UNIVERSIDAD TÉCNICA DEL NORTE

Facultad de Ingeniería en Ciencias Aplicadas

Carrera de Ingeniería en Sistemas Computacionales

Comparación de modelos de control COSO y COBIT utilizados para auditorías informáticas para instituciones académicas de educación media de la ciudad de Ibarra

Trabajo de grado previo a la obtención del título de Ingeniero en Sistemas Computacionales

Autor:

Bryan Alexander Checa Guerrero

Director:

MSc. Daisy Elizabeth Imbaquingo Esparza

Ibarra – Ecuador

2024

UNIVERSIDAD TÉCNICA DEL NORTE
BIBLIOTECA UNIVERSITARIA

AUTORIZACIÓN DE USO Y PUBLICACIÓN A FAVOR DE LA UNIVERSIDAD TÉCNICA DEL NORTE

1. IDENTIFICACIÓN DE LA OBRA

En cumplimiento del Art. 144 de la Ley de Educación Superior, hago la entrega del presente trabajo a la Universidad Técnica del Norte para que sea publicado en el Repositorio Digital Institucional, para lo cual pongo a disposición la siguiente información:

DATOS DE CONTACTO			
CÉDULA DE IDENTIDAD:	1004079453		
APELLIDOS Y NOMBRES:	Checa Guerrero Bryan Alexander		
DIRECCIÓN:	Ibarra		
EMAIL:	bachecag@utn.edu.ec		
TELÉFONO FIJO:		**TELÉFONO MÓVIL:**	0959843913

DATOS DE LA OBRA	
TÍTULO:	Comparación de modelos de control COSO y COBIT utilizados para auditorías informáticas para instituciones académicas de educación media de la ciudad de Ibarra
AUTOR (ES):	Bryan Alexander Checa Guerrero
FECHA: DD/MM/AAAA	14 de febrero de 2024
SOLO PARA TRABAJOS DE GRADO	
PROGRAMA:	■ **PREGRADO** ☐ **POSGRADO**
TITULO POR EL QUE OPTA:	Ingeniero en sistemas computacionales
ASESOR /DIRECTOR:	MSc. Daisy Elizabeth Imbaquingo Esparza

2. CONSTANCIAS

El autor (es) manifiesta (n) que la obra objeto de la presente autorización es original y se la desarrolló, sin violar derechos de autor de terceros, por lo tanto la obra es original y que es (son) el (los) titular (es) de los derechos patrimoniales, por lo que asume (n) la responsabilidad sobre el contenido de la misma y saldrá (n) en defensa de la Universidad en caso de reclamación por parte de terceros.

Ibarra, a los 14 días del mes de febrero de 2024

EL AUTOR:

Bryan Checa

CERTIFICACION DIRECTOR DEL TRABAJO DE TITULACIÓN

Ibarra, 14 de febrero de 2024

MSc. Daisy Elizabeth Imbaquingo Esparza

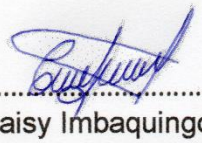
DIRECTORA DE TRANAJO DE TITULACIÓN

CERTIFICA:

Que el trabajo de titulación "COMPARACIÓN DE MODELOS DE CONTROL COSO Y COBIT UTILIZADOS PARA AUDITORÍAS INFORMÁTICAS PARA INSTITUCIONES ACADÉMICAS DE EDUCACIÓN MEDIA DE LA CIUDAD DE IBARRA" previo a la obtención del titulo de Ingeniero en Sistemas Computacionales ha sido desarrollado y terminado en su totalidad por el Sr. Checa Guerrero Bryan Alexander, con cedula de identidad numero 1004079453, bajo mi supervisión.

Es todo cuanto pudo certificar en honor a la verdad.

Atentamente,



.....

Ing. Daisy Imbaquingo MSc.

C.I.: 1002873048

AGRADECIMIENTO

En primer lugar, agradezco a Dios por permitirme culminar esta etapa de mi vida.

Agradezco a mis padres por el sacrificio, apoyo, paciencia y amor que me brindan para poder formarme como persona. De igual manera a mi hermano y mi hermana por su forma de ser.

A mi tutora MSc. Daisy Imbaquingo, estaré infinitamente agradecido por brindarme el soporte necesario como docente para culminar esta etapa de la mejor manera.

Gracias a toda mi familia por el apoyo incondicional, consejos y por sus ocurrencias que alegran nuestros días.

Finalmente agradecer a todos los buenos amigos que he conocido en esta bella etapa universitaria.

DEDICATORIA

Este trabajo está dedicado a mis padres Doris y Patricio por su apoyo incondicional para poder culminar esta etapa, por su sacrificio son mi motivo y fuerza para superarme.

A la persona que siempre estuvo durante esta etapa de igual manera quiero dedicar este logro Alison Martínez tu apoyo y cariño incondicional fue de gran ayuda poder cumplir este objetivo.

Finalmente, también va dedicado a todas las personas que confiaron en mí.

Bryan Checa

ÍNDICE

ÍNDICE DE FIGURAS

ÍNDICE DE TABLAS

ÍNDICE DE ANEXOS

RESUMEN

Las instituciones de Educación media de la ciudad de Ibarra utilizan distintos sistemas informáticos para realizar actividades como ingreso de notas, matriculas, planificaciones, consultas, entre otras; es por ello imprescindible realizar un análisis de los diferentes recursos tecnológicos (TI) de la institución para evaluar la seguridad y el estado en que se encuentran; principalmente del departamento de informática, ya que es el área utilizada para realizar estos procedimientos por docentes y estudiantes. Sin embargo, la evidencia de efectuar un proceso de auditoría informática en estas instituciones es limitada, principalmente por el desconocimiento de las metodologías, procesos o modelos de control que pueden ser aplicados en una auditoría, por lo que el propósito de la presente investigación es realizar un análisis bibliográfico acerca del proceso de auditoría y sus modelos de control como COSO y COBIT, los cuales son comparados en base a métricas como propósito, supervisión y monitoreo, seguridad de la información y adaptación, para determinar el modelo de control más apropiado para ser utilizado en una auditoría informática por las instituciones de educación media. Como resultado se obtiene que entre COSO y COBIT existe una superposición que permite que sus diferencias complementen en el entorno de TI, por lo que se propone una guía estandarizada bajo los dos marcos referenciales para un proceso de auditoría del departamento de informática de las instituciones de educación media, guía que es validada por el método Delphi.

Palabras clave: Auditoría informática, Modelos de control, Control interno, COSO, COBIT, Guía, Método Delphi, Institución de educación media.

ABSTRACT

In Ibarra, the institutions from secondary education use different informatics systems to do activities such as: entering grades, enrollment, planning, consultation, and others; It is therefore essential to carry out an analysis of the different technological resources (IT) of the institutions to assess their security and their status; mainly from the IT department, since it is the area used to carry out these procedures by teachers and students. However, the evidence of carrying out a computer audit process in those institutions is limited, it is because of the lack of knowledge involving methodologies, processes or control models that can be applied in an audit, so the main purpose of this research is to carry out a bibliographical analysis about the audit process and its control models such as COSO and COBIT, which are compared based on metrics, purpose, supervision and monitoring, information security and adaptation, to determine the most appropriate control model to be used in a computer audit by secondary education institutions.

As a result, it was evidenced that there is an overlap between COSO and COBIT that allows their differences to complement each other in the IT environment, for which a standardized guide is proposed under the two reference frameworks for an audit process of the IT department from secondary education institutions, this guide is validated by the Delphi method.

***Keywords*:** Informatics audit, Control models, Internal control, COSO, COBIT, Guide, Delphi Method, Secondary Education Institution.

INTRODUCCIÓN

Antecedentes

La auditoría desde sus orígenes ha tenido como base el análisis de la información de hechos económicos, situaciones y acontecimientos pasados. Durante el siglo XIX antes de la revolución industrial en los años 50 la auditoría cumplía dos funciones: controlar la eficacia de aplicar las políticas de una empresa y recomendar las normas adecuadas para el mejoramiento de algunos procesos (Biler-Reyes, 2017). En Estados Unidos las empresas comenzaron a expandirse y surgió la necesidad de instaurar herramientas que se enfoquen en el descubrimiento de fraudes y responsabilidad financiera (Silva & Mata, 2015)

Con el surgimiento de la industria al final del siglo XIX, los sistemas informáticos no existían y las actividades eran realizadas de forma manual un riesgo de manipulación de la información; por lo que se vio la necesidad de vigilar las operaciones financieras de las compañías tanto a nivel interno y externo. Desarrollándose nuevos sistemas de supervisión, gestión y control de riesgos (Chuquimarca et al., 2020).

