***¿Qué metodología cumple con la mayor cantidad de actividades para un proceso de auditoría informática?***
- Comparar las alternativas de auditoría informática existentes, en términos de los criterios de estandarización de la auditoría.
- Explicar cómo el proceso de estandarización de la auditoría afecta la calidad y la seguridad de los resultados obtenidos por los auditores en las instituciones de educación superior.
- Proponer un método de auditoría informática basado en sistemas de procesamiento avanzado de datos que permita minimizar el riesgo de calidad y de seguridad de los resultados.

1.4. Preguntas de investigación

Para el desarrollo de la investigación se han establecido una serie de preguntas, indicada en la Tabla 1.1, que permiten identificar los requerimientos y parámetros necesarios en el desarrollo del método de auditoría informática. Entre los principales temas a investigar se consideran la calidad del proceso de auditoría, la seguridad de la información, los estándares, marcos referenciales y metodologías más reconocidos en auditoría informática con sus fases y actividades que se adapten a las IES.

Tabla 1.1 Preguntas de investigación

N°	Preguntas de investigación
PI1	¿Qué es calidad en auditoría?
PI2	¿Cuáles son los factores que impactan en la calidad de auditoría?
PI3	¿Cuáles son las métricas para evaluar calidad de auditorías informáticas?
PI4	¿Cuáles son los estándares internacionales de la seguridad de la información?
PI5	¿Cuáles son las métricas para evaluar la seguridad en las IES?
PI6	¿Cuáles son los marcos referenciales y metodologías más reconocidos en auditoría informática?
PI7	¿Cuáles son las fases en un proceso de auditoría informática?

PI8	¿Cuáles son las actividades para desarrollar un proceso de auditoría informática?
PI9	¿Qué metodología cumple con la mayor cantidad de actividades para un proceso de auditoría informática?

1.5. Alcance

El presente trabajo tiene como alcance la definición de un método de auditoría informática, basado en sistemas de procesamiento avanzado de datos, que permita minimizar el riesgo de calidad de los resultados, utilizando una estandarización del proceso construido e implantado por parte de auditores informáticos. Basado en la preocupación de que a través de estos sistemas fluye la información crítica institucional, que sirve para dirigir y operarlo, constituyéndose de esta manera en una infraestructura crítica, que debe ser evaluada en función de los riesgos que su operación conlleva.

1.6. Estructura del trabajo

Este trabajo consta de cinco capítulos, sobre los que se presentan los aspectos generales:

El Capítulo 1 presenta el contexto según el cual se establece el objetivo general y los objetivos específicos, así como el alcance. Adicionalmente, se presenta la estructura del trabajo y las contribuciones derivadas de la investigación.

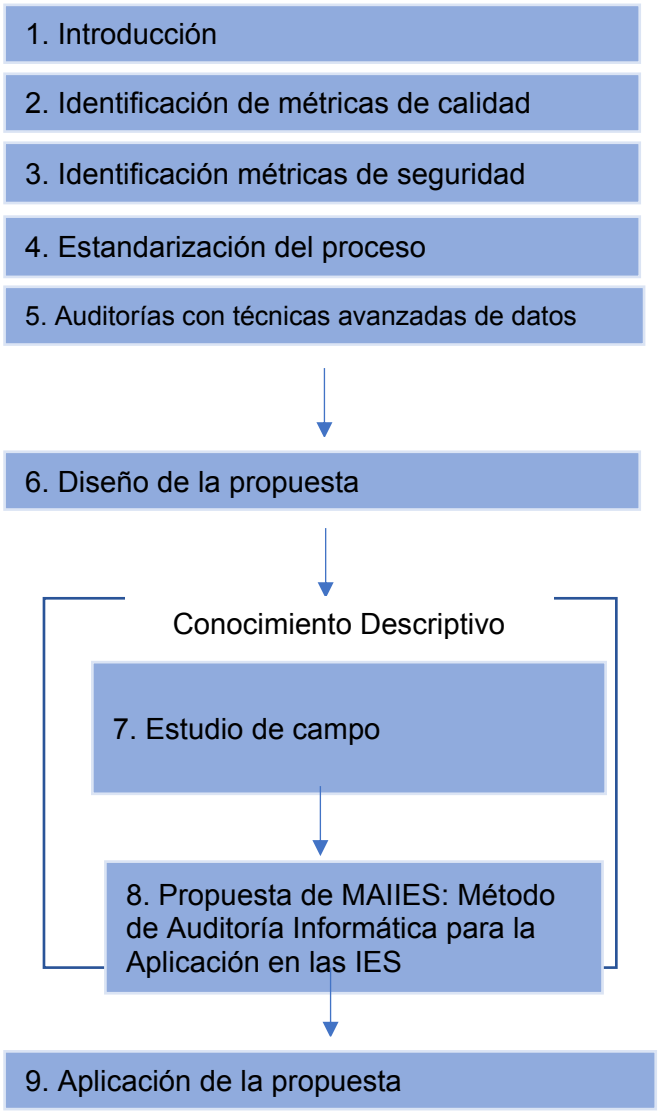
En el Capítulo 2 se describen los conceptos asociados a la auditoría informática en IES de Ecuador, el proceso y los niveles de seguridad y calidad de la información generada durante este proceso de importancia para entidades académicas, tomando en cuenta que en el Ecuador.

En el Capítulo 3 se expone el desarrollo de la solución, basada en las cuatro (4) etapas que permitirán establecer el punto de partida para desarrollar un método de auditoría informática utilizando técnicas avanzadas de datos, pudiendo aplicarse en cualquier Institución de Educación Superior.

En el Capítulo se reportan los hallazgos en cuanto a la valoración sobre la investigación y finalmente se definen futuras líneas de investigación.

En el Capítulo 5. Se presenta la lista de referencias utilizadas en el este trabajo.

En la figura 1.1 se presenta un esquema de la estructura propuesta para la investigación.



1.7. Contribuciones originales

Durante el desarrollo de esta tesis se han comunicado resultados parciales a través de distintas publicaciones que a continuación se detallan:

Publicaciones

Imbaquingo, D. (2019). *Evaluation of university informatic security systems: Teacher evaluation system a case study* - Revista Ibérica de Sistemas e Tecnologías de Información, N(E22), 349-362, ISSN: 1646-9895

Imbaquingo, D., Díaz J. et all (2020). Information security issues in educational institutions- *Revista IEEE Xplore, 2020 15th Iberian Conference on Information Systems and Technologies (CISTI), 2020, pp. 1-7, doi: 10.23919/CISTI49556.2020.9141014*.

Imbaquingo, D., Díaz J. et all (2020). "Evaluation model of computer audit methodologies based on inherent risk," *Revista IEEE Xplore,2020 15th Iberian Conference on Information Systems and Technologies (CISTI)*, 2020, pp. 1-7, doi: 10.23919/CISTI49556.2020.9140877.

Imbaquingo, D., Díaz J. (2020). “Análisis de las principales dificultades de la auditoría informática, una revisión sistemática de literatura”- Revista Ibérica de Sistemas e Tecnologías de Información, N(E32), 427-440, ISSN: 1646-9895.

Imbaquingo, D., Díaz J. (2021). “Let's talk about Computer Audit Quality: A systematic literature review”, International Conference on Maintenance and Intelligent Asset Management (ICMIAM), doi: 10.1109/ICMIAM54662.2021.9715192.

Imbaquingo, D., Díaz J. (2022). “Computer Auditing Quality Assessment Based on Human, Technical and Contextual Factors”, International Conference on Advanced Research in Technologies, Information, Innovation and Sustainability (ARTIIS), doi: 10.1007/978-3-031-20316-9_25.

Imbaquingo, D., Díaz J. (2022). “Information Security at Higher Education Institutions: A Systematic Literature Review” Information and Communication Technologies, TICEC 2022, doi: 10.1007/978-3-031-18272-3_20

Congresos Internacionales

Imbaquingo, D. (CISTI 2020). Análisis de las principales dificultades de la auditoría informática, una revisión sistemática de literatura. 15ª Conferencia Ibérica de Sistemas y Tecnologías de Información. - Sevilla, España: Universidad de Sevilla.

Imbaquingo, D. (CISTI 2020). Information security issues in educational institutions- 15ª Conferencia Ibérica de Sistemas y Tecnologías de Información. - Sevilla, España: Universidad de Sevilla.

Imbaquingo, D. (CISTI 2020). “Evaluation model of computer audit methodologies based on inherent risk” - 15ª Conferencia Ibérica de Sistemas y Tecnologías de Información. - Sevilla, España: Universidad de Sevilla.

Imbaquingo, D. (ICMIAM 2021). “Let's talk about Computer Audit Quality: A systematic literature review” - 2021 International Conference on Maintenance and Intelligent Asset Management – Ballarat, Australia: Universidad de la Federación Ballarat Victoria.

Imbaquingo, D. (ARTIIS 2022). “Computer Auditing Quality Assessment Based on Human, Technical and Contextual Factors” - 2022 International Conference on Advanced Research in Technologies, Information, Innovation and Sustainability – Madrid, España.

Imbaquingo, D., Díaz J. (2022). “Information Security at Higher Education Institutions: A Systematic Literature Review” Information and Communication Technologies, TICEC 2022, 10th Ecuadorian Conference, TICEC 2022, Manta, Ecuador, October.

2. CAPÍTULO II

2.1. Estado del arte

Según (Tapia et al., 2016) la auditoría radica en revisar que los hechos, fenómenos y operaciones se ejecuten en la forma en que fueron planteados; además que las políticas y procedimientos establecidos se observen y representen. En este orden de ideas, (Lorenzo, 2019) agrega que en una auditoría se deben involucrar tres partes: el cliente, el auditor y el auditado. Del papel que juegan cada una de ellas y de cómo se interrelacionan va a depender el progreso y las consecuencias de la auditoría. Una idea similar se puede encontrar en (Blanco, 2008) quien afirma que la auditoría es el conjunto de procedimientos, metodologías y métodos organizados lógicamente para la obtención y valoración de información que permita el control y cumplimiento de los objetivos establecidos en el desarrollo de todo tipo de actividades.

Existen criterios generalizados para clasificar la auditoría, atendiendo a diferentes objetivos, sujetos, alcance, entre otros; no obstante, las contralorías o tribunales de cuenta de cada país establecen en la ley de auditoría los criterios que serán de aplicación. En el caso de la República de Ecuador, por ley de la Contraloría, la auditoría se clasifica atendiendo a: quién la ejerce en auditoría externa o auditoría interna, y por su naturaleza en administrativa u operacional, financiera y exámenes especiales (Murgueytio, 2017). Dentro de la realización de la auditoría informática (Campos et al., 2019) señala tres principales fases o etapas: Planificación, ejecución e informe.

El surgimiento de la auditoría en informática es reciente, asimismo, se tiene como antecedente cercano a los Estados Unidos de América. En los años cuarenta se empezaron a dar resultados relevantes en el campo de la computación, con sistemas de apoyo para estrategias militares; sin embargo, la seguridad y el control solo se limitaba a dar custodia física a los equipos y a permitir el uso de estos solo a personal altamente calificado.

La importancia de las auditorías informáticas radica en la facultad de determinar las fortalezas y debilidades en la gestión de proyectos, el nivel de funcionalidad de los sistemas de información automatizados, la adecuación de

la configuración de la plataforma informática, el nivel de calidad de los servicios prestados por la unidad encargada y la situación de los contratos con proveedores de productos y servicios, entre otros aspectos (Arcentales & Caycedo, 2017).

Evolución de la auditoría

La auditoría surge por la necesidad de un sistema de control, que en sus inicios tenía como procedencia dar veracidad a las personas, evitar fraudes, manejar correctamente cuentas y garantizar resultados de actividades económicas y comerciales (San Pedro, 2022). En la Tabla 2.1 se indican los acontecimientos más notables en el trascurso del tiempo, lo que permitirá entender la evolución de la auditoría.

A principios de los años 80, se empiezan a aplicar técnicas de tratamiento de la información por medio de ordenadores, como apoyo a la labor de los auditores. El auditor de sistemas de información empieza a ser también experto en el uso de lenguajes informáticos que le sirven para escribir, compilar y ejecutar programas para la consecución de pruebas y obtención de evidencia. Surge de este modo la denominada auditoría con el ordenador. En la misma década se empiezan a aplicar los principios básicos de la auditoría operativa a la auditoría de los sistemas de información, dando lugar a la auditoría operativa de proceso de datos, que se centra en la eficacia y eficiencia del tratamiento automático de los datos (M. Álvarez, 2008).

Con el paso de los años la informática y todos los elementos tecnológicos que la rodean han ido creando necesidades, en cada sector social y se han vuelto un requerimiento permanente para el logro de soluciones. Además, del conocimiento y la información se han convertido en el elemento esencial dentro de una institución, debido a que son el insumo para favorecer el aprendizaje colectivo, mantener la innovación y su desarrollo (Almuiñas & Galarza, 2015). Por ello es necesario proteger dicho recurso, de forma física y en los medios donde se genera, almacena, procesa, transmite, circula y transforman todos los datos (Valencia Duque & Orozco Alzate, 2017).

Tabla 2.1 Evolución de la auditoría

Año	Acontecimientos
1760 - 1840	Revolución Industrial: crece el comercio y la industria nace la contabilidad industrial y con ello un nuevo sistema de control.
1851	Asociación de auditores en Venecia: se crea la primera asociación.
1862	Profesión de auditoría: se reconoce a la auditoría como profesión independiente.
1879	Obligatoriedad en Bancos: se dispuso como obligatorio para los bancos realizar auditorías independientes.
1896	Contadores Públicos Certificados: Se designa para esta área a personas que cumplen con las regulaciones para ser auditor.
1921	Auditoría gubernamental: nace esta área de la auditoría y se crea Oficina General de contabilidad en Estados Unidos
1960	Auditoría informática: se origina está área estratégica en Estados Unidos.
1968	Requisitos técnicos para la auditoría de tecnologías de la información: En el Instituto de Contadores Públicos se publica los requisitos para cumplimiento obligatorio.
1969	Asociación Internacional de Auditoría y Control de Sistemas de Información (ISACA): Nace la primera organización de auditorías de tecnologías de la información
1970	Investigación: en esta década se inician investigaciones sobre temas relacionados a auditorías de información.
1984	Marco legal: en la Unión Europea se realiza el marco legal de la profesión de la auditoría
Actualidad	Está alcanzando diferentes áreas como la operativa y de calidad.

El entorno competitivo obliga a las organizaciones a gestionar su información, lo que se evidencia en el incremento de Sistemas de Información (SI) que se encargan de automatizar los procesos, proporcionar información de apoyo a la toma de decisiones y así lograr ventajas competitivas (Hamidian & Ospino, 2015); no obstante, en el proceso de automatización se desconoce el

nivel de seguridad con el que se cuenta, por tanto, es una prioridad buscar mecanismos de protección para cualquier organización (Soriano, 2014).

En este contexto las IES incorporan paulatinamente tecnologías de la información y la comunicación en donde se gestionan datos críticos que requieren de procesos para evitar correr riesgos en su seguridad, aunque son pocas las instituciones que le dan la importancia adecuada, de acuerdo con un informe emitido por la Red Nacional de Investigación y Educación del Ecuador el 17% de las universidades aún no tiene una política de seguridad debidamente formalizada y aprobada. El 69% tiene un responsable de seguridad de la información y más de la mitad realizan auditorías específicas de seguridad de la información. El 55% cuenta con el servicio de respuesta a incidentes de seguridad (CSIRT) y un 10% por uno propio (Cadena et al., 2018).

Con el desarrollo de la tecnología se llega a la automatización de procesos por medio de sistemas informáticos, proporcionando velocidad y precisión en el tratamiento de la información; pero, así como ha generado beneficios ha creado también riesgos inherentes a su empleo e incertidumbre sobre su uso eficaz y eficiente. En este sentido (Acosta, 2015), afirma que, el avance de los medios tecnológicos y de comunicación aumenta la necesidad de proteger la información generada en una organización, debido a que el número de incidentes con la pérdida de los datos se incrementa año con año, que obedece a los siguientes factores: fallas humanas, tecnológicas o presencia de vulnerabilidades.

De esta manera, se puede concluir que la auditoría surge desde la necesidad de evaluar sistemas informáticos, la información generada en los mismos y todos los componentes relacionados (Imbaquingo, Diaz, Ron, et al., 2020). Para poder desarrollar una auditoría informática es necesario cumplir con ciertos requisitos, tales como: hacer uso de una metodología predeterminada, tener una fecha de ejecución fija y debe ser realizada por un auditor externo al servicio informático (Guindel, 2010). Por esta razón es necesario aplicar evaluaciones constantes en las áreas de TI, para mejorar la seguridad de los productos y procesos que tienen como activo la información. Sin duda, la auditoría obtiene un rol importante para gestionar el manejo de la información, los servicios utilizados y personal involucrado. La importancia de sus resultados

radica en el análisis y diagnóstico para una gestión adecuada de este importante recurso (Altamirano, 2019; Soy i Aumatell, 2003).

2.2. Contexto actual de la auditoría informática

Actualmente la auditoría informática se lleva a cabo por profesionales especialmente capacitados para el efecto, y que consiste en recoger, agrupar y evaluar evidencias para determinar si un sistema de información salvaguarda el activo empresarial, mantiene la integridad de los datos, lleva a cabo eficazmente los fines de la organización, utiliza eficientemente los recursos, y cumple con las leyes y regulaciones establecidas.

Tomando en cuenta que “Investigadores del área de auditoría afirman que es necesaria más investigación académica para comprender plenamente los efectos de alejarse de los procesos de auditoría tradicional, para aprovechar plenamente los beneficios de grandes volúmenes de datos y cómo el uso de análisis de datos más avanzados tendrá un impacto en el juicio del auditor (Brown et al., 2015). Por tanto, es importante tomar en cuenta las principales dificultades que los auditores informáticos tienen que afrontar en la actualidad. “*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”* (Imbaquingo, Diaz, Saltos, et al., 2020).

Así mismo, se requiere identificar que: “Uno de los problemas actuales que atraviesa la auditoría informática es que los auditores aún no se han adaptado al uso de técnicas modernas para evaluar tecnologías, como el uso de Big Data, Business Intelligence, Correlacionadores de eventos (SIEM), sistemas de AI y otros” (Gepp et al., 2018). Por lo anterior, se hace necesario una auditoría de información que funcione como una herramienta clave para la evaluación de los recursos informáticos o de información, debido a su impacto en la prevención o detección de violaciones que afecten la confidencialidad, integridad, disponibilidad y trazabilidad de los recursos de una organización.

2.3. Calidad en auditorías

El término calidad resulta muy ambiguo. La RAE define la calidad como la "propiedad o conjunto de propiedades inherentes a algo, que permiten juzgar su valor" y a lo referente a control es la "adecuación de un producto o servicio a las características especificadas" (Real Academia Española, 2021).

La calidad de auditoría es difícil de definir y hasta la fecha no existe un concepto reconocido de manera universal, pero está relacionada por estándares aplicables al auditar, la definición más cercano es la medición del éxito de la realización del proceso (Havelka & Merhout, 2013). En la tabla 2.2 se presentan las contribuciones de varios autores con respecto al concepto de calidad en auditorías.

Tabla 2.2 Calidad de auditoría

Artículo	Contribución
Guidelines on Audit Quality (Committee Contact of Heads of EU SAIs, 2004)	La calidad de la auditoría parte del proceso para identificar y gestionar las actividades que darán cumplimento a los objetivos e indicadores de calidad establecidos por las entidades de regulación y control, quiénes aseguran que los problemas en la calidad de las auditorías están directamente relacionados con la forma en que se diseñó el proceso.
What do we know about audit quality? (Francis, 2004)	El autor plantea la definición de calidad con base en todos los fallos de la auditoría, esto significa que cuanto mayor sea la tasa de fallas, menor será la calidad de la auditoría.
Regulating audit quality: Restoring trust and legitimacy (Holm & Zaman, 2012)	La calidad de las auditorías está definida en base a los resultados obtenidos, y se enfatiza que, a pesar de varios intentos de mejorar la calidad sigue siendo un tema digno de atención e investigación.
Audit Committee and Internal Audit: implications on	La calidad de la auditoría es un componente clave para justificar la demanda del servicio de auditoría y que garantiza la credibilidad de las entidades y sus procesos.

audit quality (Yasin & Nelson, 2012)	
Audit Quality Attributes and Audit Client Satisfaction (Yuniarti & Zumara, 2013)	La calidad de una auditoría se basa en el conjunto de atributos inherentes que cumple con los objetivos y requisitos establecidos en el plan de auditoría y con las expectativas del cliente.
Audit quality: Insights from the academic literature (Knechel et al., 2013)	La calidad en auditorías proviene de auditores calificados y motivados para diseñar correctamente el proceso, para adaptarse al cliente y gestionar los riesgos inherentes a la auditoría. Además, la percepción de calidad depende del punto de vista del personal involucrado en el proceso.
A framework for audit quality (International Auditing and Assurance Standards Board, 2014)	La idea de calidad difiere entre los involucrados de la auditoría y se debe acomodar a las necesidades de cada organización, persona, área o proceso. En el marco propuesto por la Junta de Normas Internacionales de Auditoría y Aseguramiento se menciona que la calidad es el cumplimiento de estándares, controles y la ética empleada durante el proceso.
The effect of auditor features on audit quality (Zahmatkesh & Rezazadeh, 2017)	La calidad de la auditoría es el resultado del trabajo del auditor representado en un informe de auditoría confiable basado en estándares establecidos.
Selecting an auditor for Bradco using indicators of audit quality	La calidad de la auditoría está definida por la capacidad que tiene el auditor al momento de detectar e informar los errores, también con el cumplimiento reglamentario y la satisfacción que se obtiene del cliente.

(Dickins et al., 2018)	Lo que más destaca es que la necesidad de auditorías de alta calidad es universalmente reconocida y la categoriza en dos factores principales: en el lado de la oferta se toma en cuenta la perspectiva y habilidades del auditor, mientras que el lado de la demanda se enfoca en las características del cliente.
People and Audit Process Attributes of Audit Quality: Evidence from China (Ye et al., 2014)	La calidad de la auditoría no es inmediata, ni directa y difícil de calcular. Se la relaciona directamente con la capacidad del auditor para identificar y reportar los hallazgos resultantes del proceso.
How audit effort affects audit quality: An audit process and audit output perspective (Xiao et al., 2020)	La calidad de la auditoría es el proceso que detecta, ajusta y presenta los errores materiales, al mismo tiempo relaciona el término “calidad” con la disponibilidad de información y el esfuerzo que se aplique en la auditoría debido a que es necesario el trabajo duro para tener éxito.

Como resultado de la revisión de esta terminología se han logrado identificar seis aspectos clave para lograr una definición de calidad de una auditoría, indicados a continuación:

1. Conocer el diseño del proceso
2. Satisfacer al cliente en sus necesidades.
3. Cumplir con los objetivos, requisitos e indicadores de calidad que se ajusten a la entidad auditada.
4. Comprender y gestionar el riesgo inherente de una auditoría.
5. Realizar informes de auditoría de calidad.
6. Minimizar fallas o errores en el proceso.

En base a lo anterior y a la revisión de literatura es posible concluir que: “La calidad de auditoría informática como el proceso de revisión y validación de los resultados obtenidos en el ejercicio de control, el cual se aplica para analizar si los productos de la auditoría cuentan con los criterios de pertinencia,

oportunidad y suficiencia, agregan valor al negocio o proveen información objetiva, verificada e independiente para la toma de decisiones en las áreas, procesos y actividades relacionadas con el objeto auditado".

2.4. Factores que impactan en la calidad de auditoría

Tomando en cuenta que cada proceso de auditoría es único, es importante que se identifique, defina y determine los factores que pueden afectar al éxito de una auditoría, que pueden variar según las circunstancias del proyecto, es decir, la industria, el tamaño de la organización auditada, la complejidad de los sistemas involucrados, entre otros (Havelka & Merhout, 2007).

La calidad de las auditorías sobre todo en el área informática gira alrededor de varios elementos clave que al integrarse permiten aumentar la probabilidad de que la auditoría sea de calidad. La revisión de la bibliografía permitió identificar tres categorías que se ajustan a cada una de las condiciones de la auditoría de calidad que se han agrupado en los siguientes factores: humano, técnico y contextual, tal y como se muestra en la tabla 2.3:

Tabla 2.3 Factores de calidad

Factor	Ejemplos del factor	Fuente
Humano	Auditor. Profesionales de auditoría. Gestión del personal. Interacciones clave. Gestión de relaciones. Cliente.	(Guindel, 2010; Harris & Williams, 2020; Havelka & Merhout, 2007, 2013; International Auditing and Assurance Standards Board, 2014; Public Company Accounting Oversight Board, 2015; Refaat & El-Henawy, 2019; Sulaiman et al., 2018, 2019; Ye et al., 2014; Yuniarti & Zumara, 2013; Zahmatkesh & Rezazadeh, 2017)

Técnico	Proceso de auditoría. Organización de la auditoría. Metodología. Toma de decisiones. Estrategia y planeación. Control de calidad y mejora. Trabajo de campo. Resultados e informes.	(Committee Contact of Heads of EU SAIs, 2004; González & Ponjuán, 2014; Guindel, 2010; Harris & Williams, 2020; Havelka & Merhout, 2007, 2013; Imbaquingo Esparza et al., 2020; International Auditing and Assurance Standards Board, 2014; Knechel et al., 2013; Public Company Accounting Oversight Board, 2015; Refaat & El-Henawy, 2019; Sulaiman et al., 2018, 2019; Yuniarti & Zumara, 2013)
Contextual	Entorno regulatorio y empresarial. Cultura organizacional. Percepciones. Recursos.	(Guindel, 2010; Havelka & Merhout, 2013; Holm & Zaman, 2012; International Auditing and Assurance Standards Board, 2014; Public Company Accounting Oversight Board, 2015; Sulaiman et al., 2018)

2.4.1 Factor Humano

El factor humano es la categoría que integra al equipo auditor, el cliente y todos los involucrados en el proceso. Por lo que se considera de vital importancia la percepción de la calidad de la auditoría de todos los participantes ya que cada uno de ellos puede tener puntos de vista diferentes sobre la evaluación de los indicadores (San Pedro, 2022).

El equipo de auditoría es identificado como responsable directo de la realización de una auditoría (Committee Contact of Heads of EU SAIs, 2004) y el resultado de su trabajo se verá reflejado exitosamente en un informe de auditoría confiable basado en los estándares determinados (Zahmatkesh & Rezazadeh, 2017).

Al hablar de calidad en auditorías es relevante tomar en cuenta la experiencia que tiene el auditor, (Strous, 2002) da a conocer como el hecho de trabajar en equipo apoya al crecimiento profesional del auditor siendo este uno de los temas más relevantes al hablar de calidad en auditorías. Además, indica que para cubrir los requisitos de una auditoría y para que su proceso sea menos complejo. es necesaria la cooperación de varias disciplinas que cubran toda el área a auditar, también enfatiza que esa necesidad viene dada para que todos los involucrados (auditor, desarrolladores, ingenieros, etc.) comprendan lo que se va a efectuar y de este modo su participación sea favorable (San Pedro, 2022).

(Imbaquingo, Díaz, et al., 2020) afirman que los auditores, deberían poseer cualidades que garanticen que se realice una auditoría de calidad, entre ellas están tener los conocimientos necesarios para auditar, tener firmeza con los resultados obtenidos para tomar decisiones ante cualquier situación, ser discreto además de tener una buena comunicación con el auditado siendo honesto sincero y parcial con los resultados.

(Knechel et al., 2013) y (Harris & Williams, 2020) afirman que la experiencia de un auditor, las habilidades y conocimientos especializados del personal de auditoría en la industria están relacionados positivamente con la calidad de las auditorías, entre dichas habilidades destacan: destrezas de comunicación y colaboración, conocimiento de dominio y proceso, desarrollo profesional, rasgos de personalidad, conocimientos técnicos y de auditoría, etc. (Guindel, 2010; Havelka & Merhout, 2013; International Auditing and Assurance Standards Board, 2014; Yuniarti & Zumara, 2013).

Dado que los auditores experimentados pueden seguir mejor las normas y detectar errores se encontró que están asociados con una menor probabilidad de falla en la auditoría (Ye et al., 2014). Todas estas cualidades juntas conducen a una planificación y programas de auditoría adecuados que producen resultados confiables que pueden afectar directamente la satisfacción del cliente, que es un factor crucial a la hora de evaluar la calidad (Yuniarti & Zumara, 2013).

Entonces se puede observar que cada elemento que forma parte del proceso de auditoría juega un papel de vital importancia para generar, almacenar y

respaldar resultados de alta calidad, por consecuencia se entiende que este factor es un impacto positivo al evaluar la calidad de la auditoría.

2.4.2 Factor Técnico

El factor técnico está relacionado estrechamente con el desempeño del auditor durante el proceso de la auditoría en la planificación, la selección de las metodologías, visitas in situ, evidencias, control de calidad del proceso y en los resultados que vendrían a ser los informes finales de todo el proceso de auditoría (Imbaquingo et al., 2021).

La calidad de la auditoría depende en gran magnitud de los juicios y resultados que emite el auditor durante todas las etapas de la auditoría cumpliendo con las leyes, regulaciones y estándares aplicables (International Auditing and Assurance Standards Board, 2014), por lo tanto, después de analizar los problemas de calidad de la auditoría relacionados con el profesional se procede con los aspectos específicos del proceso de auditoría y los procedimientos de control de calidad (Knechel et al., 2013) en donde se identifican y gestionan las actividades necesarias para lograr los objetivos, la mayoría de los problemas relacionados con la calidad de las auditorías son principalmente el resultado de una mala gestión del proceso de auditoría (Committee Contact of Heads of EU SAIs, 2004).

Para que el proceso de auditoría se desarrolle de manera satisfactoria debe pasar por una adecuada organización en donde se toman en cuenta ciertas características como: el tamaño y funcionamiento de la empresa a auditar, el uso de tecnologías, la disponibilidad de recursos, la competencia y selección del equipo auditor (Havelka & Merhout, 2013; International Auditing and Assurance Standards Board, 2014).

Dentro del proceso de auditoría se incluyen la selección de herramientas, técnicas, metodologías y métodos específicos que el equipo auditor va a seguir, algunos de los identificadores de esta sección son: el uso de buenas prácticas para la gestión de proyectos, la revisión del trabajo de campo, la planificación, el alcance del proyecto, el impacto de la auditoría, las prácticas y procedimientos de auditoría, etc. (Havelka & Merhout, 2007; International Auditing and Assurance Standards Board, 2014).

Una vez ejecutada la auditoría basada en la organización y siguiendo el diseño del plan de auditoría, se debe cumplir con el control de calidad que requiere una comprensión clara de dónde reside la responsabilidad de todos los involucrados y sus decisiones particulares. Los procesos de control de calidad deben llevarse a cabo de la manera prescrita y documentarse. Estos procesos pueden estar respaldados por cuestionarios y listas de verificación en formas prescritas (Committee Contact of Heads of EU SAIs, 2004).

2.4.3 Factor Contextual o del Entorno

El factor contextual en la calidad de la auditoría está directamente ligado a los dos factores anteriores que han sido analizados y que son parte del proceso de auditoría, el factor incluye la empresa auditada y la auditora, su marco regulatorio y el manejo de los recursos.

El entorno en el que se llevan a cabo los procesos de auditoría varía de un país a otro. A medida que un país se desarrolla y, en particular, a medida que las empresas crecen en tamaño y necesitan mayor seguridad en sus procesos internos, el entorno se vuelve más complejo. En respuesta, evolucionan las leyes, los requisitos de seguridad y los procesos de gobierno corporativo (International Auditing and Assurance Standards Board, 2014).

Algunas empresas han utilizado durante mucho tiempo algunos conceptos para gestionar sus prácticas de auditoría, entre ellos se señala: comunicación y colaboración intra organizacional, estructura y cultura, actitudes hacia la autoridad, comportamiento colectivo y transparencia (Havelka & Merhout, 2013; International Auditing and Assurance Standards Board, 2014). Por el lado de la normativa se tiene: el estado legal de las leyes, la inspección de la auditoría, la investigación cuando falla el proceso, la adopción de medidas disciplinarias, estas características son más efectivas si se cumplen adecuadamente (International Auditing and Assurance Standards Board, 2014). Así mismo se debe considerar como se gestiona y optimiza los recursos de la empresa en apoyo al cumplimiento de estrategias y para intentar disminuir costos tanto para el auditado como para la empresa auditada (Cajas & Luje, 2019; Guindel, 2010).

El compromiso de las partes es un factor vital que afecta la calidad y éxito de una auditoría porque tienen efectos interactivos significativos con las entradas y el proceso de auditoría. Sin embargo, debido a la falta de disponibilidad de grandes conjuntos de datos sobre el esfuerzo de auditoría, la evidencia de la relación entre el esfuerzo de auditoría y la calidad de la auditoría es escasa (Xiao et al., 2020)

En resumen, para que una auditoría sea de buena calidad se debe ejecutar un proceso bien diseñado por auditores capacitados y debidamente motivados, que comprenden los factores contextuales y se ajustan adecuadamente a cada una de las condiciones únicas de la auditoría. Los tres factores mencionados deben manejarse conjuntamente y también tenerse en cuenta al considerar y evaluar la calidad de la auditoría (Imbaquingo et al., 2021).

2.4.4 Métricas para evaluar calidad en auditorías informáticas

De acuerdo con el comunicado emitido por la (Public Company Accounting Oversight Board, 2015) los indicadores o métricas son considerados una herramienta que dependen del contexto o situación en la que surjan. No son algoritmos, ni puntos de referencia contra la ejecución u otras reclamaciones, no conducen directamente a fórmulas para determinar la calidad de una auditoría en particular y tampoco todos los factores que impulsan la calidad de las auditorías pueden medirse directamente con facilidad. Después de la revisión de literatura se encontró y agrupó las métricas de acuerdo con el factor determinado en el punto anterior, en la tabla 2.4 se detallan las métricas identificadas.

Tabla 2.4 Métricas de calidad

Métrica	Ítem	Fuente
Factor Humano		
Liderazgo	El líder del equipo auditor o auditor individual tiene características de liderazgo	(Holm & Zaman, 2012; Public Company Accounting Oversight Board, 2015)
	El representante de la organización auditada tiene características de liderazgo	

Experiencia	El personal que realiza la auditoría tiene suficiente experiencia como auditor	(Dickins et al., 2018; Harris & Williams, 2020; Havelka & Merhout, 2007; Holm & Zaman, 2012; International Auditing and Assurance Standards Board, 2014; Stoel et al., 2012; Yasin & Nelson, 2012; Ye et al., 2014; Zahmatkesh & Rezazadeh, 2017)
	El personal que realiza la auditoría tiene experiencia en el área informática	
Valores éticos	Los miembros del equipo auditor demuestran honestidad y respeto al realizar su trabajo	(Holm & Zaman, 2012; International Auditing and Assurance Standards Board, 2014; Zahmatkesh & Rezazadeh, 2017)
	Los miembros del equipo auditor trabajan en la auditoría con ética y transparencia	
Relaciones con el cliente	El equipo auditor mantiene una relación cordial con el auditado	(Havelka & Merhout, 2007; Holm & Zaman, 2012; Knechel et al., 2013; Stoel et al., 2012)
	El equipo auditor responde a las necesidades del cliente	
	El auditor sabe escuchar y es receptivo con el cliente	
	El auditor se comunica de manera respetuosa tanto de forma verbal como por escrito con el cliente	

	El equipo auditor procura que el cliente participe en todo el proceso de auditoría	
	El equipo auditor obtiene la conformidad del cliente acerca de las actividades desarrolladas	
	El equipo auditor y el cliente orientan esfuerzos hacia un mismo objetivo	
Competencias y habilidades (talento)	El personal que realiza la auditoría tiene las competencias necesarias para realizar su trabajo	(Havelka & Merhout, 2007; Holm & Zaman, 2012; Stoel et al., 2012; Sulaiman et al., 2019; Zahmatkesh & Rezazadeh, 2017)
	El personal que realiza la auditoría tiene habilidades para tratar situaciones sensibles	
	El personal que realiza la auditoría demuestra ser asertivo en respuesta a situaciones difíciles y resolución de problemas	
	El auditor posee habilidades blandas	
	El personal que realiza la auditoría brinda sugerencias efectivas a la Institución	
	El personal de auditoría tiene alta capacidad de observación	
Actitudes y cualidades personales	El auditor respeta la confidencialidad de la información del cliente	(Holm & Zaman, 2012; International Auditing and Assurance Standards Board, 2014)
	El auditor mantiene la mente abierta al recibir nuevas ideas	
	El auditor sabe tratar a las personas	

	El auditor está seguro de sí mismo y su trabajo	
Independencia	El equipo auditor mantiene su independencia en apariencia y acción	(Public Company Accounting Oversight Board, 2015; Stoel et al., 2012; Strous, 2002)
	El equipo auditor no se involucra en acciones que comprometan su independencia	
	El auditor reporta al responsable todos los eventos que pueden afectar su independencia	
Objetividad	El equipo auditor se centra en los hechos	(Public Company Accounting Oversight Board, 2015; Strous, 2002; Zahmatkesh & Rezazadeh, 2017)
	El equipo auditor muestra objetividad e integridad	
	El equipo auditor ejecuta la auditoría de manera imparcial y sin prejuicios	
Motivación	El auditor tiene oportunidades de mejora	(Zahmatkesh & Rezazadeh, 2017)
	El equipo auditor recibe apoyo para lograr las metas	
Esfuerzo	El equipo auditor se esfuerza al realizar la auditoría	(Xiao et al., 2020)
Educación	El auditor se preocupa por su formación y actualización continua	(Ye et al., 2014)
	El auditor cuenta con certificaciones nacionales e internacionales en el área de auditoría y auditoría informática	
Escepticismo profesional	El auditor demuestra escepticismo durante todo el trabajo de auditoría	(International Auditing and Assurance

		Standards Board, 2014; Sulaiman et al., 2019)
Conocimiento	El equipo auditor demuestra conocimientos necesarios para el proceso de auditoría informática	(Harris & Williams, 2020; International Auditing and Assurance Standards Board, 2014; Stoel et al., 2012)
	Los conocimientos del equipo auditor aportan valor a la organización auditada	
	Los miembros del equipo auditor demuestran conocimiento en seguridad de la información y procesamiento de datos	
Interacciones entre involucrados en el proceso	Las diferencias con el cliente son tratadas de forma oportuna, profesional y objetiva	(Hasas Yeghaneh et al., 2015; Havelka & Merhout, 2007; International Auditing and Assurance Standards Board, 2014)
	El equipo auditor está disponible para atender las solicitudes del cliente	
	Los involucrados en la auditoría mantienen una comunicación frecuente	
Reuniones del equipo auditor	El equipo auditor mantiene reuniones regulares, formales y claras para el análisis de avances y resultados	(Yasin & Nelson, 2012)
Cooperación (equipo de auditoría)	El auditor vincula expertos como apoyo en el proceso de auditoría para obtener resultados y recomendaciones para el cliente	(Hasas Yeghaneh et al., 2015; Havelka & Merhout, 2007)
	El equipo auditor es parte de un equipo técnico que trabaja en proyectos de investigación	

	El equipo auditor selecciona apropiadamente expertos y consultores	
Compromiso	El auditor sigue políticas y procedimientos que reglamentan su cumplimiento ético y profesional	(Guindel, 2010; Refaat & El-Henawy, 2019)
	El equipo auditor y responsables de la organización auditada muestran su compromiso al desarrollar el trabajo con calidad, principios y valores	
Factor Técnico		
Buenas prácticas	El equipo auditor usa plantillas y formularios para documentar	(Holm & Zaman, 2012)
	El equipo auditor tiene procedimientos de aprobación para las actividades completadas de la auditoría	
Proceso de revisión y seguimiento	El auditor y responsables de la organización auditada dan seguimiento a los problemas de auditorías informáticas anteriores	(Holm & Zaman, 2012)
Fiabilidad	Los hallazgos y conclusiones de la auditoría son un reflejo exacto de los hechos reales del proceso auditado	(Committee Contact of Heads of EU SAIs, 2004; Strous, 2002)
	Los resultados de la auditoría están totalmente respaldados y documentados con las evidencias recopiladas al auditar	
Seguridad	Los miembros del equipo auditor y responsables de la institución	(Strous, 2002)

	aseguran en todo momento la información	
Eficacia	Se logran los objetivos planteados en el plan de auditoría	(Committee Contact of Heads of EU SAIs, 2004; Strous, 2002)
	Los hallazgos, conclusiones y recomendaciones fueron receptados positivamente por el cliente	
Eficiencia	Los recursos asignados a la auditoría van de acuerdo con la importancia y complejidad de la auditoría	(Committee Contact of Heads of EU SAIs, 2004; Strous, 2002)
Importancia	El sistema, proceso u objeto auditado tiene importancia para la organización	(Committee Contact of Heads of EU SAIs, 2004)
	El cliente entiende el proceso y propósito de la auditoría informática	
Alcance	En el alcance se abordan todos los elementos necesarios para auditar exitosamente	(Committee Contact of Heads of EU SAIs, 2004; Hasas Yeghaneh et al., 2015; Stoel et al., 2012)
	La ejecución de la auditoría cumple con los elementos acordados en el alcance	
Puntualidad	El equipo auditor cumple con los compromisos adquiridos en las fechas establecidas	(Committee Contact of Heads of EU SAIs, 2004)
	Los resultados se entregan en el momento adecuado y establecido	
Evaluación de riesgos	El modelo de evaluación de riesgos es comprensible	(Havelka & Merhout, 2007;

(Complejidad)	El plan de auditoría toma en cuenta los riesgos relacionados con el cliente	Knechel et al., 2013; Sulaiman et al., 2019)
Tiempo asignado para la auditoría	El equipo auditor está de acuerdo con la fecha límite para completar la auditoría	(Dickins et al., 2018; Havelka & Merhout, 2007; International Auditing and Assurance Standards Board, 2014)
Rigor en el proceso de auditoría	El proceso de auditoría se desarrolla con exactitud y precisión	(International Auditing and Assurance Standards Board, 2014)
Informes de auditoría (Resultados)	El informe de auditoría es claro y conciso con sus resultados	(Committee Contact of Heads of EU SAIs, 2004; Holm & Zaman, 2012; International Auditing and Assurance Standards Board, 2014; Knechel et al., 2013)
	El alcance, hallazgos y recomendaciones son entendibles para cualquier persona que haga uso del informe de auditoría	
	La presentación de informes se realiza bajo las políticas, estándares, manuales, directrices y prácticas de auditoría informática	
	La forma y el contenido del informe sigue el estándar y cumple con los requisitos como: título, firma, fecha, objetivos, alcance, destinatario, base legal, entre otros	

	Las observaciones, evaluaciones y conclusiones del informe están debidamente respaldadas y documentadas	
Trabajo de campo (Implementación de la auditoría)	El equipo auditor realiza el trabajo de campo de manera adecuada	(Hasas Yeghaneh et al., 2015; Stoel et al., 2012)
	La auditoría se ejecuta bajo las políticas, estándares, manuales, directrices y prácticas de auditoría informática	
	El equipo auditor conoce técnicas y procedimientos para recopilar las evidencias de la auditoría	
	Todas las actividades se desarrollan de acuerdo con lo planificado	
	La documentación está debidamente referenciada	
	Las listas de verificación están completas, aprobadas y documentadas	
	El trabajo de campo es revisado por un experto	
Auditabilidad	El cliente o responsables de la organización auditada brindan apoyo competente para la recopilación de la información	(Hasas Yeghaneh et al., 2015; Stoel et al., 2012)
	La información y resultados de anteriores auditorías están disponibles para revisión	
Planificación	La auditoría se planifica adecuadamente	

	La planificación se desarrolla de acuerdo con políticas, estándares, manuales, directrices y prácticas de auditoría informática	(Hasas Yeghaneh et al., 2015; Stoel et al., 2012)
	Los objetivos y el alcance de la auditoría están especificados adecuadamente	
	Las actividades y herramientas para la auditoría están descritas claramente	
	Los miembros del equipo auditor tienen una comprensión clara y coherente del plan de auditoría	
	El presupuesto y cronograma de auditoría se establecen de manera adecuada	
	Se evalúa los recursos necesarios para realizar la auditoría	
	Se evalúa los requisitos de personal y equipos asignados para la auditoría	
	El plan de auditoría es elaborado, revisado y aprobado por los supervisores, responsables de la organización y miembros del equipo auditor	
Metodología	El equipo auditor utiliza una metodología de auditoría informática para planificar, gestionar y desarrollar la auditoría	(Havelka & Merhout, 2007; Stoel et al., 2012)
	El equipo auditor usa herramientas tecnológicas y	

	nuevas metodologías para realizar su trabajo	
	Factor Contextual	
Cultura Organizacional (Entorno empresarial)	La estructura organizacional de la institución se refleja en el plan de auditoría	(Holm & Zaman, 2012; International Auditing and Assurance Standards Board, 2014)
	El auditor promueve a través de sus informes una cultura organizacional basada en buenas prácticas de seguridad informática	
Control de calidad	El equipo auditor tiene estrictos procedimientos de control de calidad	(International Auditing and Assurance Standards Board, 2014; Knechel et al., 2013; Sulaiman et al., 2019)
	El líder del equipo auditor está comprometido con el sistema de control de calidad	
Leyes y reglamentos	La normativa y regulaciones emitidas por organismos de control se reflejan en el plan de auditoría	(International Auditing and Assurance Standards Board, 2014)
	El equipo auditor presenta recomendaciones que la organización debe seguir por actualización en normas internacionales, regulación local, objetivos estratégicos y cambios en el entorno	
	El equipo auditor conoce la información relevante de leyes y regulaciones que puedan tener un	

	impacto significativo en los objetivos de la auditoría	
Reglamento de auditoría	El equipo auditor tiene los permisos necesarios para desarrollar la auditoría	(Havelka & Merhout, 2007; International Auditing and Assurance Standards Board, 2014)
	Se aplican medidas disciplinarias en caso de incumplir con lo planificado o la normativa legal regulatoria vigente	
Entorno de litigio	El equipo auditor está preparado ante el riesgo de litigio	(International Auditing and Assurance Standards Board, 2014; Public Company Accounting Oversight Board, 2015)
Recursos	El equipo auditor tiene acceso a recursos humanos y técnicos para una auditoría especializada	(Hasas Yeghaneh et al., 2015; Stoel et al., 2012)
	El equipo auditor tiene acceso a los recursos necesarios para cumplir con el alcance y calendario de la auditoría	
Honorarios de auditoría	El costo de la auditoría va de acuerdo con la complejidad y las actividades desarrolladas	(Harris & Williams, 2020; Knechel et al., 2013)
Control interno	El equipo auditor está bien informado sobre los controles internos	(Public Company Accounting

	El equipo auditor identifica los elementos clave del sistema de control interno del cliente	Oversight Board, 2015)

Las auditorías con altos niveles de calidad involucran a los auditores que aplican un riguroso proceso de auditoría que incluye la selección de herramientas, metodologías, métodos, etc., para que su resultado sea más claro y confiable (International Auditing and Assurance Standards Board, 2014).

El entorno en el que se llevan a cabo las auditorías varía de un país a otro, a medida que un país se desarrolla y que las empresas crecen en tamaño, el entorno se vuelve más complejo por su evolución en las leyes, requisitos, procesos de gobierno corporativo y la cultura organizacional, por tal motivo es necesario conocerlo y manejarlo adecuadamente (International Auditing and Assurance Standards Board, 2014).

2.5. Estándares internacionales de seguridad de la información

Después de la revisión bibliográfica se encontró que los estándares de seguridad de la información más destacados son: ISO/IEC 27000, COBIT e ITIL (ver tabla 2.5).

Tabla 2.5 Estándares de seguridad de la información

Estándar	Artículos seleccionados
ISO 27000	(Cheng et al., 2008; Florentino et al., 2021; Hadlington et al., 2021; Hemphill & Longstreet, 2016; Höne & Eloff, 2002; Karie et al., 2021; Lundgren & Möller, 2019; Meriah & Arfa Rabai, 2019; Mirtsch, Kinne, et al., 2021; Peltier, 2001; Ranaweera et al., 2022; Schmitz et al., 2021; Shrivastava et al., 2021; Wang & Tsai, 2009; Zhou et al., 2022)
COBIT	(Cheng et al., 2008; O. M. Fal', 2017; Hadlington et al., 2021; Knight et al., 2007; Lundgren & Möller, 2019; Meriah & Arfa Rabai, 2019; Mesquida & Mas, 2015a; Mirtsch, Blind, et al., 2021)

ITIL	(Al-Karaki et al., 2020; A. M. Fal', 2010; Florentino et al., 2021; Gebremichael et al., 2020; Hsu et al., 2020)

2.5.1 ISO/IEC 27000

Existen varios estándares de seguridad de la información, iniciando por el grupo de estándares ISO/IEC 27000 que integran un sistema de administración de seguridad de la información, el mismo que está enfocado en la seguridad de la información bajo un explícito control administrativo de la misma (Mesquida & Mas, 2015b).

ISO 27000 es una serie de estándares internacionales sobre seguridad de la información que contiene un conjunto de buenas prácticas para establecer, implementar, mantener y mejorar los Sistemas de Gestión de Seguridad de la Información (de la Rosa, 2021). Los principales pilares de la familia 27000 son los estándares 27001 y 27002, la principal diferencia entre estos dos estándares es que el 27001 se basa en la gestión continua de la seguridad, apoyada en la identificación continua de riesgos. Y la 27002 es una guía de buenas prácticas que describe un conjunto de objetivos de control y gestión que una organización debe perseguir (Cheng et al., 2008).

ISO/IEC 27001 es reconocido internacionalmente porque garantiza que una empresa u organización está cumpliendo los requisitos básicos en seguridad de la información y que su sistema de gestión de la información sea adecuado. Estos requisitos incluyen todas las medidas y documentos que son necesarios para proporcionar una protección óptima de los datos, salvaguardar la integridad de los datos de operaciones y garantizar la disponibilidad de los sistemas informáticos de la empresa, incluyendo sus planes de emergencia y análisis de riesgos (Cheng et al., 2008).

ISO/IEC 27002 es un estándar para la seguridad de la información creada por la organización internacional de normalización y comisión electrotecnia internacional, la misma que brinda diferentes recomendaciones de las mejores prácticas en la gestión de la seguridad de la información a todos los interesados y responsables. La seguridad de la información se consigue con la implementación de un conjunto de controles que incluyen políticas, procesos,

estructuras organizativas y funciones de hardware y software. Estos controles se deben establecer, implementar, supervisar, revisar y mejorar cuando sea necesario para asegurar que se cumplan los objetivos específicos de seguridad y de negocio de la organización (Guamán, 2019).

2.5.2 COBIT

El modelo COBIT (Control Objectives for In- formation and related Technology) es el marco internacional de buenas prácticas para controlar la información de TI y los peligros que conlleva. COBIT se utiliza para llevar a cabo el régimen de TI y mejorar sus controles (Hsu et al., 2020). Así mismo, tiene fines de control, directrices de aseguramiento, mediciones de funcionamiento y resultados, componentes críticos de triunfo y modelos de madurez (Gebremichael et al., 2020).

Permite a los gerentes cubrir la brecha entre los requisitos de control, los aspectos técnicos y riesgos de negocio (Karie et al., 2021). COBIT hace viable el desarrollo de una política clara y buenas prácticas para los controles de TI a través de las organizaciones (Mesquida et al., 2014). Este estándar hace énfasis en la conformidad de regulaciones, ayuda a las organizaciones a incrementar el valor alcanzado desde la TI, permite el alineamiento y simplifica la implementación de COBIT (Siponen & Willison, 2009).

La nueva versión de esta normativa se basa en cinco principios clave (Breda & Kiss, 2020; Hemphill & Longstreet, 2016):

Principio 1: Satisfacer las necesidades de las Partes Interesadas.