Varias corporaciones estuvieron involucradas en prácticas cuestionables, despertando la preocupación de algunos legisladores a cerca de la importancia del control interno (Luna, 2013). Estas compañías se internacionalizaron y vieron la necesidad de emitir informes de la situación de la empresa, los datos generados eran de mayor complejidad y resultaba imposible realizarlo de manera manual; por lo que era necesario el uso de herramientas tecnológicas (Chuquimarca et al., 2020), desarrollándose programas y aplicaciones a través de ordenadores que permitan tener el control de los datos de una institución originándose la auditoría operativa de proceso de datos (Florian, 2015).

La auditoría permite que exista un adecuado manejo de los datos y sistemas informáticos garantizando su confidencialidad, disponibilidad e integridad a través de metodologías de control interno como son COBIT 5 y COSO III (Sendón et al., 2020).

Situación actual

En el Ecuador las instituciones educativas para el manejo de los datos utilizan diferentes sistemas informáticos los cuales se encargan de realizar algunos procedimientos como: matriculas, ingreso de notas, pagos, entre otros (Jafeth & Mosquera, 2018). En los últimos años se han visto involucrados en problemas de seguridad (Baldeón & Coronel, 2012) plantean que desde el año 2002 las instituciones educativas del Ecuador han sufrido 308 ataques informáticos exitosos de sus sitios web.

La evidencia acerca de la realización de auditorías a los sistemas informáticos a las instituciones de educación media es limitada por lo que existe un alto grado de desconocimiento del uso de un método de control interno lo cual impide establecer una línea base que permita el mejoramiento en sus sistemas informáticos, por eso, es importante conocer los modelos que se adaptan para la ejecución de auditorías (Giraldo, 2015).

Prospectiva

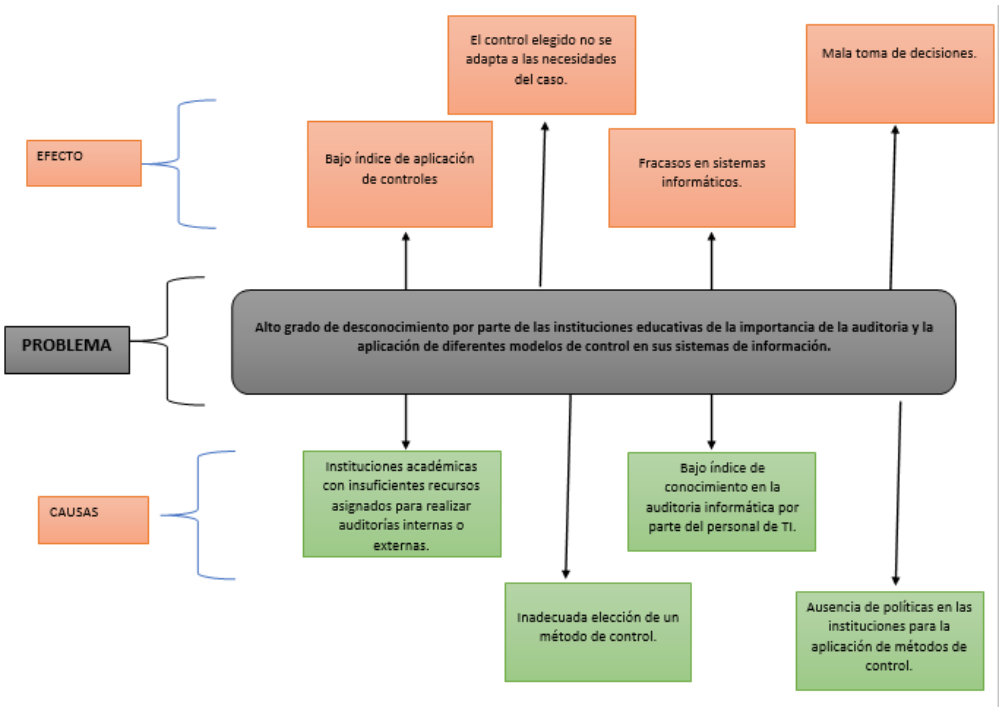
Mediante la investigación del trabajo de titulación basado en la comparación de métodos de control COSO III y COBIT 5 facilitará a las instituciones académicas de educación media de la ciudad de Ibarra elegir el modelo de control más apropiado para evitar fallos en los sistemas de información y una adecuada toma de decisiones en cuanto a seguridad informática.

Planteamiento del problema

Las instituciones educativas no llevan un modelo de control adecuado de auditoría informática, debido a la dificultad de elegir el modelo de control más apropiado por lo cual existe una alta probabilidad de fallos en los sistemas informáticos, pudiéndose detectar problemas como: duplicidad de trabajo, filtración de datos personales, robo y cambio de información, retrasos en los procesos académicos desencadenando en un fracaso institucional.

Figura 1.

Árbol de problemas.



Nota. Elaboración propia. Árbol de problemas con causas y efectos de la importancia de la auditoria y la elección de un modelo de control.

Objetivos

Objetivo general

Comparar entre modelos de control COSO y COBIT utilizados en auditorías informáticas para instituciones académicas de educación media para la ciudad de Ibarra.

Objetivos específicos

- Estudiar el modelo COSO y COBIT para fortalecer el conocimiento e importancia de la aplicación de un método de control en las auditorías informáticas.
- Comparar las metodologías de COSO y COBIT en base a métricas comparativas.
- Proponer una guía de lineamientos del método de control más adecuado en auditorías informáticas para las instituciones académicas de educación media en la ciudad de Ibarra.

- Validar los resultados, mediante una encuesta dirigida a conocedores del tema que permita conocer el grado de aceptación de la investigación.

Alcance

La presente investigación tuvo como finalidad realizar una comparación sobre los modelos de control COSO III y COBIT 5 que son utilizados en auditorías informáticas a través de una recopilación bibliográfica de diferentes bases de datos, la información obtenida sirvió como pauta para establecer métricas que permitieron comparar estos dos modelos para conocer sus similitudes y diferencias. Posteriormente se diseñó una guía con lineamientos que orienten a las instituciones académicas de educación media de la ciudad de Ibarra a elegir entre los dos modelos al más adecuado de acuerdo con sus necesidades al realizar una auditoría informática.

Justificación

El presente estudio tuvo un enfoque en los Objetivos de Desarrollo Sostenible planteados por la ONU y la UNESCO en su literal Nro 9: “Crear infraestructura resistente, fomentar la industrialización inclusiva y sostenible y promover la innovación".

Para el cumplimiento de este objetivo, se establecen metas que son cumplidas en la investigación.

9.4 Para 2030, modernizar la infraestructura y transformar las industrias para hacerlas sostenibles, utilizar los recursos de manera más eficiente y promover la introducción de tecnologías y procesos industriales y amigables con el medio ambiente, así como lograr que todos los países actúen de acuerdo con sus respectivas capacidades (Parra, 2018).

9.5 Fortalecer la investigación científica y la capacidad tecnológica del sector industrial en todos los países, especialmente en los países en desarrollo, mediante la promoción de la innovación y el aumento de personas que trabajan en investigación y desarrollo para el 2030, el número de personas que trabajan en investigación y desarrollo por millón de habitantes y los gastos de los sectores público y privado en investigación y desarrollo.

9b. Apoyar el desarrollo, la investigación y la innovación de tecnología nacional en los países en desarrollo, incluida la garantía de un entorno normativo propicio para la diversificación industrial y la creación de valor comercial. (Parra, 2018).

Justificación Metodológica. - El proyecto se desarrolló bajo un enfoque cualitativo porque gracias a este enfoque se recopiló información bibliográfica y análisis documentales que acompañados de un método deductivo y comparativo se consiguió llegar a nuestros resultados y conclusiones (Prieto, 2018).

Una vez analizado los controles se tuvo una metodología aplicada, la misma que se vio reflejada en una guía para que las instituciones educativas a las cuales nos dirigimos puedan tomar como referencia este estudio para su beneficio.

Justificación Tecnológica. - El desarrollo de sistemas informáticos ha sido clave en el desarrollo de instituciones, los sistemas han ido evolucionando cada vez en busca de aumentar beneficios, y las formas de auditar han sido modificadas en función de las necesidades que se van presentando (León et al., 2018). Por ello, se vio la necesidad de implementar una guía de referencia para que las instituciones académicas de educación media de la ciudad de Ibarra puedan elegir un modelo de control adecuado en sus auditorías informáticas.

CAPÍTULO 1

Marco Teórico

Auditoría

La auditoría es un proceso ordenado para conseguir, consultar, verificar y evaluar evidencias de forma objetiva mediante documentación e información distintas actividades de la organización (Manrique, 2019).