Principio 2: Cubrir la organización de principio a fin. Integrando el Gobierno corporativo con el Gobierno de las TI. Orientación al negocio.

Principio 3: La aplicación de un único marco de trabajo integrado.

Principio 4: Habilitación de un enfoque holístico. Para conseguir una Gestión y Gobierno de las TI con eficiencia y eficacia.

Principio 5: La separación la Gestión de Gobierno.

2.5.3 ITIL

La Biblioteca de Infraestructura de Tecnologías de la Información ITIL está basado en un conjunto de mejores prácticas para la gestión de servicios de

tecnologías de la información en lo referente a personas, procesos y tecnología, las cuales fueron desarrolladas por la OGC (Oficina Gubernamental de Comercio) del Reino Unido (Mirtsch, Blind, et al., 2021).

A través de las buenas prácticas detalladas en ITIL se hace posible para departamentos y organizaciones reducir costos, mejorar la calidad del servicio, tanto a clientes externos como internos y optimizar al máximo las habilidades y destrezas del personal mejorando su productividad (Humphreys, 2011).

2.6. Métricas para evaluar seguridad de la información

Para la clasificación de los artículos se han tomado en cuenta los controles para evaluar el cumplimiento de los pilares de seguridad, específicamente: disponibilidad, integridad, confidencialidad, autenticidad y trazabilidad (Gómez Enciso & Porras Flores, 2018). En la tabla 2.6 se exponen los resultados obtenidos de la revisión bibliográfica para las métricas de evaluación en seguridad de la información.

Tabla 2.6 Pilares de seguridad identificados

Pilar de Seguridad	Artículos
Autenticidad	(Dhanaraj et al., 2021; Diesch et al., 2020; Fang et al., 2021; Hong et al., 2018; Ma, 2022; Philippou et al., 2020)
Integridad	(Eom et al., 2019; Gunes et al., 2021; Halabi & Bellaiche, 2017; Halvorsen et al., 2019; Heigl et al., 2021; Khaleel & Abduljaleel, 2021; Kure et al., 2018; Ramos et al., 2017; Wagner & Eckhoff, 2019)
Confidencialidad	(Alcaraz Velasco et al., 2021; Baldi et al., 2019; Cho et al., 2016; Deng et al., 2017; Domingo-Ferrer et al., 2020; Guo & Wang, 2020; McLeod & Dolezel, 2022)
Disponibilidad	(Ahmed & Pathan, 2020; Behal & Kumar, 2017; Falco et al., 2018; Gunes et al., 2021; Jiang & Atif, 2021; Kure et al., 2018)
Trazabilidad	(Ahmed & Pathan, 2020; Andersson et al., 2021; Enoch et al., 2020; Kure et al., 2018; Shan et al., 2018)

La Tabla 2.7 muestra detalladamente las métricas para evaluar la seguridad de la información que se han encontrado en los artículos analizados.

Tabla 2.7 Métricas de seguridad

Pilar de Seguridad	Métricas	Artículos
Autenticidad	Esfuerzo de defensa ante ataques	(Hong et al., 2018)
	Seguridad física, control de acceso, concienciación e infraestructura	(Behal et al., 2021; Dhanaraj et al., 2021; Diesch et al., 2020; Shan et al., 2018)
	Control de amenazas, autorización, autenticación	(Jiang & Atif, 2021; Ma, 2022)
	Detección de antipatrón	(Dhanaraj et al., 2021)
	Control de personal autorizado, efectividad del proceso	(Philippou et al., 2020)
Integridad	Seguridad del proceso, software, red y organización	(Gunes et al., 2021; Khaleel & Abduljaleel, 2021; Kure et al., 2018; Ramos et al., 2017)
	Privacidad y entropía	(Halabi & Bellaiche, 2017; Wagner & Eckhoff, 2019)
	Observación y ataques	(Halvorsen et al., 2019)
	Control de transmisión de datos	(Heigl et al., 2021)
	Impacto de ataques	(Eom et al., 2019)

Confidencialidad	Confiabilidad y mantenibilidad	(Cho et al., 2016; Domingo-Ferrer et al., 2020; McLeod & Dolezel, 2022)
	Validez de datos	(Guo & Wang, 2020; Hassandoust et al., 2022)
	Capacidad de secreto e interrupción del secreto	(Baldi et al., 2019; Deng et al., 2017)
Disponibilidad	Accesibilidad a activos	(Gunes et al., 2021; Jiang & Atif, 2021; Kure et al., 2018)
	Funcionamiento de sistemas informáticos	(Behal et al., 2021; Falco et al., 2018)
	Interrupciones del servicio	(Jiang & Atif, 2021)
	Salvaguarda de recursos	(Ahmed & Pathan, 2020)
Trazabilidad	Registro de actividades (quién hizo, qué hizo, cuándo lo hizo)	(Kure et al., 2018)
	Control de incidentes	(Ahmed & Pathan, 2020; Andersson et al., 2021; Enoch et al., 2020)
	Control de atacantes	(Enoch et al., 2020; Shan et al., 2018)

2.7. Métodos, metodologías y marcos referenciales utilizados en auditoría informática

Las auditorías se consideran como una herramienta para la toma de decisiones y mejora continua dentro de la gestión de los sistemas. Este principio es el mejor punto de inicio porque están diseñadas para ayudar y no deben crear un problema. Cuando una organización decide implementar un sistema de gestión de mejora continua, toma una decisión estratégica a nivel de negocio y, luego, deben ejecutarla a nivel operativo (Cienfuegos et al., 2021).

El incremento y la evolución de la tecnología aumenta la necesidad de realizar un análisis de amenazas, vulnerabilidades y riesgos a los que están expuestos los activos informáticos, por esa razón la seguridad informática juega un papel muy importante dentro de las instituciones, para evitar todo tipo de corrupción de datos, ya que en la mayoría de las organizaciones los datos son gestionados por un sistema informático (Escobar, 2021).

Si bien la información en una organización constituye un activo esencial que genera ventajas competitivas, innovación, desarrollo e ingresos (Stable-Rodríguez, 2012), en ciertos escenarios se considera a los datos como “el nuevo petróleo”. Debido al desarrollo de la tecnología, al entorno cada vez más cambiante y a la cantidad de información generada, se pone mayor énfasis en el tema de auditar el ambiente técnico y tecnológico de las organizaciones o instituciones.

A pesar de no existir una metodología que sea reconocida de manera general dentro de las auditorías informáticas, la experiencia y conocimiento del auditor ayuda a que se seleccione la óptima y que sirva de apoyo. Cualquiera que sea la metodología seleccionada debe cubrir todos los problemas y seguir el mismo estándar para tener acciones y resultados documentados satisfactoriamente (Committee Contact of Heads of EU SAIs, 2004; San Pedro, 2022; Trujillo Albarrán et al., 2019).

Cabe resaltar que en la actualidad a nivel internacional se han encontrado marcos referenciales, estándares o normas que apoyan en la administración de la seguridad de la información. La búsqueda permitió encontrar variedad de marcos de referencia que gestionan las auditorías informáticas, así como, en el

área de ciberseguridad (Arcentales Fernández & Caycedo Casas, 2017). Los resultados se presentan en la tabla 2.8, clasificados por el organismo normativo internacional.

Tabla 2.8 Marcos de referencia para auditorías informáticas

Organismo Normativo	Marco de Referencia
Australian Goverment. Departament of Enviroment	Indepent Audit and Audit Report Guidelines
ECA	European Court of Auditors: Guideline for audit of IT enviroment
ENISA	European Union Agency for Network and Information Security: Auditing Framework for TSPs
HITRUST CSF	Health Information Trust Alliance: HITRUST Common Security Framework
INCIBE	Instituto Nacional de Ciberseguridad España: Taxonomía de Soluciones de Ciberseguridad.
IIA'S	The Institute of Internal Auditors: Global Technology Audit Guidelines
ISACA	Systems Audit and Control Association: ITAF -Information Technology Assurance Framework
	COBIT 4.1/COBIT 5
ISSAI/INTOSAI	International Standars of Supreme Audit Institutions/International Organization of Supreme Audit Institutions: Guidelines on IT Audit ISSAI 5300.
ISO	ISO / IEC 27001: 2013 - Information technology - Security techniques - Information security management systems - Requirements
	ISO 19011 - Directrices para la auditoría de Sistemas de Gestión
NIST	National Institute of Standars and Technology: Cybersecurity Framework Audit Program.
NSW Government	New South Wales Government: Indepent Audit Guideline
PCAOB	Public Company Accounting Oversight Board: Risk Assessment Auditing Standars

Fuente: (Cajas & Luje, 2019)

Los marcos referenciales escogidos en este estudio están basados en el cumplimiento de ciertos parámetros y son los siguientes:

2.7.1. ISO 19011

La norma proporciona pautas que permiten auditar sistemas de gestión, una de las ventajas de esta norma es que es aplicable a cualquier organización o institución que necesite planificar y preparar auditorías internas y externas o planes de auditoría de gestión, considerando la integridad, objetividad, cuidado profesional, confidencialidad, enfoque basado en evidencia y riesgo como principios de auditoría (ISO 19011, 2018).

2.7.2. ITAF

Es un marco de referencia que establece directrices de auditoría, buenas prácticas, estándares, define funciones, aseguramiento de roles y responsabilidades profesionales en base a conocimientos y habilidades para asegurar una auditoría de TI. Está basado en el material de ISACA que es una fuente de conocimiento para profesionales y expertos de auditoría, cuenta con un amplio catálogo de guías, procedimientos de investigación, políticas y desarrollo de informes para auditorías de TI efectivas (ISACA, 2020).

Está estructurado por normas generales (atributos del auditor, principios del auditor), directrices de rendimiento (parámetros de seguimiento de tareas) y directrices de informes (reportes, comunicación de informes).

2.7.3. ISSAI 5300

Es un marco de referencia desarrollado en base a la norma ISSAI, tiene un alcance global y establece lineamientos y principios para realizar auditorías informáticas. La norma puede ser utilizada como guía para la implementación de la auditoría, el desarrollo de capacidades de auditoría y la gestión de sus recursos, su objetivo es brindar seguridad a la organización auditada para mejorar la integridad y confiabilidad de los resultados obtenidos (INTOSAI & ISSAI, 2016).

2.7.4. IIA's CTAGs

El objetivo de la guía es ayudar a los auditores internos a sentirse más cómodos con los controles generales de TI para que puedan comunicarse con confianza con el comité de auditoría y comunicar ideas de riesgo y control con el director de información y su administración. Proporciona guías que orientan a los auditores internos a comprender el entorno de TI en la organización considerando las áreas de TI, seguridad de TI y auditoría de TI y sus conceptos (GTAG, 2012).

2.8. Técnicas avanzadas de datos en auditoría

Las técnicas avanzadas junto con otros desarrollos tecnológicos de procesamiento de datos despiertan gran interés y se aplican intensamente en muchas organizaciones para recopilar, transformar, analizar e identificar patrones en grandes volúmenes de datos, apoyar argumentos y tomar decisiones (Krieger & Drews, 2018; Moutaz et al., 2018).

El incremento del 27% al 31% de la tasa bruta en matrículas e ingresos en IES en el 2021 (Instituto Nacional de Estadística y Censos, 2021), ha requerido la implementación de sistema académicos para facilitar la gestión de usuarios, infraestructura, notas, tareas, entre otros y sumando el entorno virtual de clases en épocas de pandemia, da como resultado una gran cantidad de datos e información que complican la tarea del auditor, sin embargo la aplicación de técnicas avanzadas de datos en la auditoría puede acelerar el proceso sin sesgo de información (Moutaz et al., 2018).

La capacidad del manejo de grandes volúmenes de datos obliga al auditor informático a adoptar técnicas avanzadas de datos con el fin de identificar fallas e interpretar de mejor manera la información para optimizar los procesos tradicionales (Castello, 2006). Además, con la aplicación de técnicas de BigData y el análisis de datos es posible realizar pruebas de auditoría sobre un porcentaje más alto o incluso la totalidad de una población.

En los últimos años, se manifestó un creciente interés en el uso de modelos de BigData a nivel empresarial a pesar de la poca experiencia en tecnologías de la información y presupuesto adecuado para la inversión de estas tecnologías (Redavid et al., 2018).

En la actualidad existen técnicas que ya se aplican, y que están relacionadas con la inteligencia artificial o machine learning, las mismas que trabajan monitoreando operaciones contables en tiempo real (Blázquez, 2018), sin embargo después de la información analizada no se especifica una técnica avanzada de datos que se aplique en procesos de auditoría informática dentro de IES.

2.9. Funciones sustantivas en IES

Los procesos y acciones dentro de las IES están siempre relacionados con el hombre, la ciencia y la sociedad. La palabra universidad se asocia con lo universal en dos sentidos, por un lado, se entiende como un centro de educación superior que reúne diferentes ciencias y disciplinas, y por otro lado, por la validez universal de los conocimientos adquiridos (Fabre, 2005).

Las IES tienen la necesidad de integrar sus procesos para asegurar su correcto accionar y proyecciones de sostenibilidad (García & Fernández, 2020), con el fin de transformar y mejorar el entorno social. En ese contexto, se concretan tres procesos conocidos como funciones sustantivas, que se ponen en ejecución por acción del conocimiento: docencia, investigación y vinculación o extensión según la (Ley Orgánica de Educación Superior, 2018).

Las funciones sustantivas son los vehículos a través de los cuales las IES aspiran a cumplir su misión y los objetivos estratégicos institucionales, de acuerdo con su descripción de la tabla 2.9:

Tabla 2.9 Funciones Sustantivas en Educación Superior

Función Sustantiva	Descripción	Indicadores
Docencia	Función de las IES para estructurar, enseñar y evaluar los programas de formación integral de los estudiantes, en todas las modalidades, ciclos, lugares y metodologías.	Cobertura e incremento de matrículas. Tasa de retención y eficiencia terminal, de las universidades y escuelas politécnicas.
Investigación	Función que impulsa en las IES el desarrollo de la ciencia, tecnología e innovación para la	Impacto y aplicabilidad de las investigaciones a los problemas del país. Pblicaciones científicas.

	creación e implementación de soluciones a problemas sociales y como apoyo a los procesos de enseñanza – aprendizaje.	Registros que otorguen derechos de propiedad intelectual. Innovaciones generadas que contribuyan a la reducción de la pobreza, promoción de la equidad, incremento de la productividad o al mejoramiento de la estructura productiva del país.
Vinculación	Función de las IES para el desarrollo integral y sostenible de personas, comunidades y territorios, a través de proyectos que generen impacto en la sociedad.	Contribución de las IES a la solución de los problemas sociales, ambientales y productivos, con especial atención en los grupos vulnerables.

Fuente: (Ley Orgánica de Educación Superior, 2018).

2.10. Resumen

Sobre la base de lo expuesto, se resume que:

En las IES del Ecuador existen acciones de cambio para el desarrollo del entorno académico y tecnológico a pesar de la complejidad de los procesos que manejan y la constante actualización de leyes que el órgano de control presenta en las instituciones. De acuerdo con estudios realizados por CEDIA las IES más grandes del país ya han logrado automatizar sus procesos, mientras que en las IES pequeñas cumplir con ese objetivo se ha vuelto más lento por la falta de recursos y la baja cantidad de datos administrados.

Considerando el crecimiento de sistemas de información dentro de las IES, se vuelve una necesidad verificar su desempeño e identificar fallas a través de una auditoría informática para así garantizar la calidad y mejora de la gestión académica, el rendimiento institucional, su eficiencia y consistencia, considerando sus necesidades y funciones sustanivas.

Para lograr que una auditoría cumpla con estándares de calidad y seguridad en los resultados que generen se deben considerar normas para la seguridad de la información y los 3 factores de calidad (factor humano, factor técnico y

factor contextual) con sus aspectos más relevantes, lo que garantiza un proceso bien diseñado por auditores capacitados que comprenden el entorno y se ajustan a herramientas y técnicas únicas de la auditoría.

Para ayudar al desarrollo de procesos de auditoría informática en el que se manejen grandes cantidades de datos es necesario incluir técnicas de datos que ayuden a mejorar los mecanismos para la manipulación y abstracción de la información permitiendo el uso de herramientas que permiten agilizar las tareas prolongadas a los auditores.

3. CAPÍTULO III

3.1. Situación actual de la auditoría

Los sistemas de información de las IES presentan “insuficiencias en su desempeño integral para contribuir a un control de gestión para la toma de decisiones, que responda a las Normas Técnicas Ecuatorianas (NTE) vigentes en el país”. Por lo que se ha visto la necesidad de aplicar evaluaciones para mejorar la seguridad de los productos y procesos que tienen como activo la información (Altamirano, 2019)

Según el Director del Departamento Informática y Comunicaciones de la Universidad Estatal de Bolívar al contar con verdaderos indicadores de TIC en las IES del Ecuador es posible establecer estrategias y líneas de acción de desarrollo, como ayuda para lograr la homogeneidad del proceso y de la información académica superior del país (Rivadeneira Ramos, 2018).

Para tratar de dar respuestas a esta situación, se trabajará en dos fases. La primera fase presenta un estudio de la situación actual en las IES y de temas relacionados con auditoría informática (metodologías, herramientas, calidad y seguridad en los resultados, entre otros). En la segunda fase se propone un método de auditoría informática para IES que describe la estandarización del proceso basado en la ISO 9001 el cual se irá describiendo paso a paso para su ejecución.

Las tecnologías de la información y la comunicación soportan servicios y procesos críticos dentro de las IES, por tanto, es necesario que estos estén implantados con estándares de calidad y seguridad para proteger la información. Para verificar que los procesos se estén ejecutando correctamente se ejecutan auditorías como método de evaluación, de acuerdo con un estudio realizado por CEDIA al grupo de IES que pertenecen a la corporación se conoce que el 17% de las universidades aún no tiene una política de seguridad debidamente formalizada y aprobada. El 69% tiene un responsable de seguridad de la información y más de la mitad realizan auditorías específicas. El 55% cuenta con el servicio de respuesta a incidentes de seguridad (CSIRT) proporcionado por CEDIA y un 10% por uno propio. El 69% no cuenta con un plan de contingencia y el 36% no cuenta con un plan de continuidad de los servicios. Dada la importancia que están cobrando las TIC en las universidades,

esto son riesgos que las universidades no deberían correr (Cadena et al., 2018). Las auditorías implementadas en las IES han utilizado como técnicas para la recolección de información las entrevistas al personal y encargados del área tecnológica, análisis documental, análisis FODA, así como también cuestionarios e inspecciones al área de evaluación (Freire, 2016; Llumiquinga & Pilco, 2015; Paredes & Vega, 2011; Pusdá & Imbaquingo, 2015). Los datos están basados en la tabla 3.1:

Tabla 3.1 Datos estudio de CEDIA

Universo	Universidades públicas y privadas del Ecuador, en total 60
Ámbito	Ecuador
Procedimiento de muestreo	Sistema de Encuestas para el levantamiento de información
Tasa de Respuesta	70%
Tamaño de muestra	42 universidades
Nivel de confianza	95%
Margen de error	8%
Trabajo de campo	junio – noviembre 2018

En este contexto, con los factores y métricas identificadas se describe la situación actual en las IES con respecto al nivel de calidad de los resultados de procesos de auditoría informática en IES Ecuatorianas, con ese fin se aplicó una encuesta a las 42 IES que forman parte de la Corporación Ecuatoriana para el Desarrollo de la Investigación y la Academia (CEDIA), sin embargo, solamente 19 de las instituciones encuestadas han pasado por un proceso de auditoría informática, tal y como se muestra en la tabla 3.2.

Tabla 3.2 IES que han sido parte de una auditoría informática

Auditoría Informática	IES	Porcentaje
Sí	19	76%
No	6	24%

Total	25	100%

De las 19 IES en las que se ha realizado algún tipo de auditoría informática se conoce que el 73% han sido auditorías internas y el 26% auditorías externas, en su mayoría por parte de la Contraloría General del Estado, tal y como se muestra en la tabla 3.3:

Tabla 3.3 Auditoría interna o externa en IES

Tipo de Auditoría	IES	Porcentaje
Interna	14	73,68%
Externa	5	26,32%
Total	19	100%

La encuesta aplicada permite evaluar cada factor con las métricas identificadas para cada uno, a cada métrica se le asigna una calificación en un rango del 1 al 10 de acuerdo con cómo se ejecutó el proceso de auditoría. Esta calificación es un valor que debe señalar como se consideró la métrica durante el proceso de auditoría y poder comparar con todas las involucradas en la calidad.

La calificación total del conjunto de métricas se presenta a través de un promedio acompañado del porcentaje del nivel de calidad de los resultados del proceso de auditoría. De esta manera se puede prestar atención a aquellos aspectos con bajas calificaciones para poder mejorarlas en procesos futuros.

El promedio final refleja el nivel de calidad que tienen los resultados del proceso de auditoría informática evaluado (ver tabla 3.4) y se interpreta de la siguiente manera:

Entre 85% y 100%: CALIDAD DE LA AUDITORÍA ALTA.

Entre 64% y 84%: CALIDAD DE LA AUDITORÍA MEDIA.

Menos de 65% CALIDAD DE LA AUDITORÍA BAJA.

Tabla 3.4 Nivel de calidad de auditoría en IES

Cod IES	Nivel de Calidad	Nivel Factor Humano	Nivel Factor Técnico	Nivel Factor Contextual
IES01	99%	100%	99%	100%
IES02	40%	40%	40%	40%
IES03	71%	75%	73%	51%
IES04	74%	69%	76%	81%

IES05	93%	92%	93%	90%
IES06	93%	92%	97%	80%
IES07	87%	88%	86%	86%
IES08	67%	71%	66%	60%
IES09	80%	84%	79%	73%
IES10	73%	78%	69%	74%
IES11	100%	100%	100%	100%
IES12	84%	78%	87%	87%
IES13	79%	81%	79%	71%
IES14	40%	40%	40%	40%
IES15	93%	92%	93%	90%
IES16	67%	71%	66%	60%
IES17	73%	78%	69%	74%
IES18	84%	78%	87%	87%
IES19	80%	84%	79%	73%

De acuerdo con los resultados obtenidos se tiene que de las 19 IES encuestadas 6 han tenido procesos de auditoría con nivel alto de calidad en sus resultados, mientras que 11 instituciones han tenido un nivel medio y los 2 restantes han sido de bajo nivel.

Bajo los criterios de evaluación en los resultados se puede observar que el nivel general de calidad de 77,67%, siendo el factor contextual quien tiene la más baja puntuación, seguido del factor técnico y por otro lado es el factor humano el mejor calificado (ver Tabla 3.5).

Tabla 3.5 Resumen del nivel de calidad de auditoría

Nivel de Calidad	Nivel Factor Humano	Nivel Factor Técnico	Nivel Factor Contextual
77,67%	78,42%	77,79%	74,66%

Para conocer la situación actual de las IES en términos de seguridad de la información y con el estándar determinado se hace la evaluación bajo las métricas identificadas en el estado del arte, una vez aplicado el instrumento se determina que el nivel de seguridad en las IES evaluadas es bajo (ver Tabla 3.6):

Tabla 3.6 Nivel de seguridad en IES

Promedio	Nivel de Seguridad
6,52	65%

Los puntos estratégicos de la ISO 27000 con los que se evaluó a las IES y que contiene los problemas y recomendaciones asociados a políticas para la seguridad de la información, control de acceso, seguridad ligada a los recursos humanos, seguridad en la operativa, gestión de incidentes, cifrado, gestión de activos y cumplimiento.

De acuerdo con la evaluación aplicada a las IES, el 15,79% de instituciones no cuenta con políticas para la seguridad de la información, ni control de acceso a infraestructura y servicios de TI, lo que genera una serie de riesgos relacionados a daños físicos, pérdida de servicios esenciales, afectaciones por radiación, acceso a la información, fallos técnicos, acciones no autorizadas y/o errores de las funciones. Todo esto se debe a que el usuario no conoce qué se puede hacer o cómo hacer sus labores sin vulnerar la información y actuarán bajo distintos comportamientos según su propio criterio.

Se determinó que sólo el 15,8% de IES evaluadas capacita al personal e involucrados de forma frecuente y existe el 5,3% de instituciones que nunca lo han hecho, las IES deben trabajar más en reducir los riesgos relacionados al error humano que la mayoría de las veces se cometen por el desconocimiento de los procedimientos y políticas de seguridad.

El 5,3% de IES nunca han hecho una valoración de sus sistemas desde su implementación, por lo que se reduce la seguridad y no se considera los peligros de los códigos maliciosos como el robo y destrucción de la información o daños e inutilización de los sistemas de la organización.

Solamente el 80% de IES ejecutan planes de monitoreo y gestión de impacto de incidentes de seguridad en la institución de forma ocasional, esto es alarmante ya que se debería hacer con más frecuencia, para que todos los empleados, contratistas y terceros estén al tanto de los procedimientos para informar de los diferentes tipos de eventos y debilidades que puedan tener impacto en la seguridad de los activos organizacionales.

Existen aspectos alarmantes como que solo el 10,5% de instituciones clasifica y cifra la información de manera frecuente, mientras que las restantes los hacen ocasionalmente y el 26,3% nunca lo hace, lo que genera una falta de protección o control en la gestión de la información y permite la materialización de potenciales amenazas como pérdida de servicios esenciales principalmente telecomunicaciones, intercepción, espionaje en remoto, robo de equipos,

recuperación desde medios reciclados o desechados, divulgación, manipulación de software y acciones no autorizadas.

Y solamente el 10,5% de las IES evaluadas realizan auditorías de cumplimiento de forma frecuente y ocasional, lo que denota una grave falta para la adecuada gestión de la información y debe ser algo a considerar por lo beneficios y mejoras que se pueden adoptar.Entre los beneficios que se obtienen al realizar una auditoría es evaluar los procesos que se gestionan en los departamentos de TI. Además, dentro de la implementación de una auditoría se evidenció que se pueden fortalecer los procesos y actividades de las IES por medio de un análisis de riesgos, permitiendo detectar las vulnerabilidades en los procesos y actividades de adquisición e implementación (Paredes & Vega, 2011; Silva, 2018).