Este procedimiento siempre está a cargo de un individuo o un grupo de auditores que deben ser profesionales, certificados para que puedan desempeñar sus funciones en las diferentes áreas. El objetivo de la auditoría es procurar de conceder de la máxima transparencia a la información que suministra la empresa a todos los usuarios de la misma empresa u organización (Méndez, 2017).

Con los conceptos mencionados se puede concluir que la auditoría es un proceso mediante el cual personas certificadas conocidos como auditores verifican el funcionamiento correcto de una entidad para controlar puntos débiles que pueden llegar a afectar a futuro además de brindar recomendaciones para mejorar los aspectos evaluados.

Tipos de Auditoría

Existen varias clasificaciones sobre los tipos de auditoría, pero en este caso vamos a tratar dos de las cuales son las más importantes. Existe la auditoría interna y la auditoría externa (Manrique, 2019)

Además de este tipo de auditorías existen diferentes áreas en las cuales se puede aplicar una auditoría tales como son: auditorías financieras, auditorías informáticas, auditorías de gestión, entre otros (Montes Villanueva, 2018).

Auditoría interna. La auditoría interna es un control que se lleva a cabo por el personal de la empresa y su objetivo es garantizar que las operaciones se efectúen de acuerdo con la política general de la entidad, evaluando la eficacia y la eficiencia, además de proponer soluciones a las dificultades detectadas (Ramos, 2018).

Auditoría externa. La auditoría externa es llevada a cabo por un profesional independiente el cual no debe poseer un vínculo estrecho con la empresa, tiene como objetivo determinar y ofrecer un criterio acerca del sistema de información de la organización y plantear asimismo el mejoramiento de algunas técnicas (Bendermacher, 2017).

Las personas que ejecutan estos dos tipos de auditorías son conocidas como auditores, los cuales poseen algunas diferencias respecto al tipo de auditoría que realiza, estas auditorías son mostradas en la Tabla 1.

Tabla 1.

Diferencias entre auditor externo e interno

Auditor externo	**Auditor interno**
Es un profesional independiente y reconocido con soluciones y formación documentada.	Mantiene una relación laboral de dependencia con la empresa
Emite dictamen.	Capacidad profesional certificada con titulación académica.
Asume responsabilidad frente a terceros: penal, civil y profesional.	Comunica y recomienda.
Examina los estados contables y pronuncia opinión sobre su razonabilidad.	Registra frente a la organización de que depende, del trabajo cumplido.
Se acoge y lo ampara el secreto profesional.	Priva de normas generalmente aceptadas; las crean las organizaciones en función de los objetivos.
Emplea principios y normas generalmente aceptados.	Valora el sistema de control interno y plantea mejoras para la conquista de objetivos.
Expone un informe breve y sintético, según formatos preestablecidos.	Solo depende de su propia ética profesional.
Cumple su actividad metódicamente y en cortos periodos de tiempo.	Ejecuta su actividad de forma continuada durante todo el ejercicio contable.
El informe tiene efectos frente a terceros	Emite informes extensos y descriptivos del control interno, con propuestas de mejora.
	El informe es de utilidad interna.

Nota. Adaptado de Méndez, H. (2017). La auditoría: concepto, clases y evolución. En Auditoría, grado Superior (McGraw Hill, Vol. 1).

Auditoría informática

En la actualidad la mayoría de las instituciones han implementado diferentes sistemas informáticos. Para ello es importante realizar una evaluación de los mismo a través de una revisión técnica y especializada, para obtener una opinión profesional acerca de la operatividad eficiente de acuerdo con las normas establecidas (Fernández & Caycedo, 2017).

Autores como Muñoz (2012) menciona que la auditoría informática depende de cada institución o departamento siendo particular de acuerdo con el fin que se quiere alcanzar, sin embargo, algunas técnicas y procedimientos son compatibles. El conjunto de estos procedimientos, tienen el objetivo de verificar, analizar y evaluar que los servicios informáticos estén funcionando correctamente con seguridad y eficacia.

Es decir que la auditoría informática se basa en una revisión de los diferentes sistemas, así como instalaciones y equipos informáticos en los cuales se aplica diferentes procedimientos para evaluar su uso adecuado y buscar soluciones a diferentes falencias que puedan existir durante el proceso de auditoría.

El propósito principal de la auditoría informática es determinar las fortalezas y debilidades de los diferentes sistemas de información, es decir todo aquello donde exista la aplicación de las TICS en la institución, Muñoz (2012) establece los diferentes objetivos que son:

- El personal del área en sistemas debe estar capacitado y realizar una evaluación para elaborar un informe acerca de la razonabilidad de la gestión interna y operaciones del sistema del área informática (Muñoz, 2012).
- Evaluar el uso, sus equipos, periféricos e instalaciones, también de sus recursos técnicos para el procesamiento de la información (Muñoz, 2012).
- Evaluar sus sistemas operativos, paqueterías de instalación y desarrollo e instalación de nuevos sistemas (Muñoz, 2012).

- Evaluar al personal y usuarios, para determinar el cumplimiento de los diferentes programas y políticas de acuerdo con las regulaciones establecidas para los sistemas de información (Muñoz, 2012).

Por lo tanto, la auditoría informática tiene como objetivo verificar los diferentes sistemas informáticos, también evaluar el cumplimiento de las diferentes normas establecidas por la institución y comprobar que los diferentes equipos informáticos tengan un buen uso y manejo con la finalidad de implementar alternativas que mejoren el rendimiento tecnológico.

Etapas de la Auditoría informática

Las fases de la auditoría informática son similares a las de cualquier auditoría únicamente varía el objeto de estudio. Para llevar a cabo una auditoría informática autores como Nuñez (2014)establece que las principales fases de la auditoría informática son las siguientes:

- *Planificación*: es una fase de análisis preliminar para conocer la situación actual de la institución, de cómo se encuentra lo sistemas informáticos, equipos y otros elementos. En esta fase es necesario conocer cuáles son los objetivos y el alcance de la auditoría, el análisis de los riesgos existentes como: inherente, de control y detección, determinación de puntos críticos y se elabora un informe de planeación de la auditoría. También se aplica diferentes cuestionarios de control interno para conocer las fallas que sirven como indicador de que no se está operando correctamente (Pin, 2020).
- *Ejecución*: en esta etapa se lleva a cabo lo planificado en el informe de planeamiento, a través de la recopilación de documentos que permitan al auditor emitir recomendaciones, comentarios acerca de las TI. El objetivo principal es obtener la mayor información a través de entrevistas, cuestionarios, análisis de auditorías anteriores (Pin, 2020).La información recolectada se clasifica para que sea más fácil su acceso y posteriormente permita justificar los comentarios y recomendaciones proporcionados durante la auditoría (Pin, 2020).

Es decir, en esta etapa se obtiene la información suficiente que respalde al informe final proporcionado por el auditor,

- *Informe final*: en base a la información recolectada se analiza los resultados encontrados durante la auditoría para llegar a una conclusión general para conocer la situación informática de la institución (Pin, 2020). El informe presentado debe ser claro y adecuado mostrando las recomendaciones suficientes de los hallazgos encontrados durante la auditoría.

Riesgo

Definición de Riesgo

El riesgo es un factor o incidente que interfiere con el cumplimiento de los objetivos planteados en una institución, es decir, existe la posibilidad de pérdidas, provocando un resultado indeseado como consecuencia (Chávez, 2018).

Para Piattini (2016) el riesgo es la probabilidad de que una amenaza suceda por la falta de uno o varios controles, se puede amenorar con un análisis previo de las vulnerabilidades al analizar el entorno.

Riesgo informático

El continuo uso de las herramientas y aplicaciones tecnológicas han dado origen a los riesgos dentro de esta área, ya que las organizaciones están siendo atacadas por falta de protección en sus datos o su constante cambio (Pérez et al., 2018).

El riesgo informático hace referencia a los daños y pérdidas que logren presentarse debido a eventos relacionados al acceso y uso de la tecnología (Granda et al., 2017). Estos riesgos se forman durante el funcionamiento de cualquier actividad y tienen graves consecuencias para las personas, la propiedad, la infraestructura y todo lo que relacione a la organización (Pérez et al., 2018).

Los riesgos informáticos o tecnológicos son fenómenos que en su mayoría pueden ser controlados por una o varias personas. El impacto de este riesgo se debe a la alta

vulnerabilidad que puede tener en sus sistemas, en su mayoría esto se debe a la falta de controles que se deben aplicar (Zambrano & Valencia, 2017).

Gestión de Riesgos

El éxito de la gestión de una institución se enfoca en la dirigencia y control de los procesos que tiene como fin mejorar y cumplir los objetivos planteados, a través de una adecuada gestión de riesgos (Ministerio de Finanzas, 2017), para ello las organizaciones deben:

- **Identificar riesgos:** se debe determinar los eventos que pueden influir en el cumplimiento de los objetivos planteados en una institución, ya sea a través de mapas de riesgo considerando los factores internos y externos; es decir, se identifican los riesgos más importantes que enfrenta una entidad para el cumplimiento de sus objetivos (Consejo de Auditoría Interna del Gobierno de Chile, 2016)
- **Evaluación de riesgos:** permite valorar los riesgos de acuerdo con su magnitud teniendo en cuenta dos perspectivas: la probabilidad e impacto de ocurrencia. Se utilizan diferentes técnicas de valoración para su análisis ya sean cuantitativos o cualitativos (Basantes et al., 2016).
- **Tratamiento de los riesgos:** en esta etapa se analiza las diferentes medidas que se pueden aplicar para prevenir o mitigar los riesgos. Se establecen diferentes medidas como para el control y financiación del riesgo (Jara Pérez, 2018). El tratamiento de riesgo debe garantizar un funcionamiento eficiente y efectivo de la institución, realizar controles internos de acuerdo con las leyes y reglamentos vigentes (Imbaquingo, 2017).
- Las estrategias principales de control de riesgo son:

1. Evitar: minimizar la posibilidad que se produzca un riesgo a través de transferencia, elución, reducción y diversificación (Minchala, 2016).
2. Prevenir: establecer con anterioridad políticas, procedimientos que eviten la ocurrencia del riesgo, utilizando diversas formas de prevención como mantenimiento

preventivo, inspecciones y pruebas de seguridad continua, inversión en sistemas de información, entre otros (Minchala, 2016).

3. Proteger: son las medidas tomadas en caso de que el riesgo se presente, las cuales deben disminuir el impacto de este, con la aplicación de los planes de contingencia o emergencia (Minchala, 2016).

- Las medidas de tratamiento para la financiación de riesgo son:

1. Aceptar: es asumir el riesgo, así como las consecuencias que se produzcan por ello; los riesgos que se aceptan principalmente son los de impacto leve (Minchala, 2016).
2. Retener: se detiene la producción del riesgo por las posibles pérdidas que puede causar el asumirlo (Minchala, 2016).
3. Transferir: se transfiere al riesgo cuando se traspasa a otra institución (Minchala, 2016).
4. Monitoreo y evaluación de riesgos: se debe adaptar los procesos de acuerdo con las nuevas exigencias o riesgos encontrados utilizando herramientas como indicadores de riesgo y autoevaluación (Londoño & Nuñez, 2010).

Seguridad de la Información

Actualmente la tecnología se ha convertido en algo indispensable para las personas por el hecho de que en su mayoría se utilizan artefactos tecnológicos para acceder y estar conectados a la red, esto puede ir desde trabajo desde un ordenador, clases en línea desde un dispositivo móvil o incluso acceder a cuentas de correo electrónico desde dispositivos inteligentes (Figueroa-Suárez et al., 2018).

Si bien la tecnología nos permite ser más productivos y acceder a cantidades masivas de información con un solo clic, también trae consigo algunos problemas de seguridad (Vega, 2021). Un claro ejemplo puede ser el mal uso o manejo de información de cuentas bancarias porque con esta información los ciberdelincuentes pueden ocasionar graves problemas como fraudes por suplantación de identidad, compras sin autorización, débitos, etc. La entidad financiera puede verse involucrada en varias demandas por el mal manejo de la información

y la falta de controles, además de perder credibilidad en sus clientes (Figueroa-Suárez et al., 2018).

Según la ISO/IEC (2016) la seguridad de la información se puede definir como los procesos, las buenas prácticas y las metodologías con el propósito de salvaguardar la información y los sistemas de información del acceso, uso, divulgación, interrupción, modificación, alteración o destrucción no autorizados; es decir, que se debe proteger los datos y recursos de la infraestructura tecnológica de aquellos individuos que intentan hacer mal uso de ellos.

Dentro de la norma ISO 2700 plantea los siguientes objetivos para la seguridad de la información:

- **Integridad**: la información debe mostrarse en su forma original, es decir, no puede ser manipulada, copiada o alterada sin que no haya previa autorización (J. Jácome et al., 2017).
- **Confidencialidad**: garantiza que únicamente las personas o entidades autorizadas tengan el acceso a sus datos o información que además no deben ser divulgados por dichas personas (ISO/IEC, 2016).
- **Disponibilidad**: se debe garantizar que el acceso a la información o datos debe estar disponible en todo momento para las personas que lo requieran (ISO/IEC, 2016).

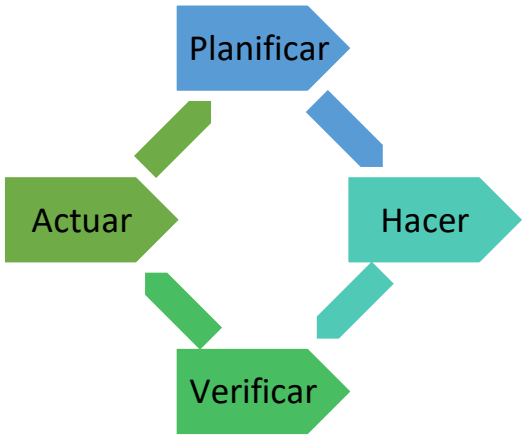
Gestión de la Información

En general se entiende la seguridad como un proceso en constante uso ya que se dice que los riesgos nunca se eliminan, pero se pueden gestionar (Calderón, 2018). Los Sistemas de Gestión de Seguridad de la Información o también conocidos como SGSI se encargan de generar políticas para la administración de la información y en general se basan en cuatro niveles que están en constante mejora, estos niveles son los mostrados en la Figura 2:

- **PLANIFICAR (Plan):** se define en establecer el contexto, en él se crean las políticas de seguridad, se realiza el análisis de riesgos, se forma la selección de controles y el estado de aplicabilidad (ISO, 2013).
- **HACER (Do):** consiste en implementar el sistema de gestión de seguridad de la información, efectuar el plan de riesgos y realizar los controles (ISO, 2013).
- **VERIFICAR (Check):** se debe hacer auditorías internas y monitorear las actividades (ISO, 2013).
- **ACTUAR (Act):** consiste en realizar tareas de mantenimiento, propuestas de mejora, acciones correctivas y preventivas (ISO, 2013).

Figura 2.

Proceso de la gestión de la información



Nota. Elaboración propia. Proceso de los cuatro pasos para la gestión de la información.

Control Interno

Definición Control Interno Informático

Hoy en día, la tecnología y la información son recursos indispensables dentro de las organizaciones porque gracias a estos elementos los directivos pueden tomar las mejores decisiones por los datos que obtienen (A. Jácome et al., 2019). Para poder tener una buena administración se debe poseer un amplio conocimiento acerca de los riesgos que implican el manejo de TI, para ello es necesario aplicar los controles necesarios dentro de la organización (Aguirre, 2015).

Según el marco de trabajo COBIT el control se define como las políticas, prácticas, procedimientos y estructura organizacional que está diseñada para abastecer seguridad de que los objetivos de negocios sean alcanzados y los eventos indeseados sean detectados y corregidos (ISACA, 2012b).

Según el marco de trabajo COSO el control interno se define como un proceso deseñado que se encarga de adjudicar seguridad en efectividad y eficiencia en las operaciones, reportes, regulaciones y cumplimiento de ley (Gonzales, 2013).

Con los conceptos mencionados anteriormente se puede llegar a concluir que el control interno informático es un sistema que está integrado al proceso administrativo, planeación, organización y control de las operaciones con el fin de proteger los recursos informáticos para mejorar en el cumplimiento de sus objetivos, además de mejorar los procesos automatizados.

Objetivos del Control Interno

Varios autores afirman que el objetivo general del control interno informático es controlar todas las actividades que relacionen a los sistemas de información automatizados, esto siempre cumpliendo con las normas, estándares y disposiciones que dispone la ley (Aguirre, 2015).

Además, entre sus objetivos también podemos destacar:

- La protección de los activos como: datos, hardware y software.
- Conservar la precisión y la integridad de los datos.
- Cumplimiento de normas legales e internas de la organización.
- Fiabilidad en los procesos y eficacia en el uso de los recursos (Aguirre, 2015).

Componentes del Control Interno

Dentro del marco integrado COSO se identifican cinco elementos de control interno (Figura 3) que están interrelacionados, además deben estar presentes en todos los sistemas de control de las organizaciones.

Figura 3.

Componentes del Control Interno

Nota. Adaptado de COSO. (2013). Componentes del Control Interno.