Asimismo, una auditoría informática permite evaluar y controlar los recursos informáticos con los que cuenta una institución, identificando necesidades y proponiendo nuevas inversiones en tecnología (Buenaño & García, 2013).

Otro beneficio importante como resultado de una auditoría informática es asegurar que la información sea eficiente, veraz y segura, proporcionando todos los datos necesarios para el manejo de reportes y el proceso de toma de decisiones dentro de una IES (Freire, 2016; Pusdá & Imbaquingo, 2015).

Es importante mencionar que se debe asegurar en todo momento la calidad y la seguridad de los resultados obtenidos en el ejercicio de la auditoría, considerando cada una de las fases y sus actividades, con el fin de evitar los problemas que se presentan con los bajos niveles de estos indicadores (ver Tabla 3.7).

Tabla 3.7 Consecuencias de bajos niveles en calidad y seguridad de resultados de auditoría

Bajos niveles de calidad	Bajos niveles de seguridad
Resultados subjetivos	Pérdida o alteración de información
Informes no calificados	Accesos no autorizados
Falta de credibilidad de las entidades y procesos	Pérdida de servicios esenciales
Información irrelevante	Fallas técnicas

3.2. Marcos referenciales utilizados en auditoría

Para la construcción del MAIIES se considera la selección para la comparación y análisis de marcos referenciales de auditoría informática de organismos internacionales reconocidos a nivel mundial. Los marcos referenciales escogidos para el estudio están basados en el cumplimiento de ciertos parámetros: vigencia y cumplimiento de la estructura general de una auditoría informática, uso e implementación frecuente en procesos de auditoría, debe ser usado por expertos en auditoría informática y que sus actividades se adapten a los procesos de las IES. En la tabla 3.8 se presentan los marcos seleccionados.

Tabla 3.8 Marcos referenciales base del MAIIES

Organismo Normativo	Marco de Referencia
ISO	ISO 19011:2018 - Directrices para la auditoría de Sistemas de Gestión
ISSAI/INTOSAI	ISSAI 5300 – Guidelines on IT Audit
ISACA	ITAF - Information Technology Assurance Framework
IIA'S	Global Technology Audit Guidelines (CTAGs)

3.3. Comparación de fases y actividades de los marcos referenciales

Dentro de cada marco referencial existen procedimientos únicos para el desarrollo del proceso de auditoría, sin embargo, es necesario la unión de dos o más marcos o metodologías para que la auditoría se considere completa y exitosa. En consecuencia, para la creación del MAIIES se identificaron las actividades de cada marco para ser usadas como base en la propuesta del método. El consenso de actividades en común e individual de cada marco se resume en las fases del proceso de auditoría.

En la fase de planeación se tienen las siguientes actividades (ver tabla 3.9):

Tabla 3.9 Comparativa fase de planeación

Planeación de la Auditoría					
Código	**Característica**	**Marco referencial**			
		ISO 19011	**ISACA ITAF**	**ISSAI 5300**	**IIAS CTAGs**
P001	Generalidades	x			
P002	Carta de auditoría		x		
P003	Definir el equipo de auditoría	x		x	
P004	Asignación de las tareas al equipo auditor	x	x	x	x
P005	Establecimiento de niveles de riesgo: Estratégico, anual y de Equipo.			x	
P006	Definición del alcance de la auditoría.	x	x	x	x
P007	Definición de metas y objetivos de la auditoría.	x		x	x
P008	Determinación de la viabilidad de la auditoría	x			
P009	Revisión de resultados de auditorías anteriores		x		x
P011	Preparación y Revisión de la información documentada	x			
P012	Comunicación y aprobación.		x		x

En la fase de ejecución de la auditoría se identificaron las siguientes actividades dentro de cada marco (ver tabla 3.10).

Tabla 3.10 Comparativa fase de ejecución

Ejecución de la Auditoría					
Código	**Caracteristíca**	**Metodología**			
		ISO 19011	**ISACA ITAF**	**ISSAI 5300**	**IIAS CTAGs**

E001	Analizar e identificar los recursos de información	x	x	x	x
E002	Recolección y verificación de la información	x			x
E003	Selección de la muestra apropiada de auditoría	x	x	x	x
E004	Uso de herramientas e instrumentos para la auditoría	x	x		
E005	Recopilación de evidencia de auditoría		x	x	x
E006	Identificación de hallazgos de auditoría	x			
E007	Comunicación durante la auditoría	x			x
E008	Revisión de las evidencias mientras se lleva a cabo la auditoría		x	x	x
E009	Determinar conclusiones y recomendaciones de la auditoría	x	x	x	x
E010	Difusión de resultados				x
E011	Seguimiento			x	

Y para la fase de comunicación de resultados se tienen las siguientes actividades por marco referencial (ver tabla 3.11).

Tabla 3.11 Comparativa fase de comunicación de resultados

Comunicación de resultados					
Código	**Característica**	**Metodologías**			
		ISO 19011	**ISACA ITAF**	**ISSAI 5300**	**IIAS CTAGs**
D001	Análisis de la evidencia	x			
D002	Elaboración del informe de auditoría	x	x	x	x
D003	Objetivos	x	x		
D004	Alcance de la terea realizada			x	
D005	Limitaciones del alcance				x
D006	Observaciones	x	x	x	x
D007	Conclusiones	x	x	x	x

D008	Recomendaciones	x	x	x	x
D009	Opinión del auditado	x	x	x	x
D010	Anexos	x	x	x	x
D011	Cierre del Informe	x	x	x	x
D012	Exposición del informe de auditoría			x	
D013	Actividades de seguimiento		x		

La norma ISO 19011 cuenta con 23 actividades en total siendo la más completa en comparación con los marcos referenciales del estudio, mientras que la IIAS CTAGs con 21 actividades y la ISSAI 5300 e ITAF con 20 cada uno, la comparativa sirve como guía para el desarrollo del MAIIES.

3.4. Fases de la auditoría

Varios autores concuerdan en que una auditoría está estructurada en 3 fases: planificación de la auditoría, ejecución de la auditoría y comunicación de resultados (Álvarez Betancourth, 2016; Alvarez, 2018; Bonilla Mariño, 2015; De Rey, 2020; Universidad Ecotec, 2019).

Mientras que para el desarrollo del MAIIES se añaden las fases de validación y seguimiento, asegurando así un método completo con retroalimentación que incluye una evaluación en base a indicadores de calidad, seguridad y cumplimiento post auditoría, además se considera el seguimiento para fomentar una respuesta adecuada a los hallazgos identificados en la auditoría y para sentar las bases para futuros trabajos de auditoría (Committee Contact of Heads of EU SAIs, 2004).

3.5. Estandarización del método

Para la propuesta del MAIIES se toma en cuenta una estandarización basada en la Norma ISO 9001 y en base a la información, marcos referenciales, estándares, diagnóstico y comparación de metodologías estudiadas anteriormente.

3.5.1 Objetivo del método

El objetivo del método de auditoría planteado es asegurar una mayor calidad y seguridad de la información mediante la recomendación de lineamientos y controles proporcionados por marcos referenciales internacionales.

3.5.2 Matriz de partes interesadas

Es importante definir las partes interesadas dentro de cualquier proceso porque son quiénes influyen y toman las decisiones en todas las actividades a desarrollar. Las partes interesadas se convierten en objeto de seguimiento y medición porque son quiénes afectan o pueden verse afectadas por los diferentes procedimientos relacionados con los procesos de auditoría y la información generada (Álvarez, 2016; Gómez, 2022). Dentro de un proceso de auditoría se manifiestan dos participantes: cliente o auditado y el auditor o equipo auditor. El cliente es quién solicita y sobre quien se realiza la auditoria y el auditor es la persona con las competencias y conocimientos necesarios para ejecutar la auditoría (Caiza, 2017). A continuación, en la Tabla 3.12 se muestra la matriz de las partes interesadas, correspondientes al MAIIES.

Tabla 3.12 Matriz de partes interesadas

MATRIZ DE PARTES INTERESADAS		
PARTE INTERESADA	**REQUISITOS**	**PROCESOS DE LA PARTE INTERESADA**
Auditor / Equipo auditor	Tener alta capacidad de observación Elaboración de documentación del proceso de auditoría Obtener aprobación del cliente en todas las actividades Orientar esfuerzos para el logro de objetivos Competencias y conocimiento necesario para realizar una auditoría informática	Planificación de auditoría Ejecución de auditoría Comunicación de resultados Validación de auditoría Seguimiento de la auditoría

	Dar sugerencias y recomendaciones efectivas para la institución Mantener la independencia en apariencia y acción Centrarse en los hechos Atender las solicitudes del cliente	
Cliente	Revisión y aprobación documental Revisión y control de actividades Facilitar apoyo e información necesaria en el proceso de auditoría Entender el proceso y propósito de la auditoría Evaluar los recursos para realizar la auditoría	Planificación de auditoría Ejecución de auditoría Comunicación de resultados Validación de auditoría Seguimiento de la auditoría

3.5.3 Inventario del método

Para el inventario del método se ha identificado y definido el macroproceso, proceso, subproceso, procedimientos y actividades presentes en la auditoría. A continuación, en la Tabla 3.13 se muestra el inventario del método con la codificación del macroproceso, proceso y cada una de las actividades, correspondientes a la auditoría informática.

Tabla 3.13 Inventario del método

Inventario del método		
Macroproceso	**Proceso**	**Actividades**
Auditoría Operacional A. O	Auditoría informática A. O. 1	**Planificación (Fase I)**
		Establecer lugar y fecha de encuentro con el cliente A. O. 1. 1
		Registar reunión inicial con el cliente A. O. 1. 2
		Identificar las partes interesadas y responsables para la auditoría A. O. 1. 3

Comprender el contexto externo del entorno a auditar A. O. 1. 4
Comprender el contexto interno de la institución a auditar A. O. 1. 5
Comprender estrategias y prioridades de la institución A. O. 1. 6
Determinar objetivos de la auditoría en base al estudio del entorno A. O. 1. 7
Determinar el riesgo relevante del proceso de auditoría A. O. 1. 8
Definir los límites organizacionales de la auditoría A. O. 1. 9
Identificar miembros del equipo auditor A. O. 1. 10
Seleccionar miembros del equipo auditor A. O. 1. 11
Definir roles acordes a los conocimientos y habilidades de los miembros del equipo auditor A. O. 1. 12
Documentar plan preliminar A. O. 1. 13
Determinar antecedentes A. O. 1. 14
Determinar objetivos específicos de la auditoría A. O. 1. 15
Determinar el alcance de la auditoría A. O. 1. 16
Determinar recursos para la auditoría A. O. 1. 17
Determinar cronograma de la auditoría A. O. 1. 18
Determinar costos de la auditoría A. O. 1. 19
Documentar los riesgos de la auditoría A. O. 1. 20
Presentar plan preliminar al cliente A. O. 1. 21

Acordar términos y condiciones de la auditoría A. O. 1. 22
Elaborar la propuesta de auditoría A. O. 1. 23
Presentar la propuesta de la auditoría A. O. 1. 24
Determinar cláusulas del contrato A. O. 1. 25
Elaborar el contrato A. O. 1. 26
Firmar el contrato A. O. 1. 27
Ejecución (Fase II)
Diseñar y documentar el plan de trabajo A. O. 1. 28
Definir instrumentos para la investigación de campo A. O. 1. 29
Elaborar instrumentos de investigación de campo determinados en el plan de trabajo A. O. 1. 30
Aplicar técnicas e instrumentos de auditoría A. O. 1. 31
Análisis y síntesis de información recopilada A. O. 1. 32
Definir hallazgos en base a la información y evidencias recopiladas A. O. 1. 33
Elaborar informe final preliminar A. O. 1. 34
Comunicación de resultados (Fase III)
Agendar fecha para presentación y discusión del informe final preliminar A. O. 1. 35
Presentar informe final preliminar para discusión y validación A. O. 1. 36
Elaborar informe final A. O. 1. 37
Agendar fecha para presentación de informe final A. O. 1. 38
Presentar informe final y documentos resultantes de la auditoría A. O. 1. 39
Cerrar el contrato A. O. 1. 40

	Retirar garantías A. O. 1. 41
	Validación (Fase IV)
	Aplicar evaluación de calidad de resultados de auditoría A. O. 1. 42
	Aplicar evaluación de seguridad de la información en las IES A. O. 1. 43
	Aplicar evaluación de cumplimiento de actividades de la auditoría A. O. 1. 44
	Data Mining A. O. 1. 45
	Seguimiento (Fase V)
	Consulta directa al auditado A. O. 1. 46
	Verificación del informe final de auditoría A. O. 1. 47

3.5.4 Caracterización del método

La caracterización del método consiste en describir y detallar cada uno de los puntos descritos en el inventario del método, de tal forma que se pueda identificar las entradas y salidas de cada actividad, los recursos humanos y materiales utilizados, riesgos e indicadores y los controles de salida (Angulo, 2022). En el Anexo A se observan las especificaciones y caracterizaciones del proceso de auditoría de la información.

3.5.5 Ficha de indicadores

Los indicadores son requisitos de la norma ISO 9001 y permiten obtener información del desempeño del método a través de una evaluación al mismo. En este caso de determinaron tres indicadores que permiten verificar la eficacia y eficiencia del método, se evalúa la calidad de los resultados después de su ejecución, la seguridad de la información y el nivel de cumplimiento de todas las actividades señaladas. En el Anexo B se describe cada indicador, su objetivo, descripción y la fórmula.

3.5.6 Lista maestra de documentos

Para que el método de auditoría sea exitoso se debe contar con los documentos y registros, donde se almacena su funcionamiento y desarrollo. Dentro de la caracterización del proceso existe un apartado para mencionar todos los documentos y registros usados en el desarrollo del proceso (Angulo, 2022), en el Anexo C se describe la lista maestra de los documentos y registros identificados con su codificación, el tipo y el subproceso al que pertenece.

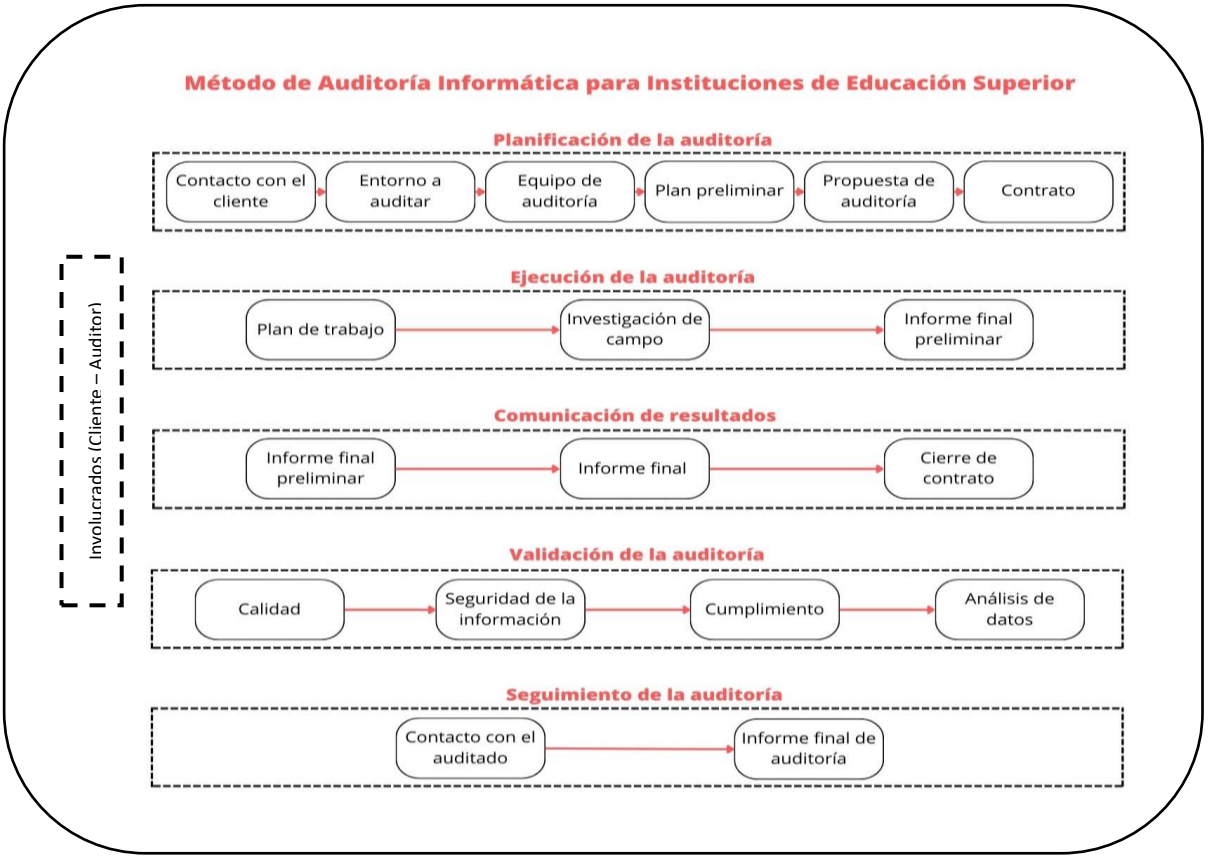
3.5.7 Manual del proceso

Es el documento que sirve de guía para ejecutar o implementar el método porque aquí se describen todos los pasos que se deben seguir para realizarlo de manera correcta. También se describen los participantes y responsables de desempeñar cada actividad. En el Anexo D se presenta el manual que contiene una portada, objetivo, responsables, glosario de términos, algunos conceptos, normas, la definición de las actividades y los documentos y registros resultantes.

3.6. Propuesta del MAIIES (Método de Auditoría Informática para Instituciones de Educación Superior)

Para la propuesta del método se consideran 5 fases del proceso de auditoría, cada una con un conjunto de pasos adaptados a las IES (ver figura 3.1).

Figura 3.1 Esquema MAIIES



3.6.1. Planificación de la Auditoría

La planificación es el primer paso para realizar una auditoría exitosa, empezando con la comprensión del auditor del ambiente y la organización en general, así como los procesos dentro del área tecnológica (Gutiérrez Garzón, 2003), es considerada como la fase fundamental en el proceso de auditoría, debido a que establece las actividades que serán desarrolladas durante su ejecución, además define los procesos, las técnicas y los temarios que se necesiten para continuar con la fase de ejecución. La importancia de esta fase es que se propone la estrategia general para producir los resultados esperados,

la escala y complejidad de la organización y el nivel de conocimiento y experiencia del auditor en la organización auditada (Bonilla Mariño, 2015).

Las actividades por cumplir se describen en la siguiente figura 3.2 y a continuación se describe a detalle cada una de ellas.

Figura 3.2 Esquema fase de planificación de la auditoría

Paso 1: Establecer lugar y fecha de encuentro con el cliente.

El primer paso para iniciar el proceso de auditoría es establecer el contacto con el cliente, se debe agendar un encuentro de mutuo acuerdo asignando el lugar y la fecha para conocer todos los aspectos relacionados con la auditoría que se va a desarrollar.

Paso 2: Registrar reunión inicial con el cliente.

El registro de cada reunión a partir de este paso se debe hacer a través de actas de reunión en donde se especifique: número de acta, quien va a dirigir la reunión, lugar y fecha, hora de inicio y fin, tema, actividades a tratar, revisiones, compromisos, pendientes, objetivos y participantes con sus firmas.

Paso 3: Identificar las partes interesadas y responsables para la auditoría.

En la reunión se debe identificar a autoridades y a los encargados del sistema, proceso o producto a auditar, quienes serán los encargados de rendir cuentas y proporcionar toda la información que se requiere para el proceso de auditoría.

Paso 4: Comprender el contexto externo del entorno a auditar.

Es importante considerar los factores externos que generalmente son los asuntos sobre los que las IES no tiene control y tienen impacto positivo o negativo sobre la institución. Entre los más importantes se tienen el entorno tecnológico, social, legal y económico.

Paso 5: Comprender el contexto interno de la institución a auditar.

Dentro de los factores internos que son los asuntos sobre los cuales las IES si tienen control se consideran: funciones sustantivas, políticas, desempeño del personal, infraestructura, tecnología con la que cuenta la institución, logística y cultura.

Es importante identificar y comprender a que función sustantiva va a estar enfocada la auditoría para el análisis documental y físico pertinente, además, se recomienda aplicar o solicitar la matriz FODA para identificar las fortalezas, debilidades (contexto interno), amenazas y oportunidades (contexto externo) que posee la institución.

Entender el contexto interno ayuda al auditor o equipo auditor a relacionar los objetivos de la institución con los de TI, esto facilita y mejora la definición del alcance de la auditoría.

Paso 6: Comprender estrategias y prioridades de la institución.

Para identificar las estrategias y prioridades se debe conocer los objetivos estratégicos de la institución y como los involucrados coordinan esfuerzos para alcanzarlos. Se debe consultar con la dirección o a través de la documentación disponible sobre la estrategia de la institución y prioridades a futuro, toda la información que se obtenga se debe documentar.

Paso 7: Determinar objetivos de la auditoría en base al estudio del entorno.

Partiendo del tipo de auditoría informática a realizar y teniendo en cuenta el estudio del entorno se debe establecer los objetivos de la auditoría, se pueden formular en términos de los objetivos genéricos de la empresa o pueden ser más específicos dependiendo de la auditoría que se va a realizar.

Paso 8: Determinar el riesgo relevante del proceso de auditoría.

Identificar el riesgo permite detectar o descubrir posibles errores durante el desarrollo de un programa de auditoría y tener mayor control en los procedimientos y actividades que pueden representar fuentes de riesgo durante la auditoría. Se debe identificar el riesgo inherente, riesgo de control y riesgo de detección.

Paso 9: Definir los límites organizacionales de la auditoría.

Se debe describir los límites organizacionales del proceso de auditoría, es decir, definir las entidades de la institución que se encuentran involucradas.

Paso 10: Identificar miembros del equipo auditor.

En base al estudio del entorno de la institución a auditar y conociendo el tema de la auditoría que se va a realizar se identifica cuántas personas y que conocimientos deben tener para el desarrollo de la auditoría.

Paso 11: Seleccionar miembros del equipo auditor.

Una vez identificados los requisitos para la selección del equipo auditor se procede al análisis de currículos vitae y la documentación de los posibles auditores y se escoge a los que se ajusten al proceso de auditoría a ejecutar.

Paso 12: Definir roles acordes a los conocimientos y habilidades de los miembros del equipo auditor.

Con el equipo auditor conformado se establece el rol de cada auditor y se comunica las funciones de cada uno en una reunión.

Paso 13: Documentar plan preliminar.

El plan preliminar es el documento que describe los antecedentes justificativos que permiten definir los objetivos de la auditoría, los recursos a emplear, tiempos, costos y un análisis de riesgos, sirve como propuesta para el cliente.

Paso 14: Determinar antecedentes.

Los antecedentes permiten identificar el grado de comprensión del tema de auditoría y de la institución a auditar, deben incluir conceptos y términos, datos

históricos que sean necesarios para entender el contexto y la necesidad de la auditoría.

Paso 15: Determinar objetivos específicos de la auditoría.

Teniendo en cuenta el objetivo general de la auditoría se debe describir las prioridades en objetivos concretos que dependen del tema real del proceso de auditoría.

Paso 16: Determinar el alcance de la auditoría.

El auditor o equipo auditor debe definir el alcance más adecuado para el compromiso de la auditoría, para ello se debe definir los principios, políticas, marcos de referencia, los procesos, servicios e infraestructura a evaluar, las estructuras organizacionales, los aspectos de comportamiento de la institución y personal, los elementos de información y el recurso humano.

Paso 17: Determinar recursos para la auditoría.

Identificar los recursos necesarios para el proceso de auditoría basado en el alcance y los riesgos determinados. Cuando se describan los recursos se deben considerar los financieros, técnicas de auditoría, procedimientos para lograr los objetivos, honorarios del equipo auditor, alcance del proceso, tiempos de movilización y hospedaje.

Paso 18: Determinar cronograma de la auditoría.

El cronograma permite organizar las actividades por hacer en el marco de tiempo establecido, de esta manera el equipo auditor trabaja bajo previa planificación.

Paso 19: Determinar costos de la auditoría.

El equipo de auditores debe identificar a través de un análisis económico todos los gastos del proceso de auditoría.

Paso 20: Documentar los riesgos de la auditoría.

Dentro del documento plan preliminar se debe documentar los riesgos identificados en el estudio del entorno.

Paso 21: Presentar plan preliminar al cliente.

Con la información documentada en el documento plan preliminar se debe agendar la reunión para presentar a los directivos o encargados de la institución el documento como propuesta para discusión. Si existen observaciones se analizan y se consideran para la documentación de la propuesta de auditoría.

Paso 22: Acordar términos y condiciones de la auditoría.

Después del análisis y revisión del plan preliminar se debe acordar con el cliente las cláusulas de los términos y condiciones para el desarrollo de la auditoría.

Paso 23: Elaborar la propuesta de auditoría.

Con las observaciones en el plan preliminar se procede a documentar la propuesta con los puntos establecidos del plan acatando los cambios acordados entre el equipo auditor y el cliente y que permita presentar una solución al requerimiento del cliente como base para la negociación y posterior contratación. El documento se debe elaborar la carta de presentación y definir antecedentes, justificación, alcance, objetivos, tiempos y precios, condiciones de ejecución, criterios de éxito y análisis de riesgos de la auditoría en base al estudio del entorno y observaciones del cliente.

Paso 24: Presentar la propuesta de la auditoría.

Con el documento propuesta de la auditoría se agenda una reunión y se acude al lugar y fecha acordado con el cliente para la presentación y aprobación de este documento por parte del cliente.

Paso 25: Determinar cláusulas del contrato.

Con el documento aprobado se determina que la ejecución de la auditoría puede empezar y se debe identificar las cláusulas a cumplir por parte del equipo auditor y el cliente.

Paso 26: Elaborar el contrato.

Los términos para el desarrollo de la auditoría se establecen en un contrato que debe ser firmado por las dos partes interesadas del proceso. El contrato

contiene encabezado, declaraciones, cláusulas: antecedentes, objeto, programa de trabajo, supervisión, coordinación de trabajos, horario de trabajo, personal asignado, relación laboral, plazo, honorarios, garantías y multas.