Modelos de control interno de la auditoría informática

Modelo COSO III

Generalidades. Comité de organizaciones patrocinadoras de la Comisión Treadway o mejor conocido por sus siglas en inglés “COSO” (Committee of Sponsoring Organizations of Treadway Commission) es una organización conformada por entidades privadas establecidas en Estados Unidos en el año 1985. Tienen como objetivo identificar las causas de la presentación de información financiera engañosa o fraudulenta y hacer recomendaciones que aseguren la máxima transparencia de la información (Gonzales, 2013).

COSO se dedica a desarrollar marcos y pautas generales para el control interno, la gestión de riesgos corporativos y la prevención del fraude, diseñados para mejorar el desempeño operativo y de supervisión de una organización (COSO, 2013).

Objetivos y componentes. Los objetivos deben complementarse entre sí, estar interrelacionados y ser consistentes con las capacidades y expectativas de la organización.

La definición de objetivos es un requisito previo para un control interno eficaz (Committee of Sponsoring Organizations of the Treadway Commission, 2013).

El Marco Integrado de Control Interno identifica tres tipos de objetivos que permiten a una organización enfocarse en diferentes aspectos de acuerdo con el (Committee of Sponsoring Organizations of the Treadway Commission (2013), como son:

Objetivos operativos: estos objetivos están relacionados con el logro de la misión y visión de la organización. Estos objetivos forman la base para evaluar los riesgos asociados con la protección de los activos de la entidad.

Reflejan el entorno empresarial, industrial y económico en el que está la entidad; además, está relacionado con la mejora del desempeño financiero, productivo, innovador, de calidad y satisfacción con su personal.

- *Objetivos de información:* hacen referencia a la preparación de reportes para uso de la organización tomando en cuenta la transparencia, veracidad y oportunidad. Dichos reportes hacen referencia a información financiera y no financiera interna y externa.

  Los informes externos cumplen con las regulaciones y estándares. Los informes internos satisfacen las necesidades dentro de la organización.
- *Objetivos de cumplimiento:* está relacionado con el cumplimiento de la ley y normativa que debe seguir la organización.

Dentro de los cinco componentes que plantea COSO que a su vez están integrados y relacionados con los objetivos de la empresa tenemos los mostrados en la Figura 4:

Figura 4.

Objetivos y componentes COSO III.

Nota. Obtenido de *Relación entre objetivos y componentes* (p. 6), por COSO (2013), Control Interno-Marco Integrado.

- *Entorno de control:* es el entorno en donde se llevan a cabo las actividades organizacionales con la supervisión de la administración. Este entorno es influenciado por factores internos y externos como la historia, los valores, la competitividad y regulación; además, comprende las reglas, procesos y estructuras que forman la base para el desarrollo del control interno de una organización (Gonzales, 2013).

  Este componente se encarga de crear disciplina dentro de la institución para generar un apoyo al cumplimiento de sus objetivos. Para lograr un entorno de control oportuno se debe tomar en cuenta aspectos como la estructura organizacional, la asignación de responsabilidades, el compromiso y finalmente una buena gerencia (Alayo, 2016).

  Al no tener un entorno de control eficaz se puede llegar a producir graves consecuencias negativas en la institución; por ello, este componente es uno de los más importantes porque es la base para que los otros componentes funcionen y tengan una buena estructura (Quinaluisa Morán et al., 2018).

- *Evaluación de los riesgos:* este componente se encarga de identificar los posibles riesgos que puedan afectar al cumplimiento de los objetivos de la institución. Toda institución debe hacer frente al conjunto de riesgos que se le presentan ya sean internos o externos (Quinaluisa Morán et al., 2018).

  Los riesgos pueden llegar a afectar en diferentes sentidos como en su imagen con la sociedad, su habilidad para competir y su estabilidad financiera.

La institución u organización debe anticipar, conocer y responder a los riesgos a los que se enfrenta, para establecer mecanismos para su identificación, análisis y mitigación (Alcedo, 2018).

- *Actividades de control:* se definen como acciones establecidas que mediante políticas y procedimientos ayuden a garantizar que se lleven a cabo acciones para reducir los riesgos que tienen un impacto potencial en los objetivos.

  Estas actividades deben ser efectuadas en todos los niveles de la organización. Se pueden llegar a clasificar en controles detectivos y preventivos (COSO, 2013).

  Las actividades que se realicen dentro de este campo deben estar orientadas a mitigar los riesgos que obstaculizan la ejecución de los objetivos generales de la organización (Dickins & Fay, 2017). Los controles permiten:

1. Evitar riesgos innecesarios.
2. Minimizar el impacto de las consecuencias.
3. Restablecer el sistema lo antes posible.

- *Sistemas de información y comunicación:* la información es indispensable para que la organización lleve a cabo las responsabilidades de control interno que apoyen al cumplimiento de sus objetivos (Moeller, 2013).

  El personal no solo debe capturar información, sino también comunicarse para desarrollar, administrar y controlar sus operaciones. Por lo tanto, este componente trata sobre cómo se identifica, obtiene y comparte información las áreas operativas, de gerencia y financieras de una institución (Dickins & Fay, 2017).

  Es de vital importancia que la administración disponga de datos confiables al momento de planificar y realizar actividades dentro de la organización.

  La comunicación es el proceso continuo e iterativo de proporcionar, intercambiar y obtener información necesaria, relevante y de calidad. Esta comunicación puede llegar a ser interna o externa. La comunicación interna hace referencia a toda la información que se difunde dentro de la institución en todos los niveles de forma ascendente o descendente. La comunicación externa tiene dos propósitos: transmitir

información externa relevante de afuera hacia dentro de la organización y proporcionar información interna relevante de adentro hacia afuera, y satisfacer las necesidades y expectativas de las partes interesadas (Dickins & Fay, 2017).

- *Actividades de monitoreo y supervisión:* se debe monitorear todo el proceso para incorporar el concepto de mejora continua; Asimismo, el sistema de control interno debe ser flexible para responder con rapidez y adaptarse a las circunstancias. Estas actividades están encargadas de evaluar si los componentes y principios están presentes y funcionando en la institución(Moeller, 2013).

  Es trascendental establecer procedimientos que se encarguen de asegurar que cualquier deficiencia detectada que afecte al Sistema de Control Interno sea informada rápidamente para tomar las decisiones oportunas (Committee of Sponsoring Organizations of the Treadway Commission, 2013).

Principios y puntos de enfoque. En la siguiente tabla se presenta la relación entre los componentes, principios y puntos de enfoque; cabe recalcar que los puntos de enfoque representan las características importantes de cada principio (Dickins & Fay, 2017).

Para determinar la efectividad del sistema de control interno, se requiere que los cinco componentes y principios mostrados en la Tabla 2, estén presentes y funcionando.

Tabla 2.

Componentes, principios y puntos de enfoque del modelo de control COSO III.

Componentes	Principios	Puntos de Enfoque
I. Entorno de control	1. La organización demuestra responsabilidad con la integridad y los valores éticos	- Constituye la modulación de la gerencia. - Instaura pautas de conducta. - Valora la cohesión a esquemas de conducta. - Decide y aborda sobre desorientaciones en forma adecuada.
	2. El consejo de administración expresa independencia de la dirección y ejecuta la	- Instaura los compromisos de supervisión de la dirección.

	supervisión del desempeño del sistema de control interno.	- Utiliza destacada experiencia. - Encarga compromisos de supervisión. - Ejecución de modo independiente. - Ofrece supervisión sobre el Sistema de Control Interno.
	3. La dirección constituye con la supervisión del Consejo, las estructuras, reportes y los niveles de autoridad y responsabilidad oportunos para la obtención de los objetivos.	- Contempla las estructuras de la entidad. - Construye líneas de reporte. - Asigna y delimita responsabilidades.
	4. La organización manifiesta responsabilidad para atraer, desarrollar y retener a profesionales oportunos, en proporción con los objetivos de la organización	- Implanta prácticas y políticas. - Valora la competitividad y direcciona las carencias - Atrae, desarrolla y retiene profesionales. - Prevé y se arregla para sucesiones.
	5. La organización define los compromisos de los individuos a nivel de control interno para la obtención de los objetivos	- Hace efectuar los compromisos a través de estructuras, autoridades y responsabilidades. - Forma medidas de desempeño, incentivos y recompensas. - Valora medidas de desempeño, incentivos y recompensas para la relevancia en curso. - Considera presiones excesivas.
II. Evaluación de riesgos	6. La organización concreta los objetivos con claridad para permitir la identificación y evaluación de los riesgos relacionados	- Objetivos Operativos. - Objetivos de Reporte Externo Financiero y no Financiero. - Objetivos de Reporte interno. - Objetivos de Cumplimiento.