Paso 27: Firmar el contrato.

El contrato se revisa y queda constancia de la aprobación y compromiso de las partes con el documento firmado.

3.6.2 Ejecución de la Auditoría

Esta fase consiste en la selección y aplicación de las técnicas y herramientas más adecuadas para la auditoría (De Rey, 2020), se espera que a través de estos procedimientos se puedan obtener los elementos de juicio relevantes para detectar, confirmar o delimitar las posibles incidencias o consecuencias que se pueden presentar en la organización (Cubero, 2017). Además, se dedica directamente al trabajo de campo, se debe considerar que las pruebas se pueden realizar en cualquier momento, con el propósito de encontrar y proteger las evidencias correspondientes a las actividades realizadas en la organización.

Las actividades de esta fase se presentan en la figura 3.3:

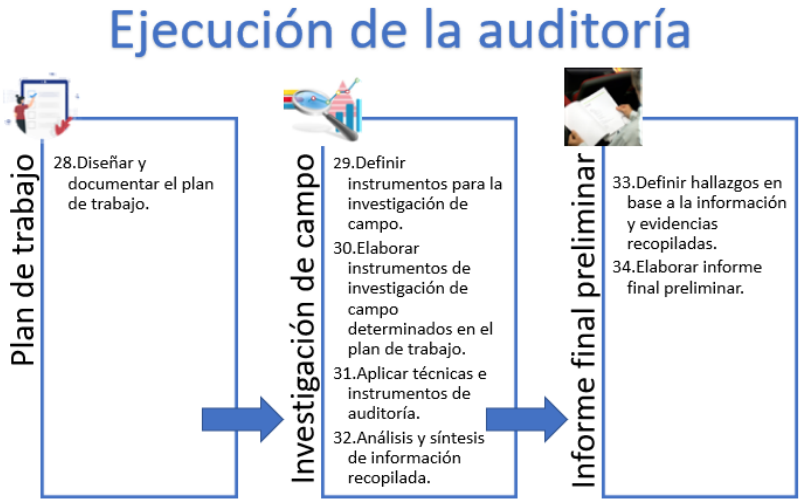


Figura 3.3 Esquema fase de ejecución

Paso 28: Diseñar y documentar el plan de trabajo.

Para iniciar con la fase de ejecución de la auditoría se elabora un documento en que se detalle el trabajo específico a realizar, las actividades de recolección

de la evidencia, las fuentes, los responsables, las fechas en las que se realizarán, su secuencia y resultados esperados.

Paso 29: Definir instrumentos para la investigación de campo.

El objetivo de la actividad es definir los instrumentos de ayuda para la investigación de campo en base de las técnicas de auditoría establecidas en el plan de trabajo.

Paso 30: Elaborar instrumentos de investigación de campo determinados en el plan de trabajo.

Elaborar los instrumentos de ayuda para la investigación de campo en base de las técnicas de auditoría establecidas en el plan de trabajo.

Entre las técnicas de recolección de información se tiene el muestreo, revisión documental, entrevista, encuesta, prueba sustantiva, simulación matemática o estadística, observación directa. Como herramientas para las técnicas de recolección se puede elegir el checklist, paquetes de auditoría, estándares, matrices de riesgo después de un análisis para la selección de la norma o metodología para el desarrollo de la auditoría. Las técnicas y herramientas elaboradas son revisadas y aprobadas por el equipo auditor.

Paso 31: Aplicar técnicas e instrumentos de auditoría.

Con las técnicas y herramientas elaboradas se procede a recolectar la evidencia de acuerdo con el plan de trabajo y cronograma establecido. Tomando en cuenta los principios deontológicos del auditor. Dentro de esta actividad se deben elaborar actas de reunión de las actividades ejecutadas, verificar la validez, idoneidad y pertinencia de la evidencia, verificar que la información esté completa, ordenar y clasificar toda la información recolectada.

Paso 32: Análisis y síntesis de información recopilada.

El análisis de la información obtenida debe ser bajo técnicas estadísticas, comparativas y correlacionales revisando que se cumpla lo establecido en los pasos anteriores. El éxito del análisis depende del estudio de los hechos y no de las opiniones, investigar las causas y no los efectos, atender razones y no excusas, no confiar en la memoria y documentar todo en tiempo real, objetividad en los informes y datos recabados.

Con el análisis de la información recolectada se debe comprender su significado y comparar con el criterio evaluador definido por la norma o estándar, determinar información faltante y completar la información para elaborar el informe.

Paso 33: Definir hallazgos en base a la información y evidencias recopiladas.

Al finalizar el análisis se elabora un borrador de los hallazgos identificados verificando que la evidencia recolectada esté completa y justifique los posibles hallazgos.

Paso 34: Elaborar informe final preliminar.

El informe final preliminar es el primer documento entregable en el que se describe el trabajo realizado para discutir concordar y validar los hallazgos y recomendaciones en base al borrador elaborado en el paso 34. El objetivo es identificar aspectos errados o incompletos para su pronta corrección.

El informe final preliminar contiene introducción, datos del equipo auditor, alcance, objetivos, metodología, técnicas y herramientas utilizados en la auditoría, cronograma, análisis de instrumentos de investigación de campo, hallazgos de la auditoría (en base a la norma, título, situación, criterio, causa y efecto), recomendaciones para cada hallazgo, actas de reunión y anexos (evidencias).

3.6.3 Comunicación de resultados

La fase de comunicación consiste en generar un informe de resultados también llamado informe de auditoría, que contiene las conclusiones y recomendaciones correspondientes a los problemas y deficiencias encontrados durante la ejecución de la auditoría (Cubero, 2017; Universidad Ecotec, 2019).

Esta fase comprende las actividades mostradas en la figura 3.4:

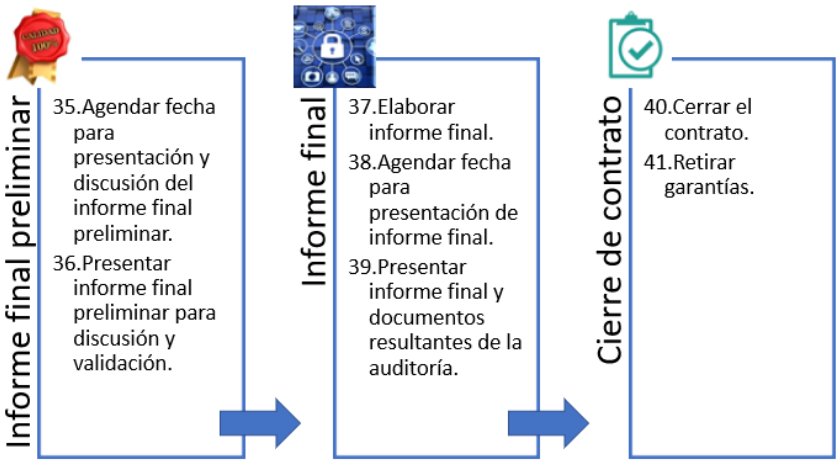


Figura 3.4 Esquema fase de comunicación de resultados

Paso 35: Agendar fecha para presentación y discusión de informe final preliminar.

En mutuo acuerdo con el cliente en este caso la IES auditada se debe acordar el lugar y fecha para la discusión del informe final preliminar.

Paso 36: Presentar el informe final preliminar para su discusión y validación.

Llegada la fecha agendada para la presentación del informe final preliminar se acude al lugar acordado y se hace la presentación de las partes del informe para discutir, acatar observaciones y aprobar para la elaboración del informe final de auditoría.

Paso 37: Elaborar informe final.

En este paso se debe elaborar un documento entregable en el que se reporta el trabajo realizado y los resultados de la auditoría, señalando especialmente los hallazgos y las recomendaciones justificadas.

El informe final contiene los enunciados del informe final preliminar con los cambios aprobados, aumentando la carta de compromiso, el organigrama de la empresa, las conclusiones y recomendaciones de los hallazgos y del proceso de auditoría en general. Además, se debe adjuntar todos los documentos anexos y evidencias dentro del informe.

Paso 38: Agendar fecha para presentación de informe final.

Se programa una reunión para la lectura y presentación del informe final.

Paso 39: Presentar informe final y documentos resultantes de la auditoría.

Se hace la presentación del informe final, resultados de la auditoría y se finaliza con la entrega los documentos objeto de la consultoría y el informe final revisado, firmado por el auditor y validado por los responsables de las áreas, funciones o temas auditados.

Paso 40: Cerrar el contrato.

Para finalizar el proceso de auditoría se elaboran las actas de entrega y se verifica el cumplimiento y conformidad del contrato para finalizar con el cierre.

Paso 41: Retirar garantías.

En el caso de existir garantías una vez finalizado el proceso y auditoría y el contrato se procede a retirarlas junto con el pago final.

3.6.4 Validación de la Auditoría

En la fase de validación se hace un examen del nivel de calidad y seguridad de los resultados obtenidos en el proceso de auditoría y que actividades del proceso se cumplieron y determinar el éxito y confiabilidad del proceso.

La fase contiene las actividades presentadas en la figura 3.5:

Figura 3.5 Esquema fase de validación

Paso 42: Aplicar evaluación de calidad de resultados de auditoría.

La calidad de una auditoría está directamente relacionada con el cumplimiento de un conjunto de características durante el proceso de una auditoría, por lo tanto, el método de evaluación está basado en 42 métricas calificadas en un rango del 1 al 10 y como resultado se tiene el porcentaje del nivel de calidad de los resultados del proceso ejecutado.

Paso 43: Aplicar evaluación de seguridad de la información en las IES.

Al ser la información un factor clave dentro de las instituciones, es importante conocer cómo se encuentran en términos de seguridad después de un proceso de auditoría, la evaluación se hace a través de 18 métricas relacionadas a los pilares de la seguridad: confidencialidad, disponibilidad e integridad.

Paso 44: Aplicar evaluación de cumplimiento de actividades de la auditoría.

La última actividad para la validación del proceso de auditoría es evaluar que actividades del MAIIES se han cumplido y cuales no para determinar si se han implementado correctamente e identificar formas potenciales de mejorar aquellas que han tenido inconvenientes, seguir todo el método asegura que el proceso se ha implementado correctamente. Los resultados pueden ser compartidos con el cliente para asegurar la confiabilidad y éxito del proceso de auditoría desarrollado.

Paso 45: Análisis de datos.

Con las métricas de validación determinadas en este estudio y aplicadas en los pasos 42, 43 y 44 se realiza una evaluación de cada una.

Se realiza un proceso de retroalimentación con cada métrica para identificar posibles mejoras en futuros procesos de auditoría informática y realizar las debidas recomendaciones.

Los valores de cada validación sirven para conocer el nivel de la auditoría informática realizada en niveles de calidad, seguridad y estandarización del proceso.

3.6.5 Seguimiento de la Auditoría

La fase de seguimiento de auditoría viene después de la emisión de un informe de auditoría y el equipo auditor debe tomar las medidas apropiadas para determinar qué acción se ha tomado para corregir los problemas revelados en el informe de auditoría y qué efecto pueden haber tenido tales acciones. El seguimiento de la auditoría tiene dos propósitos. Uno es fomentar una respuesta adecuada a los hallazgos de auditoría por parte del auditado o de otras entidades responsables. Y el otro propósito del seguimiento de la auditoría es sentar las bases para el trabajo de auditoría futuro. Si se cree que los problemas previamente revelados se han resuelto, el trabajo de auditoría posterior en esa área puede requerir solo pruebas mínimas para confirmar que el problema ya no persiste (Committee Contact of Heads of EU SAIs, 2004). Las actividades de esta fase se presentan en la figura 3.6:

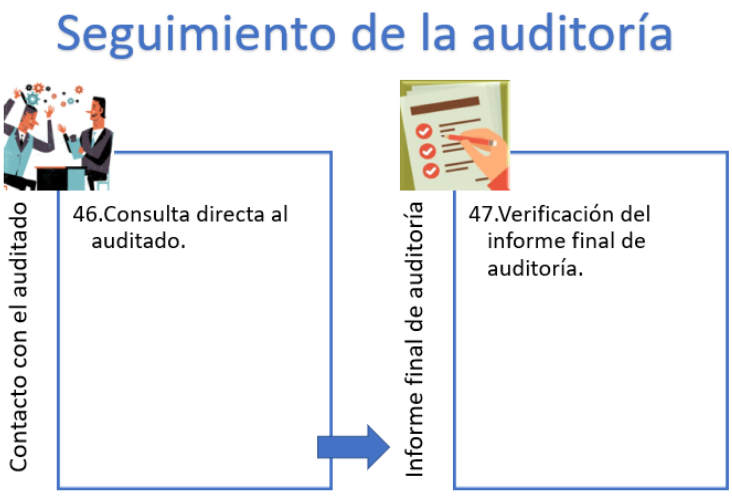


Figura 3.6 Esquema fase de seguimiento

Paso 46: Consulta directa al auditado.

El cliente debe conocer los resultados de la fase de validación del proceso de auditoría, para ello se agenda una reunión postauditoría para su entrega e inicio de la última fase en la que se planea identificar si las recomendaciones hechas en el informe final fueron consideradas para la mejora de la institución, al estar directamente con el cliente se investiga que acciones se realizaron y en el caso de no existir se consulta las razones.

Paso 47: Verificación del informe final de auditoría.

Con la reseña del cliente acerca de la toma de decisiones se evalúa que acciones se consideraron de acuerdo con las recomendaciones hechas en el informe final y así conocer si el problema revelado ha sido corregido. Si el problema no se ha superado se puede justificar un nuevo proceso de auditoría para confirmar la naturaleza y la importancia del problema, con el propósito de evocar una respuesta más apropiada del auditado.

4. CAPÍTULO IV

4.1. Métricas de calidad y seguridad

Para la fase de validación se realizó el análisis estadístico de las métricas obtenidas para la calidad y seguridad de la información en procesos de auditoría informática implementados en IES. La base de datos estuvo conformada por 54 observaciones de auditoría informática efectuadas en 54 IES del Ecuador. Las variables empleadas para la construcción del modelo de evaluación de auditoría fueron propuestas en el trabajo de (Imbaquingo et al., 2021, 2022; Stoel et al., 2012), por lo que el instrumento de evaluación contempló 91 variables de las cuales 8 fueron categóricas contemplando: el nombre de la institución, la zona donde se ubica, el nivel de estudios que se oferta, la conformidad con la realización de auditorías, la percepción de importancia de realización de auditorías, si se han realizado auditorías previas, la clase de auditoría realizada previamente, y el tipo de auditoría. Además, se incluyeron 83 variables en escala ordinal de diez niveles donde se puntuó cada una de las variables propuestas en (Imbaquingo et al., 2022), con el objetivo de medir la dimensión calidad conformada por los factores: factor humano, factor técnico y factor contextual; y la dimensión seguridad de la información, conformada por los factores: confidencialidad, integridad y disponibilidad basadas en la Norma ISO 27000. La distribución de variables para cada uno de los factores se presenta en las Tablas 4.1 y 4.2.

Tabla 0.1 Variables y factores propuestas para la evaluación de la dimensión Calidad

	Factor humano
$p1$	El equipo auditor procuró que el cliente participe en todo el proceso de auditoría
$p2$	El equipo auditor obtuvo la conformidad del cliente acerca de las actividades desarrolladas
$p4$	El personal que realiza la auditoría tenía competencias necesarias para realizar su trabajo
$p5$	El auditor contaba con habilidades blandas (características y competencias personales que demuestran como el auditor se desenvuelve con los demás)
$p6$	El personal que realizó la auditoría brindó sugerencias efectivas a la Institución
$p7$	El auditor tenía mente abierta al recibir nuevas ideas
$p8$	El auditor estaba seguro de sí mismo y de su trabajo

$p9$	El equipo auditor conservó su independencia en apariencia y acción
$p10$	El equipo auditor se centró en los hechos
$p11$	El equipo auditor recibió apoyo para lograr las metas
$p12$	El equipo auditor demostró esfuerzo al realizar la auditoría
$p13$	El auditor se preocupaba por su formación y actualización continua
$p14$	El auditor contaba con certificaciones nacionales e internacionales en el área de auditoría y auditoría informática
$p15$	Los miembros del equipo auditor demostraron conocimiento en seguridad de la información y procesamiento de datos
$p16$	Las diferencias con el cliente fueron tratadas de forma oportuna, profesional y objetiva
$p17$	El equipo auditor estuvo disponible para atender las solicitudes del cliente
$p18$	Los involucrados en la auditoría tuvieron una comunicación frecuente
$p19$	El auditor vinculó expertos como apoyo en el proceso de auditoría para obtener resultados y recomendaciones para el cliente
$p20$	El auditor siguió políticas y procedimientos que reglamentan su cumplimiento ético y profesional
	Factor técnico
$p21$	El equipo auditor usó plantillas y formularios para documentar
$p22$	Los hallazgos y conclusiones de la auditoría fueron un reflejo exacto de los hechos reales del proceso auditado
$p23$	Los resultados de la auditoría fueron respaldados y documentados con las evidencias recopiladas al auditar
$p24$	Los miembros del equipo auditor y responsables de la institución aseguraron en todo momento la información
$p25$	Los hallazgos, conclusiones y recomendaciones fueron receptados positivamente por el cliente
$p26$	Los recursos para la auditoría fueron asignados de acuerdo con la importancia y complejidad de la auditoría
$p27$	El sistema, proceso u objeto auditado tenía importancia para la organización
$p28$	En el alcance se abordaron todos los elementos necesarios para auditar exitosamente
$p29$	La ejecución de la auditoría cumplió con los elementos acordados en el alcance
$p30$	Los resultados se entregaron en el momento adecuado y establecido
$p31$	El modelo de evaluación de riesgos fue comprensible
$p32$	El plan de auditoría tomó en cuenta los riesgos relacionados con el cliente
$p33$	El proceso de auditoría se desarrolló con exactitud y precisión
$p34$	El informe de auditoría fue claro y conciso con sus resultados
$p35$	El alcance, hallazgos y recomendaciones han sido entendibles para cualquier persona que usó el informe de auditoría
$p36$	La auditoría se ejecutó bajo las políticas, estándares, manuales, directrices y prácticas de auditoría informática
$p37$	Las listas de verificación estuvieron completas, aprobadas y documentadas
$p38$	El trabajo de campo fue revisado por un experto
$p39$	El cliente o responsables de la organización auditada brindaron apoyo

	para la recopilación de la información
$p40$	La información y resultados de anteriores auditorías estuvieron disponibles para revisión
$p41$	Los objetivos y el alcance de la auditoría fueron especificados adecuadamente
$p42$	Las actividades y herramientas para la auditoría fueron descritas claramente
$p43$	Los miembros del equipo auditor tenían una comprensión clara y coherente del plan de auditoría
$p44$	El presupuesto y cronograma de auditoría se establecieron de manera adecuada
$p45$	Se evaluaron los requisitos de personal y equipos asignados para la auditoría
$p46$	El plan de auditoría fue elaborado, revisado y aprobado por los supervisores, responsables de la organización y miembros del equipo auditor
$p47$	El equipo auditor utilizó una metodología de auditoría informática para planificar, gestionar y desarrollar la auditoría
$p48$	El equipo auditor usó herramientas tecnológicas y nuevas metodologías para realizar su trabajo
	Factor contextual
$p49$	El auditor promovió a través de sus informes una cultura organizacional basada en buenas prácticas de seguridad informática
$p50$	El equipo auditor tenía estrictos procedimientos de control de calidad
$p51$	El líder del equipo auditor estuvo comprometido con el sistema de control de calidad
$p52$	La normativa y regulaciones emitidas por organismos de control fueron reflejadas en el plan de auditoría
$p53$	El equipo auditor conocía la información relevante de leyes y regulaciones que pueden tener un impacto significativo en los objetivos de la auditoría
$p54$	Se aplicaron medidas disciplinarias en caso de incumplir con el plan de auditoría o la normativa legal regulatoria vigente
$p55$	El costo de la auditoría estuvo de acuerdo con la complejidad y las actividades desarrolladas

Tabla 0.2 Variables y factores propuestas para la evaluación de la dimensión Seguridad de la Información

	Factor Confidencialidad
$p56$	Se aplican políticas para la seguridad de la información dentro de la institución
$p57$	Las políticas y procedimientos en seguridad de la información dentro de la institución se actualizan periódicamente
$p58$	Las responsabilidades en la seguridad de la información son delegadas, documentadas y entregadas formalmente a todo el personal de la institución, según su cargo
$p59$	Se aplican políticas y acciones de seguridad de la información sensible de la institución
$p60$	Se actualiza y aplica las políticas de acceso a la información en base a los roles de usuario existentes
$p61$	Se dispone de una acreditación en seguridad de la información para

	todos sus sistemas informáticos
$p62$	Se aplican procedimientos documentados para seguir en caso de incidentes de seguridad
$p63$	Se realizan auditorías de cumplimiento de seguridad de la información
$p64$	Se aplican políticas de gestión de contraseñas para los usuarios finales de la institución
$p65$	Se identifican a los usuarios que acceden a la red y las acciones que ejecutan
	Factor integridad
$p66$	Se aplica un control de acceso a la infraestructura y servicios de TI de la institución
$p67$	Se capacita e involucra a usuarios, colaboradores y personal en los temas de seguridad de la información
$p68$	Se realiza análisis de vulnerabilidades de los servicios web de la institución
$p69$	Se aplican planes de monitoreo y gestión de impacto de incidentes de seguridad en la institución
$p70$	Se actualiza y documenta el inventario de todos los activos de TI
	Factor disponibilidad
$p71$	Se dispone de aplicaciones para proteger de software malicioso a todas sus soluciones informáticas
$p72$	Se realizan copias de seguridad de la información
$p73$	Se monitorean las actividades desarrolladas por los usuarios

Con los resultados del análisis estadístico se obtienen los instrumentos de evaluación para la fase de validación de la auditoría compuesto por un conjunto de 42 métricas para medir el nivel de calidad y 18 métricas para el nivel de seguridad de los resultados de auditoría. Cada una de las métricas ubicadas en el factor correspondiente, lo que permite identificar las fortalezas y debilidades de los procesos de auditoría implementados y a examinar qué tan cerca se relacionan las métricas con los bajos niveles de calidad y seguridad de resultados de auditorías anteriores.

Mediante los puntajes ponderados obtenidos se analiza el nivel de correlación entre cada factor obteniendo las siguientes correlaciones significantes: Al analizar los factores: humano y técnico, se evidenció una correlación directa muy alta alcanzando un coeficiente ρ de Spearman de 0.93, lo que implica que a mayor puntaje del factor humano se obtendrá un mayor puntaje en el factor técnico; humano y contextual, se evidenció una correlación directa muy alta alcanzando un coeficiente ρ de Spearman de 0.85, lo que implica que a mayor puntaje del factor humano se obtendrá un mayor puntaje en el factor contextual; técnico y contextual, se evidenció una correlación directa muy alta alcanzando

un coeficiente ρ de Spearman de 0.90, lo que implica que a mayor puntaje del factor técnico se obtendrá un mayor puntaje en el factor contextual; contextual y confidencialidad, se evidenció una correlación directa alta alcanzando un coeficiente ρ de Spearman de 0.46, lo que implica que a mayor puntaje del factor contextual se obtendrá un mayor puntaje en el factor confidencialidad; confidencialidad e integridad, se evidenció una correlación directa muy alta alcanzando un coeficiente ρ de Spearman de 0.74, lo que implica que a mayor puntaje del factor confidencialidad se obtendrá un mayor puntaje en el factor integridad. Además, se pudieron evidenciar correlaciones moderadas en la comparación de las parejas restantes, lo que implica que el instrumento fue construido de manera apropiada, ya que, la relación entre factores refleja un comportamiento similar.

4.2. Aplicación del MAIIES

El MAIIES fue aplicado como una evaluación al Esquema Gubernamental de Seguridad de la Información de la Universidad de las Fuerzas Armadas ESPE, utilizando como referencia la Norma NTE INEN-ISO/IEC 27003, en base a las cinco fases del método propuesto y las fases del proceso de planificación e implementación de un EGSI.

En este contexto, se puede apreciar que las fases del trabajo realizado fueron aplicadas como un examen con niveles apropiados de pruebas de auditoría y las conclusiones obtenidas se justifican con suficiente evidencia válida y relevante, lo que permite obtener hallazgos importantes que son de apoyo a la dirección de TI de la institución.

La fase de validación nos permite obtener el nivel de calidad, seguridad y cumpliento de actividades después de realizar el ejercicio de auditoría, los resultados son los siguientes:

Nivel de calidad: 97%

Nivel de seguridad: 93%

Nivel de cumplimiento: 87%

En base a los datos generados se puede evidenciar que los resultados del ejercicio de auditoría fueron exitosos y se logró identificar las debilidades y fallos para dar las recomendaciones que apoyen a la toma de decisiones y la mejora continua del proceso dentro de la Unidad de Seguridad. A medida que

una universidad alcanza los objetivos genéricos y específicos, aumenta su nivel madurez y al mismo tiempo logra el cumplimiento de las reglamentaciones y leyes nacionales pertinentes.

CONCLUSIONES

La calidad de la auditoría considera tres factores principales: factor humano, factor técnico y factor contextual o del entorno, cada uno con un grupo de métricas asociadas a auditores bien capacitados y motivados puedan diseñar un buen proceso que entienda los factores contextuales y estén totalmente sintonizados con las condiciones únicas de cada auditoría. La identificación de factores y métricas de calidad de auditoría informática orienta a los departamentos de tecnologías de las IES sobre los aspectos relevantes de evaluación, control y gestión, para que futuras auditorías obtengan resultados de alta calidad, que asegura la confiabilidad y eficiencia del proceso.

La identificación de los pilares y métricas que inciden en la seguridad de la información brinda una guía para la prevención, control y gestión de vulnerabilidades y riesgos que afectan la seguridad de los activos informáticos de las organizaciones y sus usuarios, de manera que la implementación de medidas y la toma de decisiones en el futuro tengan resultados confiables para mantener una seguridad efectiva dentro de la institución. Los pilares de seguridad y sus métricas pueden ser utilizados para identificar y evaluar la seguridad dentro de diferentes instituciones que almacenan grandes cantidades de datos, además son de gran importancia en la identificación de vulnerabilidades para un adecuado seguimiento de auditoría y evaluación de riesgos.

Con la revisión de la literatura y los datos proporcionados por CEDIA, se concluye que son pocas las IES que cuentan con procesos de auditorías realizadas, que a su vez no siguen un proceso estándar para procesos institucionales y que controle procesos institucionales. Los auditores a cargo de realizar las auditorías utilizaron métodos empíricos y no especializados. Entre los marcos referenciales que se consideraron para la propuesta de estandarización del MAIIES se obtuvo una visión general de las actividades que se deben incluir en el método, considerando involucrados, fases, documentación, normativa legal interna y externa, recursos y los indicadores de evaluación.

Un ejercicio de auditoría debe asegurar en todo momento la calidad y la seguridad de los resultados obtenidos, considerando todos los aspectos en cada una de las fases y sus actividades, con el fin de evitar los problemas de subjetividad, informes no calificados, falta de credibilidad en las instituciones, pérdida o alteración de la información, accesos no autorizados y fallos técnicos que se presentan con los bajos niveles de estos indicadores.

El MAIIES considera una comparación y análisis de marcos referenciales de auditoría informática de organismos internacionales reconocidos a nivel mundial con vigencia y cumplimiento de la estructura general de una auditoría informática, uso e implementación frecuente en procesos de auditoría, usado por expertos en auditoría informática y que sus actividades se adapten a los procesos de las IES. La creación del MAIIES involucra las fases y las actividades resultantes de la identificación y análisis de cada marco para ser usadas como base en la propuesta del método, teniendo como resultado una propuesta completa y enfocada en funciones sustantivas de la educación superior.

RECOMENDACIONES

Todos los involucrados en el proceso de la auditoría informática deben conocer y garantizar que el trabajo realizado sea de calidad para que la revisión y validación de los resultados obtenidos en el ejercicio de control cuenten con los criterios de pertinencia, oportunidad y suficiencia, agreguen valor a la Institución y provean información objetiva, verificada e independiente para la toma de decisiones en las áreas, procesos y actividades relacionadas con el objeto auditado. Se recomienda la implementación de auditorías informáticas en las que se consideren los factores que influyen en la calidad y seguridad con el fin de garantizar que el proceso sea ejecutado bajo métricas e indicadores que aseguren la confiabilidad en los resultados obtenidos al auditar.

Se recomienda conocer y garantizar que los procedimientos y actividades a seguir brinden resultados óptimos y eficientes en la toma de decisiones para salvaguardar la información crítica de la Institución y sus usuarios, por lo que se recomienda la implementación de estándares de seguridad informática con el fin de garantizar la seguridad de la información bajo los pilares que aseguran la confidencialidad, integridad, disponibilidad, autenticidad y trazabilidad con sus métricas.

Se recomienda utilizar la propuesta del MAIIES porque contiene lo más relevante de cada marco referencial analizado, lo que asegura un método de auditoría informática estandarizado y actualizado que permitirá evaluar aspectos y condiciones de la actualidad que no se encuentren contemplados en metodologías anteriores. La propuesta de estandarización si bien se encuentra enfocada para las IES de Ecuador, esta puede ser utilizada para auditar IES internacionales ajustando a sus requerimientos.

Se recomienda asegurar la calidad y la seguridad de los resultados obtenidos en el ejercicio de la auditoría para asegurar que la información sea eficiente, veraz y segura, proporcionando todos los datos necesarios para el manejo de reportes y el proceso de toma de decisiones dentro de una IES y así fortalecer sus procesos y actividades.

Se recomienda seguir el MAIIES en sus cinco fases con el objetivo de asegurar una mayor calidad y seguridad de la información con los lineamientos y controles proporcionados por marcos referenciales internacionales, debido a que incluye una evaluación en base a indicadores de calidad, seguridad y cumplimiento postauditoría, además se considera el seguimiento para fomentar una respuesta adecuada a los hallazgos identificados en la auditoría y para sentar las bases para futuros trabajos de auditoría.

TRABAJO FUTURO

Como trabajo futuro se plantea la implementación del método en Instituciones de Educación Superior, siendo una propuesta de evaluación para el Consejo de Aseguramiento de la Calidad de la Educación Superior (CACES), que es el organismo público que tiene a su cargo la regulación, planificación y coordinación del sistema de aseguramiento de la calidad de la educación superior.

REFERENCIAS

Acosta, X. (2015). *Desarrollo de un modelo de seguridad para la prevención de pérdida de datos DLP, en empresas PYMES*. UDLA.

Ahmed, M., & Pathan, A.-S. K. (2020). False data injection attack (FDIA): an overview and new metrics for fair evaluation of its countermeasure. *Complex Adaptive Systems Modeling*, *8*(1), 4. https://doi.org/10.1186/s40294-020-00070-w

Al-Karaki, J. N., Gawanmeh, A., & El-Yassami, S. (2020). GoSafe: On the practical characterization of the overall security posture of an organization information system using smart auditing and ranking. *Journal of King Saud University - Computer and Information Sciences*. https://doi.org/10.1016/j.jksuci.2020.09.011

Alcaraz Velasco, F., Palomares, J. M., & Olivares, J. (2021). Lightweight method of shuffling overlapped data-blocks for data integrity and security in WSNs. *Computer Networks*, *199*, 108470. https://doi.org/10.1016/j.comnet.2021.108470

Almuiñas, J., & Galarza, J. (2015). La gestión de la información y el conocimiento: Una oportunidad para las instituciones de educación superior. *Revista Universidad y Sociedad*, *7*(2), 16–22. http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S2218-36202015000200003

Altamirano, M. (2019). Modelo para la gestión de la seguridad de la información y los riesgos asociados a su uso. *Avances*, *21*(2), 248–263.

Álvarez Betancourth, N. (2016). Manual de Procesos y Procedimientos de Auditoría Interna. *Auditora Interna SE*, 18.

Alvarez, M. (2018). La auditoría: concepto, clases y evolución. *Conceptos Juridicos Fundamentales*, 1–14. https://www.mheducation.es/bcv/guide/capitulo/8448178971.pdf

Álvarez, M. (2008). La auditoría: concepto, clases y evolución. *Conceptos Juridicos Fundamentales*, 1–14. https://www.mheducation.es/bcv/guide/capitulo/8448178971.pdf

Álvarez, N. (2016). Manual de Procesos y Procedimientos de Auditoría Interna. *Auditora Interna SE*, 18.

Andersson, J., Grassi, V., Mirandola, R., & Perez-Palacin, D. (2021). A conceptual framework for resilience: fundamental definitions, strategies and metrics. *Computing*, *103*(4), 559–588. https://doi.org/10.1007/s00607-020-00874-x

Angulo, B. (2022). *DISEÑO DE UN SISTEMA DE GESTIÓN POR PROCESOS BASADO EN LA NORMA ISO 9001:2015 PARA LA MICROEMPRESA TEXTIL BRAPIN UBICADA EN LA PROVINCIA DE IMBABURA* [Universidad Técnica del Norte]. http://repositorio.utn.edu.ec/bitstream/123456789/12003/2/04 IND 331 TRABAJO GRADO.pdf

Arcentales, D., & Caycedo, X. (2017). Auditoría informática: un enfoque efectivo. *Dominio de Las Ciencias*, *3*(3), 157–173. https://doi.org/10.23857/dom.cien.pocaip.2017.3.mono1.ago.157-173

Arcentales Fernández, D., & Caycedo Casas, X. (2017). Auditoría informática: un enfoque efectivo. *Dominio de Las Ciencias*, *3*(3), 157–173. https://doi.org/10.23857/dom.cien.pocaip.2017.3.mono1.ago.157-173

Baldi, M., Maturo, N., Ricciutelli, G., & Chiaraluce, F. (2019). Physical layer security over fading wiretap channels through classic coded transmissions with finite block length and discrete modulation. *Physical Communication*, *37*, 100829. https://doi.org/10.1016/j.phycom.2019.100829

Behal, S., & Kumar, K. (2017). Detection of DDoS attacks and flash events using information theory metrics–An empirical investigation. *Computer Communications*, *103*, 18–28. https://doi.org/10.1016/j.comcom.2017.02.003

Behal, S., Kumar, K., & Sachdeva, M. (2021). D-FAC: A novel ϕ-Divergence based distributed DDoS defense system. *Journal of King Saud University - Computer and Information Sciences*, *33*(3), 291–303. https://doi.org/10.1016/j.jksuci.2018.03.005

Blanco, L. (2008). *Auditoría y Sistemas Informáticos*. Félix Varela. https://elibro.net/es/ereader/utnorte/71229?page=14

Blázquez, J. (2018). *La aplicación del Big Data y el Data Analytics en auditoría*. Auren. https://auren.com/es/blog/la-aplicacion-del-big-data-y-el-data-analytics-en-auditoria/#:~:text=En primer lugar%2C con la,resultado de la prueba realizada.

Bonilla Mariño, M. F. (2015). AUDITORÍA DE SISTEMAS INFORMÁTICOS, DE LA COMPAÑÍA HIDALGO BRONCANO CÍA. LTDA., UBICADA EN LA CIUDAD DE RIOBAMBA, PROVINCIA DE CHIMBORAZO, DURANTE EL AÑO 2012. *Escuela de Contabilida y Auditoría*, *31*(sup3.2). https://doi.org/10.7705/biomedica.v31i0.530

Breda, G., & Kiss, M. (2020). Overview of information security standards in the field of special protected industry 4.0 areas & industrial security. *Procedia Manufacturing*, *46*, 580–590. https://doi.org/10.1016/j.promfg.2020.03.084

Brown, H., Issa, H., & Lombardi, D. (2015). Behavioral implications of big data's impact on audit judgment and decision making and future research directions. *Accounting Horizons*, *29*(2), 451–468. https://doi.org/10.2308/acch-51023

Buenaño, L., & García, G. (2013). *Auditoría Informática en la Facultad de Administración de Empresas, Escuela Superior Politécnica de Chimborazo, para mejorar los sistemas de gestión de tecnologías de la información y comunicación*. https://doi.org/10.7705/biomedica.v31i0.530

Cadena, S., Córdova, J., Enríquez, R., Llorens, F., & Padilla, R. (2018). *Estado de las Tecnologías de la Información y la Comunicación en las Universidades Ecuatorianas*. CEDIA. https://www.cedia.edu.ec/dmdocuments/publicaciones/Libros/UETIC_2018.pdf

Cadena, S., Córdova, J., Enríquez, R., & Padilla, R. (2019). *Estado de las Tecnologías de la Información y la Comunicación en las Universidades Ecuatorianas*. CEDIA. https://www.cedia.edu.ec/dmdocuments/publicaciones/Libros/UETIC_2019.pdf

Caiza, A. (2017, December 7). *AUDITORÍA DE CALIDAD: PARTICIPANTES EN LA AUDITORIA DE CALIDAD, TIPOS DE AUDITORÍA*. ClubEnsayos. https://www.clubensayos.com/Negocios/AUDITORÍA-DE-CALIDAD-PARTICIPANTES-EN-LA-AUDITORIA-DE/4232069.html

Cajas, F., & Luje, A. (2019). *Evaluación de metodologías de Auditoría Informática basado en su riesgo inherente* [Universidad de las Fuerzas Armadas ESPE]. http://repositorio.espe.edu.ec/jspui/handle/21000/22149

Campos, J., Narváez, C., Erázo, J., & Ordoñez, Y. (2019). Aplicación del sistema COBIT en los procesos de auditoría informática para las cooperativas de ahorro y crédito del segmento 5. *Visionario Digital*, *3*(2.1.), 445–475. https://doi.org/10.33262/visionariodigital.v3i2.1..584

Castello, R. (2006). *Auditoría en entornos informáticos*. Creative Commons. https://econ.unicen.edu.ar/monitorit/index.php?option=com_docman&task=doc_download&gid=552&Item%0Aid=19

Cheng, J., Goto, Y., Morimoto, & Horie, D. (2008). A security engineering environment based on ISO/IEC standards: Providing standard, formal, and consistent supports for design, development, operation, and maintenance of secure information systems. *Proceedings of the 2nd International Conference on Information Security and Assurance*, 350–354. https://doi.org/10.1109/ISA.2008.106.

Cho, C.-S., Chung, W.-H., & Kuo, S.-Y. (2016). Cyberphysical Security and Dependability Analysis of Digital Control Systems in Nuclear Power Plants. *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, *46*(3), 356–369. https://doi.org/10.1109/TSMC.2015.2452897

Cienfuegos, S., Gómez, N., & Millas, Y. (2021). *Guía para la realización de las auditorías internas de los sistemas de gestión* (AENOR Inte). https://www.marcialpons.es/media/pdf/9788417891343_extracto.pdf

Committee Contact of Heads of EU SAIs. (2004). *Guidelines on Audit Quality*. 57. https://www.eurosai.org/handle404?exporturi=/export/sites/eurosai/.content/documents/materials/Guidelines-on-Audit-Quality-ECA.pdf

Cubero, T. (2017). *Manual de auditoría de gestión Enfoque empresarial y de riesgos*.

de la Rosa, M. (2021). *Automation of an information security management system based on the ISO / IEC 27001 Standard*.

De Rey, A. M. (2020). *Auditoría de Estado*.

Deng, D., Li, X., Fan, L., Zhou, W., Qingyang Hu, R., & Zhou, Z. (2017). Secrecy Analysis of Multiuser Untrusted Amplify-and-Forward Relay Networks. *Wireless Communications and Mobile Computing*, *2017*, 1–11. https://doi.org/10.1155/2017/9580639

Dhanaraj, R. K., Ramakrishnan, V., Poongodi, M., Krishnasamy, L., Hamdi, M., Kotecha, K., & Vijayakumar, V. (2021). Random Forest Bagging and X-Means Clustered Antipattern Detection from SQL Query Log for Accessing Secure Mobile Data. *Wireless Communications and Mobile Computing*, *2021*, 1–9. https://doi.org/10.1155/2021/2730246

Dickins, D., Johnson-Snyder, A. J., & Reisch, J. T. (2018). Selecting an auditor

for Bradco using indicators of audit quality. *Journal of Accounting Education*, *45*, 32–44. https://doi.org/10.1016/j.jaccedu.2018.07.001

Diesch, R., Pfaff, M., & Krcmar, H. (2020). A comprehensive model of information security factors for decision-makers. *Computers & Security*, *92*. https://doi.org/doi.org/10.1016/J.COSE.2020.101747

Domingo-Ferrer, J., Muralidhar, K., & Bras-Amoros, M. (2020). General Confidentiality and Utility Metrics for Privacy-Preserving Data Publishing Based on the Permutation Model. *IEEE Transactions on Dependable and Secure Computing*, 1–1. https://doi.org/10.1109/TDSC.2020.2968027

Enoch, S. Y., Huang, Z., Moon, C. Y., Lee, D., Ahn, M. K., & Kim, D. S. (2020). HARMer: Cyber-Attacks Automation and Evaluation. *IEEE Access*, *8*, 129397–129414. https://doi.org/10.1109/ACCESS.2020.3009748

Eom, T., Hong, J. B., An, S., Park, J. S., & Kim, D. S. (2019). A Systematic Approach to Threat Modeling and Security Analysis for Software Defined Networking. *IEEE Access*, *7*, 137432–137445. https://doi.org/10.1109/ACCESS.2019.2940039

Escobar, J. (2021). *Desarrollo de un sistema web para fortalecer el proceso de auditoría y seguridad informática en Instituciones de Educación Superior* [Universidad Técnica del Norte]. http://repositorio.utn.edu.ec/handle/123456789/11368

Fabre, C. (2005). Las Funciones Sustantivas de la Universidad y su articulación en un Departamento Docente. *CIVE 2005 Congreso Internacional Virtual de Educación*. www.cibereduca.com

Fal', A. M. (2010). Standardization in information security management. *Cybernetics and Systems Analysis*, *46*(3), 512–515. https://doi.org/10.1007/s10559-010-9227-9

Fal', O. M. (2017). Standardization in Information Technology Security. *Cybernetics and Systems Analysis*, *53*(1), 78–82. https://doi.org/10.1007/s10559-017-9908-8

Falco, G., Caldera, C., & Shrobe, H. (2018). IIoT Cybersecurity Risk Modeling for SCADA Systems. *IEEE Internet of Things Journal*, *5*(6), 4486–4495. https://doi.org/10.1109/JIOT.2018.2822842

Fang, Y., Jian, Z., Jin, Z., Xie, X., Lu, Y., & Li, T. (2021). Fast Policy Interpretation and Dynamic Conflict Resolution for Blockchain-Based IoT System. *Wireless Communications and Mobile Computing*, *2021*, 1–14. https://doi.org/10.1155/2021/9968743

Florentino, A. C. B., Barbalho, S. C. M., & Machado, R. C. S. (2021). Proposal and Validation of a Standard Protection Profile for Homologation of Commercial Videoconferencing Equipment. *IEEE Access*, *9*, 24288–24304. https://doi.org/10.1109/ACCESS.2021.3056491

Francis, J. R. (2004). What do we know about audit quality? *British Accounting Review*, *36*(4), 345–368. https://doi.org/10.1016/j.bar.2004.09.003

Freire, V. (2016). *Implementacion de una Auditoria Informatica al Sistema de Matriculacion de Estudiantes (SAIS) de la Universidad Agraria del Ecuador* [Universidad Agraria del Ecuador]. http://www.dspace.espol.edu.ec/xmlui/handle/123456789/39369

García, R., & Fernández, M. (2020). Percepción sobre la integración de las funciones sustantivas en la Universidad Católica de Cuenca. *Varona. Revista Científico Metodológica*, *70*. http://scielo.sld.cu/scielo.php?script=sci_arttext&pid=S1992-82382020000100042

Gebremichael, T., Ledwaba, L., Eldefrawy, M., Hancke, G., Pereira, N., Gidlund, M., & Akerberg, J. (2020). Security and Privacy in the Industrial Internet of Things: Current Standards and Future Challenges. *IEEE Access*, 152351–152366. https://doi.org/10.1109/ACCESS.2020.3016937

Gepp, A., Linnenluecke, K., O'Neill, J., & Smith, T. (2018). Big data techniques in auditing research and practice: Current trends and future opportunities. *Journal of Accounting Literature*, *40*(1), 102–115. https://doi.org/10.1016/j.acclit.2017.05.003

Gómez, A. (2022, February 3). *Matriz de partes interesadas según ISO 9001*. Asesor de Calidad. http://asesordecalidad.blogspot.com/2019/01/matriz-de-partes-interesadas-segun-iso.html#.YftmSOrMLIU

Gómez Enciso, E., & Porras Flores, E. E. (2018). Modelo de evaluación de seguridad para transmitir datos usando Web Services. *Industrial Data*, *21*(1), 123. https://doi.org/10.15381/idata.v21i1.14927

González, M., & Ponjuán, G. (2014). Metodologías y modelos para auditar la información: Análisis reflexivo. *Revista General de Informacion y Documentacion*, *24*(2), 233–253. https://doi.org/10.5209/rev_RGID.2014.v24.n2.47402

GTAG. (2012). Information Technology Risk and Controls. *Global Technology Audit Guide*, *2nd editio*, 36. http://www.theiia.org/bookstore/downloads/freetomembers/0_1006.dl_gtag 1 2nded.pdf

Guamán, V. (2019). *EVALUACIÓN DE SEGURIDAD DE LA INFORMACIÓN APLICADO AL SISTEMA DE EVALUACIÓN DE DOCENTES DE LA UNIVERSIDAD TÉCNICA DEL NORTE BASADO EN LA ISO 27002:2017 CON LA METODOLOGÍA MAGERIT V3* [Universidad Técnica del Norte]. http://repositorio.utn.edu.ec/bitstream/123456789/9535/2/04 ISC 524 TRABAJO DE GRADO.pdf

Guindel, E. (2010). *Calidad y seguridad de la información y auditoría informática*. Universidad Carlos III de Madrid. https://e-archivo.uc3m.es/handle/10016/8510

Gunes, B., Kayisoglu, G., & Bolat, P. (2021). Cyber security risk assessment for seaports: A case study of a container port. *Computers & Security*, *103*, 102196. https://doi.org/10.1016/j.cose.2021.102196

Guo, J., & Wang, L. (2020). Learning to upgrade internet information security and protection strategy in big data era. *Computer Communications*, *160*, 150–157. https://doi.org/10.1016/j.comcom.2020.05.043

Gutiérrez Garzón, L. (2003). La auditoria de información como herramienta de evaluación y mejoramiento de la gestión de documentos. *Biblios*, *4*(16), 14–22. https://www.redalyc.org/pdf/161/16101604.pdf

Hadlington, L., Binder, J., & Stanulewicz, N. (2021). Exploring role of moral disengagement and counterproductive work behaviours in information

security awareness. *Computers in Human Behavior*, *114*, 106557. https://doi.org/10.1016/j.chb.2020.106557

Halabi, T., & Bellaiche, M. (2017). Towards quantification and evaluation of security of Cloud Service Providers. *Journal of Information Security and Applications*, *33*, 55–65. https://doi.org/10.1016/j.jisa.2017.01.007

Halvorsen, J., Waite, J., & Hahn, A. (2019). Evaluating the Observability of Network Security Monitoring Strategies With TOMATO. *IEEE Access*, *7*, 108304–108315. https://doi.org/10.1109/ACCESS.2019.2933415

Hamidian, B., & Ospino, G. (2015). *¿Por qué los sistemas de información son esenciales?*

Harris, M. K., & Williams, L. T. (2020). Audit quality indicators: Perspectives from Non-Big Four audit firms and small company audit committees. *Advances in Accounting*, *50*, 100485. https://doi.org/10.1016/j.adiac.2020.100485

Hasas Yeghaneh, Y., Zangiabadi, M., & Dehghani Firozabadi, S. M. (2015). Factors Affecting Information Technology Audit Quality. *Journal of Investment and Management*, *4*(5), 196–203. https://doi.org/10.11648/j.jim.20150405.19

Hassandoust, F., Subasinghage, M., & Johnston, A. C. (2022). A neo-institutional perspective on the establishment of information security knowledge sharing practices. *Information & Management*, *59*(1), 103574. https://doi.org/10.1016/j.im.2021.103574

Havelka, D., & Merhout, J. W. (2007). Development of an information technology audit process quality framework. *Association for Information Systems - AMCIS 2007 Proceedings*, *61*, 910–916. https://aisel.aisnet.org/amcis2007/61/

Havelka, D., & Merhout, J. W. (2013). Internal information technology audit process quality: Theory development using structured group processes. *International Journal of Accounting Information Systems*, *14*(3), 165–192. https://doi.org/10.1016/j.accinf.2012.12.001

Heigl, M., Anand, K. A., Urmann, A., Fiala, D., Schramm, M., & Hable, R. (2021). On the Improvement of the Isolation Forest Algorithm for Outlier Detection with Streaming Data. *Electronics*, *10*(13), 1534. https://doi.org/10.3390/electronics10131534

Hemphill, T. A., & Longstreet, P. (2016). Financial data breaches in the U.S. retail economy: Restoring confidence in information technology security standards. *Technology in Society*, *44*, 30–38. https://doi.org/10.1016/j.techsoc.2015.11.007

Holm, C., & Zaman, M. (2012). Regulating audit quality: Restoring trust and legitimacy. *Accounting Forum*, *36*(1), 51–61. https://doi.org/10.1016/j.accfor.2011.11.004

Höne, K., & Eloff, J. H. P. (2002). Information security policy — what do international information security standards say? *Computers & Security*, *21*(5), 402–409. https://doi.org/10.1016/S0167-4048(02)00504-7

Hong, J., Enoch, S., Kim, D., Nhlabatsi, A., Fetais, N., & Khan, K. (2018). Dynamic security metrics for measuring the effectiveness of moving target

defense techniques. *Computers & Security*, *79*, 33–52. https://doi.org/10.1016/J.COSE.2018.08.003

Hsu, C., Harn, L., Xia, Z., & Zhang, M. (2020). Non-Interactive Dealer-Free Dynamic Threshold Secret Sharing Based on Standard Shamir's SS for 5G Networks. *IEEE Access*, *8*, 203965–203971. https://doi.org/10.1109/ACCESS.2020.3035278

Humphreys, E. (2011). Information security management system standards. *Datenschutz Und Datensicherheit - DuD*, *35*(1), 7–11. https://doi.org/10.1007/s11623-011-0004-3

Imbaquingo, D., Diaz, J., Ron, M., Cajas, F., & Luje, A. (2020). Evaluation model of computer audit methodologies based on inherent risk. *2020 15th Iberian Conference on Information Systems and Technologies (CISTI)*, 1–7. https://doi.org/10.23919/CISTI49556.2020.9140877

Imbaquingo, D., Díaz, J., Saltos, T., Arciniega, S., De La Torre, J., & Jácome, J. (2020). Análisis de las principales dificultades en la auditoría informática: una revisión sistemática de literatura. *Revista Ibérica de Sistemas e Tecnologias de Informação*, *32*, 427–440. https://www.proquest.com/docview/2452331691?pq-origsite=gscholar&fromopenview=true

Imbaquingo, D., Diaz, J., Saltos, T., Arciniega, S., León, D., & Robayo, A. (2020). Information security issues in educational institutions. *2020 15th Iberian Conference on Information Systems and Technologies (CISTI)*, 1–7. https://doi.org/10.23919/CISTI49556.2020.9141014

Imbaquingo, D., Pusdá, M., & Jácome, J. (2016). *Fundamentos de Auditoría Informática basada en riesgos*. Editorial UTN.