	7. La organización asemeja los riesgos para la obtención de sus objetivos en todos los niveles de la entidad y los examina como base sobre la cual establece cómo se deben gestionar	- . La organización asemeja los riesgos a nivel de la entidad. - Valora la consideración de factores externos e internos. - Abarca niveles apropiados de administración. - Indaga la relevancia viable de los riesgos. - Establece la respuesta a los riesgos.
	8. La organización considera la posibilidad de fraude al valorar los riesgos para la obtención de los objetivos	- Supone varios tipos de fraude. - La valoración del riesgo de fraude evalúa incentivos y presiones.
	9. La organización asimila y evalúa los cambios que podrían alterar significativamente al sistema de control interno	- Evalúa cambios en el ambiente externo, modelo de negocios y liderazgo.
III. Actividades de control	10. La organización detalla y desarrolla actividades de control que apoyan a la mitigación de los riesgos hasta niveles tolerables para el logro de los objetivos	- Se integra con la evaluación de riesgos. - Considera factores específicos de la entidad. - Establece la importancia de los procesos del negocio. - Valora el cruce de tipos de actividades de control. - Supone en qué nivel las actividades son aplicadas. - Orienta la segregación de funciones.
	11. La organización define y crea actividades de control a nivel de entidad sobre la tecnología para apoyar la obtención de los objetivos	- Establece la correlación entre el uso de la tecnología en los procesos del negocio y los controles generales de tecnología. - Constituye actividades de control para la infraestructura tecnológica relevante. - Crea actividades de control para la administración de procesos de seguridad relevantes.

		- Establece acciones de control relevantes para los procesos de mantenimiento, desarrollo y adquisición de la tecnología.
	12. La organización extiende las actividades de control a través de políticas que constituyen las líneas generales del control interno y procedimientos.	- Implanta políticas y procesos para apoyar el despliegue de las directivas de la administración. - Establece compromisos y rendición de cuentas para ejecutar las políticas y procedimientos. - Funciona oportunamente. - Toma acciones correctivas. - Trabaja con personal adecuado. - Reevalúa políticas y procedimientos.
IV. Información y comunicación	13. La organización genera y usa información relevante y de calidad para apoyar el funcionamiento del control interno	- Reconoce los requerimientos de información. - Obtiene fuentes internas y externas de información. - Procesa datos principales dentro de la información. - Conserva la calidad mediante el procesamiento. - Considera costos y beneficios.
	14. La organización transmite la información internamente, comprendidos los objetivos y responsabilidades que son fundamentales para apoyar el funcionamiento del sistema de control interno	- Comunica la información de control interno. - Se comunica con la Junta directiva. - Suministra líneas de comunicación separadas. - Escoge alternativas de comunicación relevantes.
	15. La organización se comunica con los grupos de interés externos sobre los aspectos esenciales que alterar al funcionamiento del control interno	- Se comunica con grupos de interés externos. - Accede comunicaciones de entrada. - Se comunica con la Junta Directiva. - Suministra líneas de comunicación separadas.

		- Escoge alternativas de comunicación relevantes.
V. Actividades de supervisión – monitoreo	16. La organización elige, desarrolla y ejecuta valoraciones continuas y/o independientes para comprobar si los componentes del sistema están presentes y funcionando	- Considera una mezcla de valoraciones continuas e independientes. - Considera tasa de cambio. - Constituye un punto de referencia para el entendimiento. - Uso de personal capacitado. - Se integra con los procesos del negocio. - Ajusta el alcance y la frecuencia. - Evalúa objetivamente.
	17. La organización evalúa y comunica las deficiencias de control interno de forma adecuada a las partes responsables de aplicar medidas correctivas, incluyendo la alta dirección y el consejo, según corresponda	- Evalúa resultados. - Comunica deficiencias. - Supervisa acciones correctivas

Nota. Obtenido de Committee of Sponsoring Organizations of the Treadway Commission. (2013). *Control interno - Marco Integrado*.

Responsabilidades en el Sistema. Varios son los roles y responsabilidades que asumen los participantes internos y externos en un Sistema de Control Interno. Los participantes internos asumen responsabilidades, mientras que los externos ejecutan aportaciones valiosas (Alayo, 2016).

a. Consejo de Administración: debe ser consciente de los riesgos asociados con el logro de los objetivos de la institución, evaluar las debilidades del control interno y tomar medidas para disminuir riesgos y deficiencias. Además, juega un papel clave en el establecimiento de expectativas de integridad, valores éticos, transparencia y rendición de cuentas, en el marco del sistema de control interno (COSO, 2013)
b. Alta Dirección: se encarga de evaluar el sistema de control interno en base a la aplicación de los 17 principios. Además, debe asesorar y orientar a la Administración,

ejercer una gestión constructiva y rigurosa, aprobar políticas, transacciones y supervisar sus actividades (COSO, 2013). Los miembros de la Alta Dirección son:

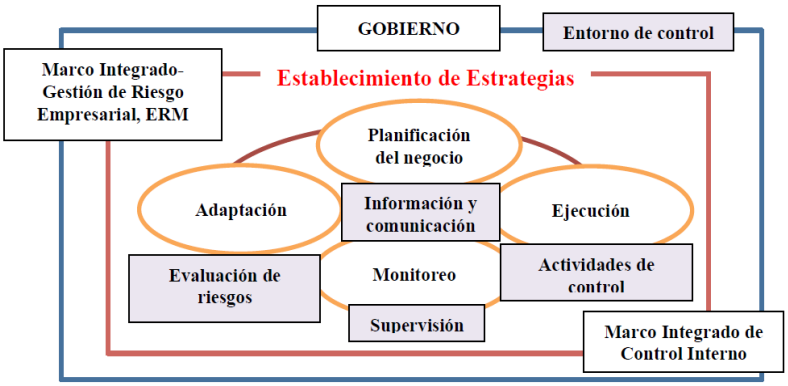
- Director administrativo
- Director ejecutivo de auditoría
- Director de cumplimiento
- Director financiero
- Director de información
- Director legal
- Director de operaciones
- Director de riesgos

c. Otros miembros de la dirección y del personal: los directivos y demás personal de la institución deben reconocer los cambios de la nueva versión del Marco Integrado de Control Interno 2013, y valorar los impactos en el actual Sistema de Control Interno de la entidad (Dickins & Fay, 2017).
d. Auditores internos: están encargados de inspeccionar los planes de auditoría y evaluar los cambios en el Marco de referencia para considerar posibles efectos a futuro. Deben ser ejecutados por profesionales competentes.
e. Auditores externos: se encargan de evaluar el Sistema de Control Interno de la institución (Gonzales, 2013).
f. Partes interesadas: el Control Interno es elaborado por la Dirección, el Consejo de Administración y demás personal de la entidad (Alayo, 2016).

Implementación. La implementación de un Marco Integrado de control Interno debe basarse en el modelo de negocio de la organización (Figura 5), que involucra en la mayoría de los procesos administración y de gobierno.

Figura 5.

Modelo de negocio para la implementación de Marco Integrado de Control Interno



Nota. Obtenido de Committee of Sponsoring Organizations of the Treadway Commission. (2013). *Control interno - Marco Integrado*.

El modelo de negocio comienza con el gobierno, incluyendo la visión y misión de la organización. También incluye las actividades de la alta dirección para asegurar la eficacia de la preparación estratégica de la organización y otros procesos de gestión. Un gobierno eficaz garantiza la rendición de cuentas, la equidad y la transparencia en las relaciones de la organización con sus diversas partes interesadas (COSO, 2013).

El desarrollo de la estrategia organizacional es el proceso mediante el cual la gerencia presenta un plan de alto nivel para conseguir uno o más objetivos relacionados con la misión de la organización (COSO, 2013).

Juntos, estos elementos de gobierno y el establecimiento de la estrategia suministran dirección al negocio y tienen un lugar para garantizar el éxito de la organización (Gonzales, 2013).

En el modelo de negocio existen cuatro elementos se basan en el circuito de Deming: planificar, hacer, comprobar y actuar (plan, do, check, actcycle).

- Planificación del negocio: define metas específicas sobre como la administración aporta al logro de los objetivos de la estrategia general; asimismo, proporciona un proceso favorable para la implementación y ejecución de la estrategia corporativa (COSO, 2013).

- Ejecución: cubre las actividades básicas de la organización logren el desempeño esperado en línea con los valores y la estrategia (COSO, 2013).
- Monitoreo: estas son las actividades establecidas por la administración para revisar y controlar el desempeño de las operaciones de la organización en comparación con el plan estratégico general, incluido el nivel aceptable de riesgo (COSO, 2013).
- Adaptación: describe los procesos organizacionales mediante los cuales se identifican los problemas se traducen en cambios ejecutables en la estrategia de la organización (COSO, 2013).