Imbaquingo, D., San Pedro, L., Díaz, J., Arciniega, S., Saltos, T., & Ortega, C. (2022). Computer Auditing Quality Assessment Based on Human, Technical and Contextual Factors. *Communications in Computer and Information Science*, 320–338. https://doi.org/10.1007/978-3-031-20316-9_25

Imbaquingo, D., San Pedro, L., Diaz, J., Saltos, T., & Arciniega, S. (2021). Let's talk about Computer Audit Quality: A systematic literature review. *2021 International Conference on Maintenance and Intelligent Asset Management (ICMIAM)*, 1–7. https://doi.org/10.1109/ICMIAM54662.2021.9715192

Imbaquingo Esparza, D. E., Ron Egas, M. B., Cajas Sinchiguano, F. A., & Luje Misacango, R. A. (2020). Evaluation model of computer audit methodologies based on inherent risk. *Iberian Conference on Information Systems and Technologies, CISTI*, 24–27. https://doi.org/10.23919/CISTI49556.2020.9140877

Instituto Nacional de Estadística y Censos. (2021). *INEC*. Programa Nacion de Estadisticas 2017- 2021. https://www.ecuadorencifras.gob.ec/documentos/webinec/Normativas Estadisticas/Planificacion Estadistica/Programa_Nacional_%0Ade_Estadistica-2017.pdf

International Auditing and Assurance Standards Board. (2014). *A framework for audit quality*. International Federation of Accountants.

https://www.ifac.org/sites/default/files/publications/files/A-Framework-for-Audit-Quality-Key-Elements-that-Create-an-Environment-for-Audit-Quality-2.pdf

INTOSAI & ISSAI. (2016). Directrices para la Evaluación de las Políticas Públicas. *ISSAI Journal*. http://www.issai.org/en_us/site-issai/issai-framework/intosai-gov.htm

ISACA. (2020). ITAF ™ Companion Performance Guidelines 2208. *ISACA Journal*.

ISO 19011. (2018). Norma Internacional ISO 19011 - Directrices para la auditoria de los sistemas de gestión. *Secretaría Central de ISO En Ginebra, Suiza, Como Traducción Oficial En Español Avalada Por El Translation Management Group*, *2018*, 55.

Jiang, Y., & Atif, Y. (2021). A selective ensemble model for cognitive cybersecurity analysis. *Journal of Network and Computer Applications*, *193*, 103210. https://doi.org/10.1016/j.jnca.2021.103210

Karie, N., Sahri, N., Yang, W., Valli, C., & Kebande, V. (2021). A Review of Security Standards and Frameworks for IoT-Based Smart Environments. *IEEE*, 121975–121995. https://doi.org/10.1109/ACCESS.2021.3109886

Khaleel, A. H., & Abduljaleel, I. Q. (2021). A novel technique for speech encryption based on k-means clustering and quantum chaotic map. *Bulletin of Electrical Engineering and Informatics*, *10*(1), 160–170. https://doi.org/10.11591/eei.v10i1.2405

Knechel, W., Krishnan, G., Pevzner, M., Shefchik, L., & Velury, U. (2013). Audit quality: Insights from the academic literature. *Auditing*, *32*(1), 385–421. https://doi.org/10.2308/ajpt-50350

Knight, S., Buffett, S., & Hung, P. C. K. (2007). The International Journal of Information Security Special Issue on privacy, security and trust technologies and E-business services. *International Journal of Information Security*, *6*(5), 285–286. https://doi.org/10.1007/s10207-007-0036-8

Krieger, F., & Drews, P. (2018). Leveraging Big Data and Analytics for Auditing: Towards a Taxonomy. *Thirty Ninth International Conference on Information Systems*. https://www.researchgate.net/profile/Paul-Drews/publication/328902212_Leveraging_Big_Data_and_Analytics_for_Auditing_Towards_a_Taxonomy/links/5beaa034a6fdcc3a8dd2122d/Leveraging-Big-Data-and-Analytics-for-Auditing-Towards-a-Taxonomy.pdf

Kure, H., Islam, S., & Razzaque, M. (2018). An Integrated Cyber Security Risk Management Approach for a Cyber-Physical System. *Applied Sciences*, *8*(6), 898. https://doi.org/10.3390/app8060898

Llumiquinga, L., & Pilco, D. (2015). *Evaluación Técnica Informática de los Laboratorios de Ciencias de la Computación de la Universidad de las Fuerzas Armadas ESPE* [ESPE]. http://repositorio.espe.edu.ec/handle/21000/10825

Ley Orgánica de Educación Superior, (2018). https://www.ces.gob.ec/documentos/Normativa/LOES.pdf

Lorenzo, L. (2019). *Auditoría del Sistema APPCC*. Diaz de Santos. https://www.editdiazdesantos.com/wwwdat/pdf/9788479788650.pdf

Lundgren, B., & Möller, N. (2019). Defining Information Security. *Science and Engineering Ethics*, *25*(2), 419–441. https://doi.org/10.1007/s11948-017-9992-1

Ma, X. (2022). IS professionals' information security behaviors in Chinese IT organizations for information security protection. *Information Processing & Management*, *59*(1), 102744. https://doi.org/10.1016/j.ipm.2021.102744

Marín, F., & Torres, A. (2005). La información en la Ciencia de la Información: tras las huellas de un concepto. *Revista Cubana de Información En Ciencias de La Salud*, *13*(5). http://scielo.sld.cu/pdf/aci/v13n5/aci09505.pdf

McLeod, A., & Dolezel, D. (2022). Information security policy non-compliance: Can capitulation theory explain user behaviors? *Computers & Security*, *112*, 102526. https://doi.org/10.1016/j.cose.2021.102526

Meriah, I., & Arfa Rabai, L. Ben. (2019). Comparative Study of Ontologies Based ISO 27000 Series Security Standards. *Procedia Computer Science*, *160*, 85–92. https://doi.org/10.1016/j.procs.2019.09.447

Mesquida, A., & Mas, A. (2015a). Implementing information security best practices on software lifecycle processes: The ISO/IEC 15504 Security Extension. *Computers and Security*, *48*, 19–34. https://doi.org/10.1016/j.cose.2014.09.003.

Mesquida, A., & Mas, A. (2015b). Integrating IT service management requirements into the organizational management system. *Computer Standards and Interfaces*, *37*, 80–91. https://doi.org/10.1016/j.csi.2014.06.005

Mesquida, A., Mas, A., Feliu, S., & Arcilla, M. (2014). Integración de Estándares de Gestión de TI mediante MIN-ITs. *Revista Iberica de Sistemas e Tecnologias de Informacao*, 31–45. https://doi.org/10.4304/risti.e1.31-45

Mirtsch, M., Blind, K., Koch, C., & Dudek, G. (2021). Information security management in ICT and non-ICT sector companies: A preventive innovation perspective. *Computers and Security*, *109*. https://doi.org/10.1016/j.cose.2021.102383

Mirtsch, M., Kinne, J., & Blind, K. (2021). Exploring the Adoption of the International Information Security Management System Standard ISO/IEC 27001: A Web Mining-Based Analysis. *IEEE Transactions on Engineering Management*, *68*(1), 87–100. https://doi.org/10.1109/TEM.2020.2977815

Moutaz, H., Kuan, L., Kholoud, A., & Maged, A. (2018). Applications of Big Data Analytics in Financial Auditing - A Study on The Big Four. *AMCIS 2018 Proceedings. 8.* https://aisel.aisnet.org/amcis2018/AccountingIS/Presentations/8

Murgueytio, J. (2017). *Modelo de gestión para las unidades de auditoría interna del sector público ecuatoriano*. Editorial Universitaria.

Paredes, G., & Vega, M. (2011). *Desarrollo de una Metodología para la Auditoría de Riesgos Informáticos (Físicos y Lógicos) y su Aplicación al Departamento de Informática de la Dirección Provincial de Pichincha del Consejo de la Judicatura*. In Phys. Rev. E. ESPOCH.

Peltier, T. (2001). *Information Security Policies, Procedures, and Standardss: Guidelines for ...* Thomas R. Peltier.

https://books.google.com.ec/books?hl=es&lr=&id=mM_LsS-W4f4C&oi=fnd&pg=PP1&dq=standards+in+information+security&ots=WhTYn3jAgg&sig=D7GOca3Eh_BT-%0AjQGyADaU6eYXP0&redir_esc=y#v=onepage&q=standards in information security&f=false

Philippou, E., Frey, S., & Rashid, A. (2020). Contextualising and aligning security metrics and business objectives: A GQM-based methodology. *Computers & Security*, *88*, 101634. https://doi.org/10.1016/j.cose.2019.101634

Public Company Accounting Oversight Board. (2015). Concept Release on Audit Quality Indicators. *PCAOB*, *005*, 1–61. https://pcaobus.org/about/rules-rulemaking/rulemaking-dockets/docket-041-concept-release-on-audit-quality-indicators

Pusdá, M., & Imbaquingo, D. (2015). Evaluación de amenazas y vulnerabilidades informáticas en sistemas académicos universitarios, aplicando ISO 27000. *SATHIRI*, *9*, 202. https://doi.org/10.32645/13906925.464

Ramos, A., Lazar, M., Filho, R., & Rodrigues, J. (2017). Model-Based Quantitative Network Security Metrics: A Survey. *IEEE Communications Surveys and Tutorials*, *19*(4), 2704–2734. https://doi.org/10.1109/COMST.2017.2745505

Ranaweera, P., Jurcut, A., & Liyanage, M. (2022). MEC-enabled 5G Use Cases: A Survey on Security Vulnerabilities and Countermeasures. *ACM Computing Surveys*, *54*(9), 1–37. https://doi.org/10.1145/3474552

Real Academia Española. (2021). *Diccionario de la lengua española*. https://dle.rae.es/calidad

Redavid, D., Corizzo, R., & Malerba, D. (2018). An OWL Ontology for Supporting Semantic Services in Big Data Platforms. *2018 IEEE International Congress on Big Data (BigData Congress)*, 228–231. https://doi.org/10.1109/BigDataCongress.2018.00039

Refaat, R., & El-Henawy, I. M. (2019). Innovative method to evaluate quality management system audit results' using single value neutrosophic number. *Cognitive Systems Research*, *57*, 197–206. https://doi.org/10.1016/j.cogsys.2018.10.014

Rivadeneira Ramos, E. (2018). *Estado de las tecnologías de la información y la comunicación en las Universidades Ecuatorianas* (Issue May). www.creativecommons.org/licences/by-nc/4.0Estedocumentosepuededescargarenformato PDFdesdehttps://www.cedia.edu.ec/es/publicaciones/libros

San Pedro, L. (2022). *Evaluación de la calidad de los resultados de procesos de auditoría de la información a Instituciones de Educación Superior de la Zona 1 del Ecuador* [Universidad Técnica del Norte]. http://repositorio.utn.edu.ec/bitstream/123456789/11207/2/04 MAUT 142 TRABAJO GRADO.pdf

Schmitz, C., Schmid, M., Harborth, D., & Pape, S. (2021). Maturity level assessments of information security controls: An empirical analysis of practitioners assessment capabilities. *Computers & Security*, *108*, 102306.

https://doi.org/10.1016/j.cose.2021.102306

Shan, C., Jiang, B., Xue, J., Guan, F., & Xiao, N. (2018). An Approach for Internal Network Security Metric Based on Attack Probability. *Security and Communication Networks*, *2018*, 1–11. https://doi.org/10.1155/2018/3652170

Shrivastava, U., Song, J., Han, B. T., & Dietzman, D. (2021). Do data security measures, privacy regulations, and communication standards impact the interoperability of patient health information? A cross-country investigation. *International Journal of Medical Informatics*, *148*, 104401. https://doi.org/10.1016/j.ijmedinf.2021.104401

Silva, O. (2018). *Auditoría Informática aplicando la metodología OCTAVE de los procesos de recaudaciones y permisos en el Gobierno Autónomo Descentralizado (GAD) de San Pedro de Pelileo*.

Siponen, M., & Willison, R. (2009). Information security management standards: Problems and solutions. *Information and Management*, *46*(5), 267–270. https://doi.org/10.1016/j.im.2008.12.007

Soriano, M. (2014). Seguridad en redes y seguridad de la información. In *Improvet*.

Soy i Aumatell, C. (2003). La auditoría de la información, componente clave de la gestión estratégica de la información. *El Profesional de La Informacion*, *12*(4), 261–268. https://doi.org/10.1076/epri.12.4.261.16889

Stable-Rodríguez, Y. (2012). Auditoría de información y conocimiento en la organización. *Ingeniería Industrial*, *XXXIII*(3), 260–271. https://rii.cujae.edu.cu/index.php/revistaind/article/view/427/466

Stoel, D., Havelka, D., & Merhout, J. W. (2012). An analysis of attributes that impact information technology audit quality: A study of IT and financial audit practitioners. *International Journal of Accounting Information Systems*, *13*(1), 60–79. https://doi.org/10.1016/j.accinf.2011.11.001

Strous, L. (2002). Audit of information systems: The need for cooperation. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *1521*, 264–274. https://doi.org/10.1007/3-540-49477-4_18

Sulaiman, N. A., Shahimi, S., & Nashtar, K. (2019). People and Audit Process Attributes of Audit Quality: Evidence From Malaysia. *Management and Accounting Review (MAR)*, *18*(2), 47. https://doi.org/10.24191/mar.v18i2.715

Sulaiman, N. A., Yasin, F. M., & Muhamad, R. (2018). Perspectives on Audit Quality: an analysis. *Asian Journal of Accounting Perspectives*, *11*(1), 1–27. https://doi.org/10.22452/AJAP.vol11no1.1

Tapia, C., Guevara, E., & Castillo, S. (2016). *Fundamentos de auditoría: aplicación práctica de las Normas Internacionales de Auditoría*. Instituto Mexicano de Contadores Públicos. http://ebookcentral.proquest.com/lib/utnortesp/detail.action?docID=5308830

Trujillo Albarrán, S., Pérez Merlos, J., Salgado Gallegos, M., & Valero Conzuelo, L. (2019). Las Metodologías de la Auditoría Informática y su

relación con Buenas Prácticas y Estándares. In *Ideas en Ciencias de la Ingeniería* (Vol. 1, Issue 1). https://ideasencienciasingenieria.uaemex.mx/article/view/14591

Universidad Ecotec. (2019). *Gestión de Auditoría*.

Valencia Duque, F., & Orozco Alzate, M. (2017). Metodología para la implementación de un Sistema de Gestión de Seguridad de la Información basado en la familia de normas ISO/IEC 27000. *RISTI - Revista Iberica de Sistemas e Tecnologias de Informacao*, *22*, 73–88. https://doi.org/10.17013/risti.22.73-88

Wagner, I., & Eckhoff, D. (2019). Technical Privacy Metrics. *ACM Computing Surveys*, *51*(3), 1–38. https://doi.org/10.1145/3168389

Wang, C.-H., & Tsai, D.-R. (2009). Integrated installing ISO 9000 and ISO 27000 management systems on an organization. *43rd Annual 2009 International Carnahan Conference on Security Technology*, 265–267. https://doi.org/10.1109/CCST.2009.5335527

Xiao, T., Geng, C., & Yuan, C. (2020). How audit effort affects audit quality: An audit process and audit output perspective. *China Journal of Accounting Research*, *13*(1), 109–127. https://doi.org/10.1016/j.cjar.2020.02.002

Yasin, F., & Nelson, S. (2012). Audit Committee and Internal Audit: implications on audit quality. *International Journal of Economics, Management and Accounting*, *20*(2), 8–10. https://journals.iium.edu.my/enmjournal/index.php/enmj/article/view/216

Ye, K., Cheng, Y., & Gao, J. (2014). How individual auditor characteristics impact the likelihood of audit failure: Evidence from China. *Advances in Accounting*, *30*(2), 394–401. https://doi.org/10.1016/j.adiac.2014.09.013

Yuniarti, R., & Zumara, W. M. (2013). Audit Quality Attributes and Audit Client Satisfaction. *International Journal of Humanities and Management Sciences*, *1*(1), 96–100. http://www.isaet.org/images/extraimages/IJHMS 0101223.pdf

Zahmatkesh, S., & Rezazadeh, J. (2017). The effect of auditor features on audit quality. *Tékhne*, *15*(2), 79–87. https://doi.org/10.1016/j.tekhne.2017.09.003

Zhou, G., Tian, X., & Zhou, A. (2022). Image copy-move forgery passive detection based on improved PCNN and self-selected sub-images. *Frontiers of Computer Science*, *16*(4). https://doi.org/10.1007/s11704-021-0450-5

ANEXOS

Anexo A: Caracterización del método

UNIVERSIDAD NACIONAL DE LA PLATA			CÓDIGO:	A.O.1.1
			VERSIÓN:	2
			ELABORADO POR:	DAISY IMBAQUINGO
CARACTERIZACIÓN DEL MÉTODO "AUDITORIA INFORMÁTICA"			REVISADO POR:	JAVIER DÍAZ
MACROPROCESO: AUDITORIA OPERACIONAL		RESPONSABLES PROCESO:	DAISY IMBAQUINGO	
PROCESO: AUDITORIA INFORMÁTICA		PARTICIPANTES:	DAISY IMBAQUINGO - JAVIER DÍAZ - MARIO RON	
OBJETIVO	El objetivo del método de auditoría planteada es aseguar una mayor calidad y seguridad de la información mediante la recomendación de lineamientos y controles proporcionados por marcos referenciales internacionales.			

CONTROL				
CÓDIGO	DOCUMENTOS	REGLAS	CÓDIGO	REGISTROS
D01.EXT.A.O.1.1	Normas estándares internacionales	Las actas de reuniones deben actualizar continuamente Los documentos generados deben estar firmados, aprobados y legalizados	R01.INT.A.O.1.1	Check list
D02.EXT.A.O.1.1	Informes de auditorias anteriores		R02.INT.A.O.1.1	Encuestas
D03.INT.A.O.1.1	Plan Preliminar		R03.INT.A.O.1.1	Entrevistas
D04.INT.A.O.1.2	Plan de auditoría		R04.INT.A.O.1.1	Actas de reunión
D05.INT.A.O.1.2	Hallazgos de auditoría		R05.INT.A.O.1.1	Evidencias de auditoría
D06.INT.A.O.1.3	Informe Final de auditoría			

NORMATIVA LEGAL		NORMATIVA
Normativa Legal Interna Políticas de seguridad de seguridad de la Información IES Ley Orgánica de Educación Superior (LOES) Política de Evaluación Institucional de Universidades y Escuelas Politécnicas en el marco del Sistema de Aseguramiento de la Calidad de la Educación Superior Ley de Protección de Datos	**Normativa Legal Externa** ISO 27002:2017 COBIT ITIL ITAF ISSAI Derechos de privacidad de la Información Normas de Control Interno 410-10	ISO 9001:2015

ENTRADAS		Actividades	SALIDAS	
Procesos anteriores / Parte interesada	**Entradas**		**Salidas**	**Parte interesada / Procesos posteriores**
Auditor-Cliente Contacto con el cliente/Auditor-Cliente Estudio del entorno / Auditor Definición del equipo de auditoría / Auditor Elaboración del plan preliminar / Auditor-Cliente Elaboración de la propuesta / Auditor-Cliente	Necesidad de requerimientos Requisitos identificados Diagnóstico del entorno Roles y responsabilidades del equipo auditor Plan Preliminar Propuesta de auditoría Propuesta aprobada	**PLANIFICACIÓN (FASE I)** - Contacto con el cliente - Entorno a auditar - Equipo de auditoría - Plan Preliminar - Propuesta de auditoría - Contrato	Requisitos identificados Diagnóstico del entorno Equipo definido Plan preliminar Propuesta de auditoría Propuesta de auditoría aprobada Contrato de auditoría firmado	Auditor / Estudio de entorno Auditor / Definir equipo Auditor / Elaboración plan preliminar Auditor-Cliente / Elaboración de propuesta Auditor-Cliente / Elaboración y firma del contrato
Elaboración y firma del contrato / Auditor-Cliente Elaboración de instrumentos para la investigación de campo / Auditor Ejecutar la investigación de campo / Auditor Análisis de la información recolectada/ Auditor	Contrato firmado Documento del plan de trabajo Instrumentos de trabajo Ejecución del plan de auditoría Evidencias y hallazgos de auditoría	**EJECUCIÓN (FASE II)** - Plan de trabajo - Investigacion de campo - Informe final preliminar	Documento del plan de trabajo Instrumentos de trabajo Ejecución del plan de auditoria Evidencias y hallazgos de auditoría Conclusiones preliminares	Auditor / Elaboración de instrumentos para la investigación de campo Auditor / Ejecutar la investigación de campo Auditor / Análisis de la información recolectada Auditor / Elaboración de las conclusiones preliminares para presentar a discusión
Elaboración de las conclusiones preliminares para presentar a discusión / Auditor-Cliente Lectura del borrador / Auditor-Cliente Entrega del informe final / Auditor-Cliente	Conclusiones preliminares Documento informe final	**COMUNICACIÓN DE RESULTADOS (FASE III)** - Informe final preliminar - Informe final - Cierre del contrato	Documento informe final Borrador aceptado Auditoría realizada	Auditor-Cliente / Lectura del borrador Auditor-Cliente / Entrega del informe final
Entrega del informe final / Auditor-Cliente Evaluación de calidad / Auditor Evaluación de seguridad / Auditor Evaluación de cumplimiento / Auditor Análisis de los datos de validación / Auditor	Cierre de contrato Instrumentos de evaluación	**VALIDACIÓN DE LA AUDITORÍA (FASE IV)** - Calidad - Seguridad de la información - Cumplimiento - Análisis de datos	Indice de calidad Nivel de seguridad Nivel de cumplimiento Resultados de análisis de datos	Auditor / Evaluación de calidad Auditor / Evaluación de seguridad Auditor / Evaluación de cumplimiento Auditor / Análisis de los datos de validación

Análisis de los datos de validación / Auditor Entrevista con el auditado / Auditor-Cliente Seguimiento de recomendaciones / Auditor	Informes de auditorías anteriores	**SEGUIMIENTO DE LA AUDITORÍA (FASE V)** - Contacto con el auditado - Informe final de auditoría	Seguimiento a auditorías anteriores	Auditor-Cliente / Entrevista con el auditado Auditor / Seguimiento de recomendaciones

RECURSOS			
MÁQUINAS Y EQUIPOS	**MATERIALES**	**INFRAESTRUCTURA**	**FINANCIERO**
Computador Celular Impresora Disco Duro externo	Normas internacionales Marcos referenciales Software específico	Departamento de Tecnologías IES	Estatal

INDICADORES
Calidad de la auditoría
Nivel de seguridad de la información
Nivel de cumplimiento postauditoría

RIESGOS	**CONTROL DE SALIDA NO CONFORME**
Riesgo inherente de la auditoría	Conocer el procedimiento Ejecutar el procedimiento (Inconsistencia del proceso de auditoría)

Anexo B: Ficha de indicadores
Calidad de auditorías

UNIVERSIDAD NACIONAL DE LA PLATA	UNIVERSIDAD NACIONAL DE LA PLATA		Código	I01.A.O.1.1
NOMBRE DEL INDICADOR	**SUBPROCESO**	**FRECUENCIA DE MEDICIÓN**	**RESPONSABLE**	
Nivel de calidad de auditoria	Auditoria Informática	Al finalizar el proceso de auditoria	Cliente	
Descripción	El objetivo del indicador es conocer el nivel de calidad de los resultados de procesos de auditoria a través de 54 métricas basadas en tres factores: factor humano, factor técnico y factor contextual o del entorno.			
Fórmula	Σ(m1+m2+m3+.....+m42)/m	**TIPO DE INDICADOR**		
		Cuantitativo		
Elaborado	Daisy Imbaquingo	**Revisado**	Mario Ron	**Aprobado** Javier Diaz

Instrumento de validación para el nivel de calidad

MÉTODO DE AUDITORÍA INFORMÁTICA PARA INSTITUCIONES DE EDUCACIÓN SUPERIOR (MAIIES)	
NOMBRE EVALUADOR:	
INSTITUCIÓN EVALUADA:	

OBJETIVO
Evaluar la calidad de los resultados de los procesos de auditoría informática a través de métricas basadas en el factor humano, factor técnico y factor contextual en Instituciones de Educación Superior (IES).

FACTORES DE CALIDAD

FACTOR DE EVALUACIÓN	MÉTRICA DE EVALUACIÓN	CALIFICACIÓN	OBSERVACIONES	RANGOS DE RESULTADOS	CÁLCULO DE RESULTADOS
Factor Humano	El equipo auditor procuró que el cliente participe en todo el proceso de auditoría			Entre 85% y 100% CALIDAD DE LA AUDITORÍA ALTA	
	El equipo auditor obtuvo la conformidad del cliente acerca de las actividades desarrolladas				
	El personal que realiza la auditoría tenía competencias necesarias para realizar su trabajo				
	El auditor estaba seguro de sí mismo y de su trabajo				
	El equipo auditor conservó su independencia en apariencia y acción				
	El equipo auditor se centró en los hechos				
	El equipo auditor recibió apoyo para lograr las metas				
	El equipo auditor demuestró esfuerzo al realizar la auditoría				

	El auditor se preocupaba por su formación y actualización continua			
	El auditor contaba con certificaciones nacionales e internacionales en el área de auditoría y auditoría informática			
	Los miembros del equipo auditor demuestraron conocimiento en seguridad de la información y procesamiento de datos			
	Las diferencias con el cliente fueron tratadas de forma oportuna, profesional y objetiva			
	El auditor vinculó expertos como apoyo en el proceso de auditoría para obtener resultados y recomendaciones para el cliente			
	El equipo auditor usó plantillas y formularios para documentar			
	Los hallazgos y conclusiones de la auditoría fueron un reflejo exacto de los hechos reales del proceso auditado			
	Los resultados de la auditoría fueron respaldados y documentados con las evidencias recopiladas al auditar			
	Los recursos para la auditoría fueron asignados de acuerdo con la importancia y complejidad de la auditoría			
	El sistema, proceso u objeto auditado tenía importancia para la organización			
	En el alcance se abordaron todos los elementos necesarios para auditar exitosamente			
	La ejecución de la auditoría cumplió con los elementos acordados en el alcance			
	El modelo de evaluación de riesgos fue comprensible			
	El plan de auditoría tomó en cuenta los riesgos relacionados con el cliente			

Factor Técnico	El proceso de auditoría se desarrolló con exactitud y precisión			**Entre 84 % y 65% CALIDAD DE LA AUDITORÍA MEDIA**
	El informe de auditoría fue claro y conciso con sus resultados			
	El alcance, hallazgos y recomendaciones han sido entendibles para cualquier persona que haga uso del informe de auditoría			
	La auditoría se ejecutó bajo las políticas, estándares, manuales, directrices y prácticas de auditoría informática			
	Las listas de verificación estuvieron completas, aprobadas y documentadas			
	El trabajo de campo fue revisado por un experto			
	La información y resultados de anteriores auditorías estuvieron disponibles para revisión			
	Los objetivos y el alcance de la auditoría fueron especificados adecuadamente			
	Los miembros del equipo auditor tenían una comprensión clara y coherente del plan de auditoría			
	El presupuesto y cronograma de auditoría se establecieron de manera adecuada			
	Se evaluaron los requisitos de personal y equipos asignados para la auditoría			
	El plan de auditoría fue elaborado, revisado y aprobado por los supervisores, responsables de la organización y miembros del equipo auditor			
	El equipo auditor utilizó una metodología de auditoría informática para planificar, gestionar y desarrollar la auditoría			
	El auditor promovió a través de sus informes una cultura organizacional basada en buenas prácticas de seguridad informática			

Factor Contextual o del Entorno	El equipo auditor tenía estrictos procedimientos de control de calidad			MENOS DE 65% CALIDAD DE LA AUDITORÍA BAJA	
	El líder del equipo auditor estuvo comprometido con el sistema de control de calidad				
	La normativa y regulaciones emitidas por organismos de control fueron reflejadas en el plan de auditoría				
	El equipo auditor conocía la información relevante de leyes y regulaciones que puedan tener un impacto significativo en los objetivos de la auditoría				
	Se aplicaron medidas disciplinarias en caso de incumplir con el plan de auditoría o la normativa legal regulatoria vigente				PUNTAJE
	El costo de la auditoría estuvo de acuerdo con la complejidad y las actividades desarrolladas				#¡DIV/0!
	TOTAL CALIFICACIÓN	#¡DIV/0!			