Herramientas de evaluación. El marco proporciona una serie de formularios o plantillas que brindan orientación para realizar el trabajo con ejemplos de cómo desarrollar evaluaciones. Estos formularios pueden personalizarse de acuerdo con las necesidades y características de la institución y otros aspectos que la dirección considere necesarios para evaluar el control interno (COSO, 2013).

Estos formularios se pueden utilizar para diversos fines de acuerdo con Gonzales (2013) en su investigación:

- Ayudar a determinar la existencia y el funcionamiento de los componentes y principios.
- Apoyar en la evaluación para comprobar si los cinco componentes del sistema de control interno están operando simultáneamente y de manera integrada.
- Ayudar a evaluar la eficacia del Sistema de Control Interno en relación con una o más categorías de objetivos.
- Documentar la evaluación de la administración en dependencia con la efectividad del Sistema de Control Interno, considerando los componentes y principios.
- Evidenciar las fallas encontradas durante el proceso de evaluación.

Modelo COBIT 5

Generalidades. Es un modelo empleado para el gobierno y gestión de la información de una institución, teniendo como enfoque el impacto de la TI, seguridad, riesgo y aseguramiento, planteando cinco principios y siete facilitadores para alcanzar los objetivos, la mejora continua y supervisar las buenas prácticas del gobierno y gestión de TI de un establecimiento. Se aplica en las auditorías de tecnología de la información a nivel mundial (de Haes et al., 2013).

El desarrollo de COBIT 5 se vio impulsado por necesidades como:

- Que las partes interesadas se involucren para conocer lo que requieren con respecto a la información y TI, teniendo en cuenta lo que esperan en la institución y que el valor obtenido sea proporcionado, obteniendo resultados transparentes y reales (León et al., 2018).
- Las organizaciones dependen de compañías externas con respecto a los TI.
- La información sea gestionada de una manera eficaz.
- Las TI sean integradas para todos los miembros de la organización, es decir que sean de manera generalizada.
- Orientar sobre las tecnologías de información que surgen en los años
- Vincular otros modelos de referencia principales a nivel mundial (León et al., 2018).

Principios. COBIT 5 se fundamenta en cinco principios claves para el gobierno y la gestión de las TI empresariales.

I. *Principio 1.* Satisfacer las Necesidades de las Partes Interesadas: Las empresas existen para generar valor para sus partes interesadas conservando el equilibrio entre la ejecución de beneficios y la optimización de los riesgos y el uso de recursos.

   Cascada de Metas de COBIT 5

La cascada de metas de COBIT 5 es el componente para convertir las necesidades de las partes interesadas en metas corporativas, metas relacionadas con las TI y metas catalizadoras específicas, útiles y a medida (ISACA, 2012b).

i. Paso 1. Los Motivos de las Partes Interesadas Influyen en las Necesidades de las Partes Interesadas
ii. Paso 2. Las Necesidades de las Partes Interesadas Desencadenan Metas Empresariales
iii. Paso 3. Cascada de Metas de Empresa a Metas Relacionadas con las TI
iv. Paso 4. Cascada de Metas Relacionadas con las TI Hacia Metas Catalizadoras

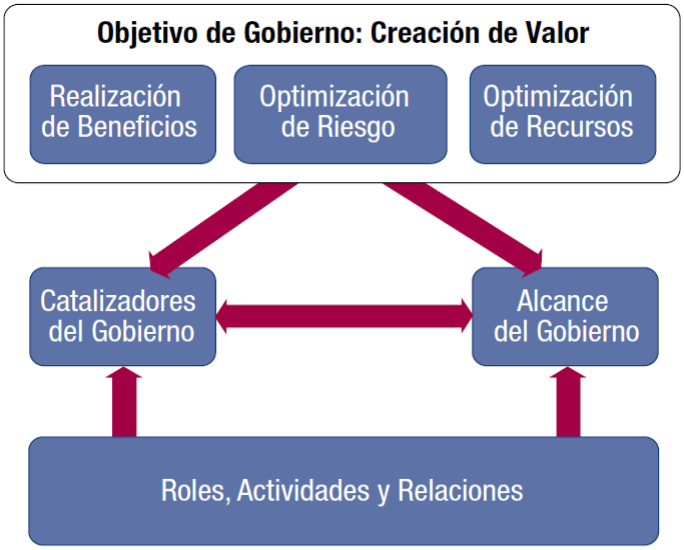
La cascada de metas es importante porque ayuda a priorizar la implementación, la mejora y el énfasis en la gobernanza de TI en la empresa, en función de los objetivos generales y los riesgos asociados (ISACA, 2012b).

II. *Principio 2.* Cubrir la Empresa Extremo-a-Extremo: COBIT 5 integra el gobierno y la gestión de TI en el gobierno corporativo; cubriendo todas las funciones y operaciones de la empresa. COBIT 5 se enfoca no solo en la "función de TI", sino que trata la información y las tecnologías relacionadas como un activo que todos en el negocio deberían tratar (ISACA, 2012b).

Enfoque de gobierno. En esta parte se van a tratar los componentes clave de un sistema de gobierno, los que se muestran en la Figura 6.

Figura 6.

Enfoque de gobierno COBIT 5



Nota. Obtenido de ISACA. (2012). Un Marco de Negocio para el Gobierno y la Gestión de las TI de la Empresa. http://linkd.in/ISACAOfficial.

Estos componentes son:

a) *Catalizadores de gobierno:* son los recursos organizativos para el gobierno como marcos de referencia, estructura, principios, procesos y practicas con el fin de alcanzar los objetivos (ISACA, 2012b).

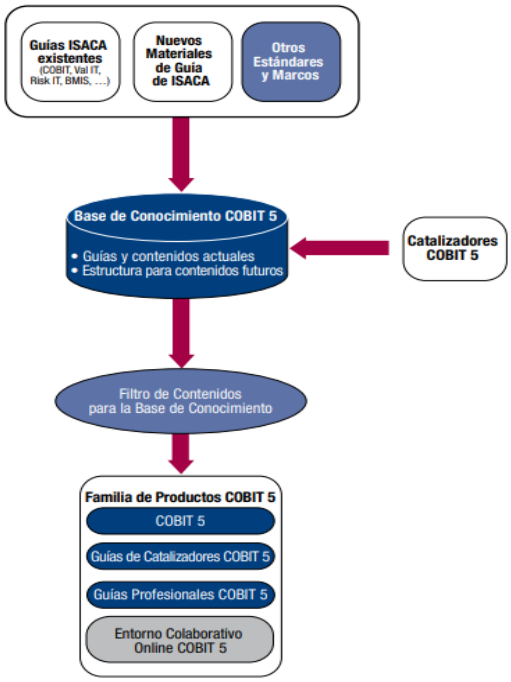
b) *Alcance de gobierno:* el gobierno puede ser aplicado a toda la empresa, es decir, puede determinar diferentes visiones de la empresa a la que se aplica el gobierno (ISACA, 2012b).

c) *Roles, Actividades y Relaciones:* Determinan quién participa en el gobierno, cómo participan, qué hacen y cómo interactúan en alcance de cualquier sistema de gobierno (ISACA, 2012).

III. *Principio 3.* Aplicar un Marco de Referencia único integrado (Figura 7): COBIT 5 está estrechamente alineado con otros estándares y marcos de trabajo, lo que lleva al marco principal para el gobierno y la gestión (ISACA, 2012b).

Figura 7.

Marco de Referencia Integrado



Nota. Obtenido de ISACA. (2012). Un Marco de Negocio para el Gobierno y la Gestión de las TI de la Empresa. http://linkd.in/ISACAOfficial.

IV. *Principio 4.* Hacer Posible un Enfoque Holístico: enfoque general que contiene todo a través de la utilización de catalizadores (ISACA, 2012b).