CONVENCIÓN	**VALOR**	**DEFINICIÓN**
(S) SOBRESALIENTE	**10**	La auditoría evaluada supera ampliamente la métrica de calidad
(B) BUENO	**7**	La auditoría evaluada cumple con la métrica de calidad
(R) REGULAR	**5**	La auditoría evaluada cumple parcialmente con la métrica de calidad
(D) DEFICIENTE	**3**	La auditoría no cumple con la métrica de calidad

NIVEL DE CALIDAD

CALIDAD DE LA AUDITORÍA ALTA: Se recomienda continuar con el trabajo realizado porque el desempeño del proceso de auditoría es eficiente

CALIDAD DE LA AUDITORÍA MEDIA: Se recomienda que siga mejorando su nivel de desempeño en los procesos de auditoría

CALIDAD DE LA AUDITORÍA BAJA: Se recomienda que trate de esforzarse por mejorar su desempeño en el proceso de auditoría

OBSERVACIONES O RECOMENDACIONES PARA EL MEJORAMIENTO

FIRMA Y NOMBRES DEL EVALUADO **FIRMA Y NOMBRES DEL EVALUADOR** **FIRMA Y NOMBRES DEL REVISOR**

UNIVERSIDAD NACIONAL DE LA PLATA	UNIVERSIDAD NACIONAL DE LA PLATA		Código	I02.A.O.1.1
NOMBRE DEL INDICADOR	**SUBPROCESO**	**FRECUENCIA DE MEDICIÓN**	**RESPONSABLE**	
Nivel de seguridad de la información	Auditoria informática	Al finalizar el proceso de auditoria	Auditor	
Descripción	El objetivo del indicador es conocer el nivel de seguridad de la información con la que cuentan las IES auditadas			
Fórmula	Σ(m1+m2+m3+.....+m18)/m		**TIPO DE INDICADOR**	
			Cuantitativo	

Elaborado	Daisy Imbaquingo	**Revisado**	Mario Ron	**Aprobado**	Javier Diaz

Instrumento de validación para el nivel de seguridad

MÉTODO DE AUDITORÍA INFORMÁTICA PARA INSTITUCIONES DE EDUCACIÓN SUPERIOR (MAIIES)	
NOMBRE EVALUADOR:	
INSTITUCIÓN EVALUADA:	

OBJETIVO
Evaluar el nivel de seguridad de la información a través de métricas basadas en los pilares de seguridad: integridad, confidencialidad integridad, autenticidad y trazabilidad en Instituciones de Educación Superior (IES).

FACTORES DE CALIDAD					
FACTOR DE EVALUACIÓN	MÉTRICA DE EVALUACIÓN	CALIFICACIÓN	OBSERVACIONES	RANGOS DE RESULTADOS	CÁLCULO DE RESULTADOS
Confidencialidad	Se aplican políticas para la seguridad de la información dentro de la institución			Entre 85% y 100% SEGURIDAD DE LA INFORMACIÓN ALTA	
	Las políticas y procedimientos en seguridad de la información dentro de la institución se actualizan periódicamente				
	Las responsabilidades en la seguridad de la información son delegadas, documentadas y entregadas formalmente a todo el personal de la institución, según su cargo				
	Se aplican políticas y acciones de seguridad de la información sensible de la institución				
	Se actualiza y aplica las políticas de acceso a la información en base a los roles de usuario existentes				
	Se dispone de una acreditación en seguridad de la información para todos sus sistemas informáticos				
	Se aplican procedimientos documentados para seguir en caso de incidentes de seguridad				

	Se realizan auditorías de cumplimiento de seguridad de la información			Entre 84 % y 65% SEGURIDAD DE LA INFORMACIÓN MEDIA
	Se aplican políticas de gestión de contraseñas para los usuarios finales de la institución			
	Se identifican a los usuarios que acceden a la red y las acciones que ejecutan			
Integridad	Se aplica un control de acceso a la infraestructura y servicios de TI de la institución			
	Se capacita e involucra a usuarios, colaboradores y personal en los temas de seguridad de la información			
	Se realiza análisis de vulnerabilidades de los servicios web de la institución			MENOS DE 65% SEGURIDAD DE LA INFORMACIÓN BAJA
	Se aplican planes de monitoreo y gestión de impacto de incidentes de seguridad en la institución			
	Se actualiza y documenta el inventario de todos los activos de TI			
Disponibilidad	Se dispone de aplicaciones para proteger de software malicioso a todas sus soluciones informáticas			
	Se realizan copias de seguridad de la información			
	Se monitorean las actividades desarrolladas por los usuarios			
	TOTAL CALIFICACIÓN	#¡DIV/0!		

NIVEL DE SEGURIDAD
#¡DIV/0!

CONVENCIÓN	VALOR	DEFINICIÓN
(S) SOBRESALIENTE	**10**	La IES cumple ampliamente con la métrica de seguridad
(B) BUENO	**7**	La IES cumple con la métrica de seguridad
(R) REGULAR	**5**	La IES cumple parcialmente con la métrica de seguridad
(D) DEFICIENTE	**3**	La IES no cumple con la métrica de seguridad

NIVEL DE SEGURIDAD

SEGURIDAD DE LA INFORMACIÓN ALTA:	Se recomienda continuar con el cumplimiento de los parámetros para la seguridad de la información
SEGURIDAD DE LA INFORMACIÓN MEDIA:	Se recomienda cumplir con los parámetros para la seguridad de la información
SEGURIDAD DE LA INFORMACIÓN BAJA:	Se recomienda implementar los parámetros para la seguridad de la información

OBSERVACIONES O RECOMENDACIONES PARA EL MEJORAMIENTO

FIRMA Y NOMBRES DEL EVALUADO **FIRMA Y NOMBRES DEL EVALUADOR** **FIRMA Y NOMBRES DEL REVISOR**

Cumplimiento de actividades

UNIVERSIDAD NACIONAL DE LA PLATA	UNIVERSIDAD NACIONAL DE LA PLATA		Código	I03.A.O.1.1
NOMBRE DEL INDICADOR	**SUBPROCESO**	**FRECUENCIA DE MEDICIÓN**	**RESPONSABLE**	
Nivel de cumplimiento postauditoria	Auditoria informática	Al finalizar el proceso de auditoria	Auditor	
Descripción	El objetivo del indicador es conocer el nivel de cumpliento de las actividades descritas en el proceso de auditoria			
Fórmula	Σ(m1+m2+m3+.....+m47)/m	**TIPO DE INDICADOR**		
		Cuantitativo		
Elaborado	Daisy Imbaquingo	**Revisado**	Mario Ron	**Aprobado** Javier Diaz

Instrumento de validación para el nivel de cumplimiento

MÉTODO DE AUDITORÍA INFORMÁTICA PARA INSTITUCIONES DE EDUCACIÓN SUPERIOR (MAIIES)	
NOMBRE EVALUADOR:	
INSTITUCIÓN EVALUADA:	

OBJETIVO

Evaluar el nivel de cumplimiento de las actividades realizadas durante la ejecución del MAIIES

FACTORES DE CALIDAD

FASES DE LA AUDITORÍA	ACTIVIDAD	CALIFICACIÓN	OBSERVACIONES	RANGOS DE RESULTADOS	CÁLCULO DE RESULTADOS
	Establecer lugar y fecha de encuentro con el cliente				
	Registrar reunión inicial con el cliente				
	Identificar las partes interesadas y responsables para la auditoría				
	Comprender el contexto externo del entorno a auditar				
	Comprender el contexto interno de la institución a auditar				
	Comprender estrategias y prioridades de la institución				
	Determinar objetivos de la auditoría en base al estudio del entorno				
	Determinar el riesgo relevante del proceso de auditoría				
	Definir los límites organizacionales de la auditoría				
				Entre 85% y 100% NIVEL DE CUMPLIMIENTO ALTO	

Planificación de la auditoría	Identificar miembros del equipo auditor			
	Seleccionar miembros del equipo auditor			
	Definir roles acordes a los conocimientos y habilidades de los miembros del equipo auditor			
	Documentar plan preliminar			
	Determinar antecedentes			
	Determinar objetivos especificos de la auditoría			
	Determinar el alcance de la auditoría			
	Determinar recursos para la auditoría			
	Determinar cronograma de la auditoría			
	Determinar costos de la auditoría			
	Documentar los riesgos de la auditoría			
	Presentar plan preliminar al cliente			

	Acordar términos y condiciones de la auditoría			Entre 84 % y 65% SEGURIDAD DE LA INFORMACIÓN MEDIA ▯ ▯ ▯
	Elaborar la propuesta de auditoría			
	Presentar la propuesta de la auditoría			
	Determinar cláusulas del contrato			
	Elaborar el contrato			
	Firmar el contrato			
Ejecución de la auditoría	Diseñar y documentar el plan de trabajo			
	Definir instrumentos para la investigación de campo			
	Elaborar instrumentos de investigación de campo determinados en el plan de trabajo			
	Aplicar técnicas e instrumentos de auditoría			
	Análisis y síntesis de información recopilada			
	Definir hallazgos en base a la información y evidencias recopiladas			
	Elaborar informe final preliminar			
	Agendar fecha para presentación y discusión del informe final preliminar			
	Presentar informe final preliminar para discusión y validación			
	Elaborar informe final			

Comunicación de resultados	Agendar fecha para presentación de informe final			Menos de 65% NIVEL DE CUMPLIMIENTO BAJO
	Presentar informe final y documentos resultantes de la auditoría			
	Cerrar el contrato			
	Retirar garantías			
Validación de la auditoría	Aplicar evaluación de calidad de resultados de auditoría			
	Aplicar evaluación de seguridad de la información en las IES			
	Aplicar evaluación de cumplimiento de actividades de la auditoría			
	Data Mining			
Seguimiento de la auditoría	Consulta directa al auditado			
	Verificación del informe final de auditoría			

PUNTAJE
0

TOTAL SI	0	
TOTAL NO	0	

CONVENCIÓN	**DEFINICIÓN**
SI	La actividad se cumplió en su totalidad
NO	La actividad no se cumplió en el desarrollo de la auditoría

NIVEL DE SEGURIDAD

NIVEL DE CUMPLIMIENTO ALTO:	Se recomienda continuar con el trabajo realizado porque el desempeño del proceso de auditoría es eficiente
NIVEL DE CUMPLIMIENTO MEDIO:	Se recomienda que siga mejorando su nivel de desempeño en los procesos de auditoría
NIVEL DE CUMPLIMIENTO BAJO:	Se recomienda que trate de esforzarse por mejorar su desempeño en el proceso de auditoría

OBSERVACIONES O RECOMENDACIONES PARA EL MEJORAMIENTO

FIRMA Y NOMBRES DEL EVALUADO **FIRMA Y NOMBRES DEL EVALUADOR** **FIRMA Y NOMBRES DEL REVISOR**

Anexo C: Lista maestra de documentos y registros

LISTA MAESTRA DE DOCUMENTOS					
COD	NOMBRE DEL DOCUMENTO	INTERNO	EXTERNO	COD	SUBPROCESO
D01.EXT.A.O.1.1	Normas o estándares internacionales		X	A.O.1.1	Auditoria informática
D02.EXT.A.O.1.1	Informes de auditorias anteriores		X		
D03.INT.A.O.1.1	Plan Preliminar	X			
D04.INT.A.O.1.2	Plan de auditoria	X			
D05.INT.A.O.1.2	Hallazgos de auditoria	X			
D06.INT.A.O.1.3	Informe Final de auditoria	X			

LISTA MAESTRA DE REGISTROS					
COD	NOMBRE DEL REGISTRO	INTERNO	EXTERNO	COD	SUBPROCESO
R01.INT.A.O.1.1	Check list	X		A.O.1.1	Auditoria informática
R02.INT.A.O.1.1	Encuestas	X			
R03.INT.A.O.1.1	Entrevistas	X			
R04.INT.A.O.1.1	Actas de reunión	X			
R05.INT.A.O.1.1	Evidencias de auditoria	X			

MACROPROCESO: AUDITORÍA OPERACIONAL (AO)

PROCESO: AUDITORÍA INFORMÁTICA

SUBPROCESO: TIPO DE AUDITORÍA INFORMÁTICA

***VERSIÓN*:** 06

FIRMAS DE REVISIÓN Y APROBACIÓN

	Nombre / Cargo	**Firma**	**Fecha**
Elaborado por:	MSc. Daisy Imbaquingo		10/02/2023

CONTROL E HISTORIAL DE CAMBIOS

Versión	Descripción del cambio	Fecha de Actualización
01	Edición Original	08/09/2021
02	Correcciones	17/12/2021
03	Revisión	29/05/2022
04	Correcciones	04/08/2022
05	Revisión final	04/10/2022
06	Revisión de validación	20/01/2023

CONTENIDO

1. OBJETIVO

El objetivo del método de auditoría planteado es asegurar una mayor calidad y seguridad de la información mediante la recomendación de lineamientos y controles proporcionados por marcos referenciales internacionales.

2. RESPONSABILIDAD

DAISY IMBAQUINGO
JAVIER DÍAZ

3. GLOSARIO DE TÉRMINOS Y ABREVIATURAS

Abreviaturas:

- IES
- ISO
- COBIT
- ITIL

Definiciones:

- INSTITUCIÓN DE EDUCACIÓN SUPERIOR
- INTERNATIONAL ORGANIZATION FOR STANDARDIZATION
- CONTROL OBJETIVES FOR INFORMATION AND RELATED TECHNOLOGY
- INFORMATION TECHNOLOGY INFRASTRUCTURE LIBRARY

4. REFERENCIAS NORMATIVAS

Normativa Legal Interna

- Políticas de seguridad de seguridad de la Información IES
- Ley Orgánica de Educación Superior (LOES)
- Política de Evaluación Institucional de Universidades y Escuelas Politécnicas en el marco del Sistema de Aseguramiento de la Calidad de la Educación Superior
- Ley de Protección de Datos

Normativa Legal Externa

- ISO 27002:2017
- Marcos referenciales (ITAF, ISSAF, ISSAI, IIAS)
- COBIT
- ITIL
- Derechos de privacidad de la Información
- Normas de Control Interno 410-10

5. DESCRIPCIÓN DE ACTIVIDADES DEL PROCEDIMIENTO

FASE I: PLANIFICACIÓN

5.1 ACTIVIDAD 1: Contacto con el cliente

N°	RESPONSABLE	DESCRIPCIÓN	REFERENCIA
1	Auditor- Cliente	Establecer lugar y fecha de encuentro con el cliente	A. O. 1. 1
2	Auditor- Cliente	Registrar reunión inicial con el cliente	A. O. 1. 2
3	Auditor- Cliente	Identificar las partes interesadas responsables de rendir cuentas	A. O. 1. 3
4	Auditor- Cliente	Comprender el contexto externo del entorno a auditar	A. O. 1. 4
5	Auditor- Cliente	Comprender el contexto interno de la institución a auditar	A. O. 1. 5
6	Auditor- Cliente	Comprender estrategias y prioridades de la institución	A. O. 1. 6

- **Documento y/o Registro del proceso**: Acta de reunión y compromiso
- **Documentos y/o Registros de otros procesos o entes externos:** N/A

5.2 ACTIVIDAD 2: Entorno a auditar

N°	RESPONSABLE	DESCRIPCIÓN	REFERENCIA
7	Auditor- Cliente	Determinar los objetivos en base al estudio del entorno	A. O. 1. 7
8	Auditor- Cliente	Determinar el riesgo relevante del proceso de auditoría	A. O. 1. 8
9	Auditor- Cliente	Definir los riesgos organizacionales de la auditoría	A. O. 1. 9

- **Documento y/o Registro del proceso**: Documento plan preliminar.
- **Documentos y/o Registros de otros procesos o entes externos:** N/A

5.3 ACTIVIDAD 3: Equipo de auditoría

N°	RESPONSABLE	DESCRIPCIÓN	REFERENCIA
10	Auditor	Identificar miembros del equipo auditor	A. O. 1. 10
11	Auditor	Seleccionar miembros del equipo auditor	A. O. 1. 11
12	Auditor	Definir roles acordes a los conocimientos y habilidades de los miembros del equipo auditor	A. O. 1. 12

- **Documento y/o Registro del proceso**: Documento plan preliminar.
- **Documentos y/o Registros de otros procesos o entes externos:** N/A

5.4 ACTIVIDAD 4: Plan preliminar.

N°	RESPONSABLE	DESCRIPCIÓN	REFERENCIA
13	Auditor	Documentar plan preliminar	A. O. 1. 13
14	Auditor	Determinar antecedentes	A. O. 1. 14
15	Auditor	Determinar objetivos específicos de la auditoría	A. O. 1. 15
16	Auditor	Determinar el alcance de la auditoría	A. O. 1. 16
17	Auditor	Determinar recursos para la auditoría	A. O. 1. 17
18	Auditor	Determinar cronograma de la auditoría	A. O. 1. 18
19	Auditor	Determinar costos de la auditoría	A. O. 1. 19
20	Auditor	Documentar los riesgos de la auditoría	A. O. 1. 20
21	Auditor	Presentar plan preliminar al cliente	A. O. 1. 21
22	Auditor- Cliente	Acordar términos y condiciones de la auditoría	A. O. 1. 22

- **Documento y/o Registro del proceso**: Documento plan preliminar.
- **Documentos y/o Registros de otros procesos o entes externos:** N/A

5.5 ACTIVIDAD 5: Propuesta de auditoría.

N°	RESPONSABLE	DESCRIPCIÓN	REFERENCIA
23	Auditor	Elaborar la propuesta de auditoría	A. O. 1. 23

24	Auditor- Cliente	Presentar la propuesta de auditoría	A. O. 1. 24

- **Documento y/o Registro del proceso**: Documento de propuesta de auditoría.
- **Documentos y/o Registros de otros procesos o entes externos:** N/A

5.6 ACTIVIDAD 6: Contrato

N°	RESPONSABLE	DESCRIPCIÓN	REFERENCIA
25	Auditor- Cliente	Determinar cláusulas del contrato	A. O. 1. 25
26	Auditor	Elaborar el contrato	A. O. 1. 26
27	Auditor- Cliente	Firmar el contrato	A. O. 1. 27

- **Documento y/o Registro del proceso**: Contrato de auditoría
- **Documentos y/o Registros de otros procesos o entes externos:** N/A

FASE II: EJECUCIÓN

5.7 ACTIVIDAD 7: Plan de trabajo

N°	RESPONSABLE	DESCRIPCIÓN	REFERENCIA
28	Auditor	Diseñar y documentar el plan de trabajo	A. O. 1. 28

- **Documento y/o Registro del proceso**: Documento de plan de trabajo.
- **Documentos y/o Registros de otros procesos o entes externos:** N/A

5.8 ACTIVIDAD 8: Investigación de campo

N°	RESPONSABLE	DESCRIPCIÓN	REFERENCIA
29	Auditor	Definir instrumentos para la investigación de campo	A. O. 1. 29
30	Auditor	Elaborar instrumentos de investigación de campo determinados en el plan de trabajo	A. O. 1. 30
31	Auditor	Aplicar técnicas e instrumentos de auditoría	A. O. 1. 31
32	Auditor	Análisis y síntesis de información recopilada	A. O. 1. 32

- **Documento y/o Registro del proceso**: Checklist, encuesta, entrevista

- **Documentos y/o Registros de otros procesos o entes externos:** N/A

5.9 ACTIVIDAD 9: Informe final preliminar

N°	RESPONSABLE	DESCRIPCIÓN	REFERENCIA
33	Auditor	Definir hallazgos en base a la información y evidencias recopiladas	A. O. 1. 33
34	Auditor	Elaborar informe final preliminar	A. O. 1. 34

- **Documento y/o Registro del proceso**: Informe final preliminar
- **Documentos y/o Registros de otros procesos o entes externos:** N/A

FASE III: COMUNICACIÓN DE RESULTADOS

5.10 ACTIVIDAD 10: Informe final preliminar

N°	RESPONSABLE	DESCRIPCIÓN	REFERENCIA
35	Auditor- Cliente	Agendar fecha para presentación y discusión del informe final preliminar	A. O. 1. 35
36	Auditor- Cliente	Presentar informe final preliminar para discusión y validación	A. O. 1. 36

- **Documento y/o Registro del proceso**: Informe final preliminar aprobado.
- **Documentos y/o Registros de otros procesos o entes externos:** N/A

5.11 ACTIVIDAD 11: Informe final

N°	RESPONSABLE	DESCRIPCIÓN	REFERENCIA
37	Auditor	Elaborar informe final	A. O. 1. 37
38	Auditor- Cliente	Agendar fecha para presentación de informe final	A. O. 1. 38
39	Auditor- Cliente	Presentar informe final y documentos resultantes de la auditoría	A. O. 1. 39

- **Documento y/o Registro del proceso**: Informe final de auditoría aprobado.
- **Documentos y/o Registros de otros procesos o entes externos:** N/A

5.12 ACTIVIDAD 12: Cierre de contrato.

N°	RESPONSABLE	DESCRIPCIÓN	REFERENCIA
40	Auditor- Cliente	Cerrar el contrato	A. O. 1. 40
41	Auditor- Cliente	Retirar garantías	A. O. 1. 41

- **Documento y/o Registro del proceso**: Acta de reunión fin de proceso de auditoría.
- **Documentos y/o Registros de otros procesos o entes externos:** N/A

FASE IV: VALIDACIÓN

5.13 ACTIVIDAD 13: Calidad

N°	RESPONSABLE	DESCRIPCIÓN	REFERENCIA
42	Auditor- Cliente	Aplicar evaluación de calidad de resultados de auditoría	A. O. 1. 42

- **Documento y/o Registro del proceso**: Nivel de calidad de resultados de auditoría
- **Documentos y/o Registros de otros procesos o entes externos:** N/A

5.14 ACTIVIDAD 14: Seguridad de la información

N°	RESPONSABLE	DESCRIPCIÓN	REFERENCIA
43	Auditor- Cliente	Aplicar evaluación de seguridad de la información en las IES	A. O. 1. 43

- **Documento y/o Registro del proceso**: Nivel de seguridad de la información.
- **Documentos y/o Registros de otros procesos o entes externos:** N/A

5.15 ACTIVIDAD 15: Cumplimiento

N°	RESPONSABLE	DESCRIPCIÓN	REFERENCIA
44	Auditor- Cliente	Aplicar evaluación de cumplimiento de actividades de la auditoría	A. O. 1. 44

- **Documento y/o Registro del proceso**: Nivel de cumplimiento de actividades.
- **Documentos y/o Registros de otros procesos o entes externos:** N/A

5.16 ACTIVIDAD 16: Análisis de datos

N°	RESPONSABLE	DESCRIPCIÓN	REFERENCIA
45	Auditor	Data Mining	A. O. 1. 45

- **Documento y/o Registro del proceso**: Resultado de análisis de datos.
- **Documentos y/o Registros de otros procesos o entes externos:** N/A

FASE V: SEGUIMIENTO

5.17 ACTIVIDAD 17: Contacto con el auditado

N°	RESPONSABLE	DESCRIPCIÓN	REFERENCIA
46	Auditor- Cliente	Consulta directa al auditado	A. O. 1. 46

- **Documento y/o Registro del proceso**: Entrevista del auditado
- **Documentos y/o Registros de otros procesos o entes externos:** N/A

5.18 ACTIVIDAD 18: Informe final de auditoría

N°	RESPONSABLE	DESCRIPCIÓN	REFERENCIA
47	Auditor- Cliente	Verificación del informe final de auditoría	A. O. 1. 47

- **Documento y/o Registro del proceso**: Informe de seguimiento.
- **Documentos y/o Registros de otros procesos o entes externos:** N/A

6. DOCUMENTOS Y REGISTROS

DOCUMENTOS					
NOMBRE	ORIGEN		TIPO		ENCARGADO
	INT	EXT	IMP	DIG	
Actas de reunión	X		X		Auditor – Cliente
Informes de auditorías anteriores	X		X		Cliente
Plan preliminar	X			X	Auditor
Propuesta de auditoría	X			X	Auditor
Contrato	X		X		Auditor – Cliente
Plan de trabajo	X			X	Auditor
Checklist	X			X	Auditor
Encuesta	X			X	Auditor
Entrevista	X			X	Auditor
Hallazgos y evidencias	X		X		Auditor
Informe final de auditoría	X		X		Auditor - Cliente

7. FLUJOGRAMA