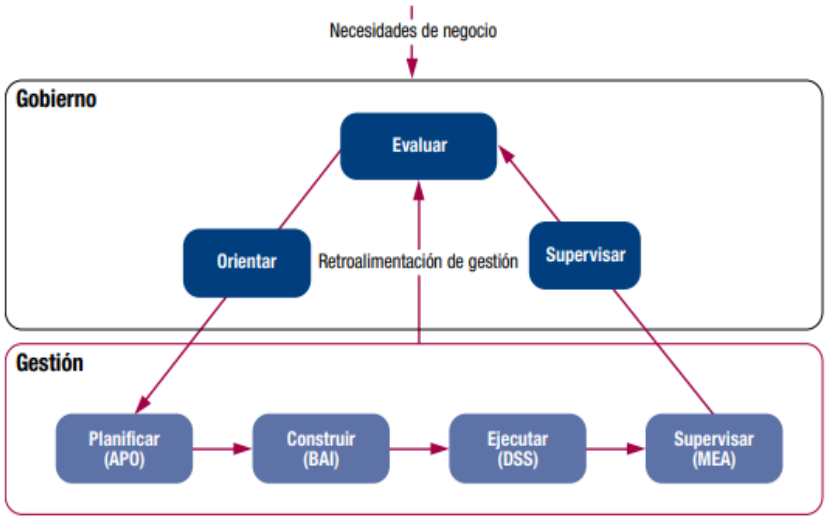
COBIT 5 describe siete categorías de catalizadores:

a. Principios, políticas y marcos de referencia.
b. Los procesos
c. Las estructuras organizativas
d. La Cultura, ética y comportamiento
e. La información
f. Los servicios, infraestructuras y aplicaciones
g. Las personas, habilidades y competencias

V. Principio 5. Separar el Gobierno de la Gestión: COBIT 5 distingue claramente entre gobierno y gestión (Figura 8). Estos dos elementos cubren diferentes tipos de actividades estas requieren diferentes estructuras organizativas y tienen diferentes propósitos (Chisag, 2017).

Figura 8.

Áreas claves del Gobierno y Gestión.

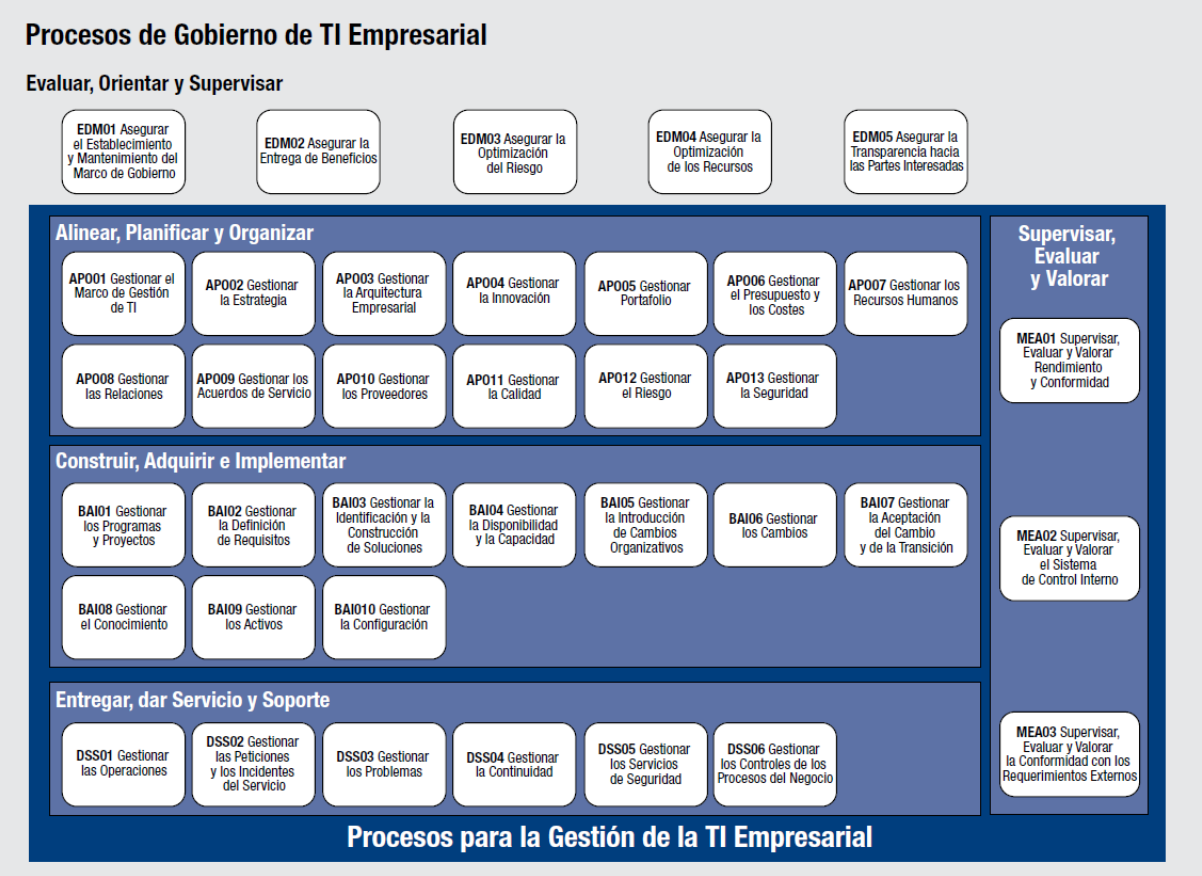


Nota. Obtenido de ISACA. (2012). Un Marco de Negocio para el Gobierno y la Gestión de las TI de la Empresa. http://linkd.in/ISACAOfficial.

COBIT 5 distingue dos áreas clave como el gobierno y gestión, el gobierno tiene la función de asegurar que se evalúen las necesidades, condiciones y opciones de las partes involucradas con el fin de lograr los objetivos acordados; estableciendo la dirección mediante la priorización y la toma de decisiones (ISACA, 2012b), mientras que la gestión posee la función de planificar, desarrollar, ejecutar y controlar las actividades de acuerdo con las direcciones establecidas por el gobierno para alcanzar las metas empresariales (ISACA, 2012b), estas dos áreas se encuentran divididas en diferentes dominios de procesos como los mostrados en la Figura 9.

Figura 9.

Modelo de Referencia de Procesos



Nota. Obtenido de ISACA. (2012). Un Marco de Negocio para el Gobierno y la Gestión de las TI de la Empresa. http://linkd.in/ISACAOfficial.

Implementación. ISACA provee amplias y prácticas guías de implementación en su publicación COBIT 5 que está establecida en un ciclo de vida de mejora continua. No pretende ser un enfoque obligatorio ni una solución completa, sino más bien una guía para evitar errores comunes, aprovechar las mejores prácticas y ayudar a lograr resultados positivos.

- *Un Enfoque de Ciclo de Vida:* la implementación del ciclo de vida proporciona una forma para que las organizaciones utilicen COBIT para abordar los desafíos y la complejidad que a menudo surgen durante la implementación. Los tres componentes interrelacionados del ciclo de vida son:

    i. Ciclo de vida de Mejora continua.

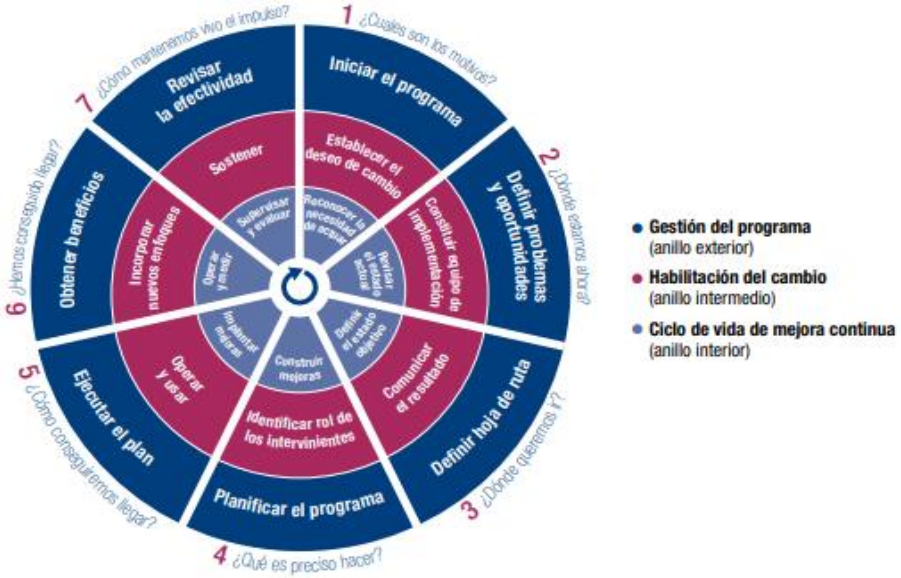
ii. Habilitación del cambio.

iii. Gestión del programa.

Se debe crear el entorno apropiado para asegurar la implementación exitosa o la mejora de la iniciativa. El ciclo costa de siete etapas como se muestra en la Figura 10 (de Haes et al.,2013).

Figura 10.

Las Siete Fases de la Implementación del Ciclo de Vida



Nota. Obtenido de ISACA. (2012). Un Marco de Negocio para el Gobierno y la Gestión de las TI de la Empresa. http://linkd.in/ISACAOfficial.

1. La fase 1 comienza por reconocer y aceptar la necesidad de una iniciativa de implementación o mejora. Identifica los puntos débiles actuales y desencadena con el fin de crear ánimo de cambio a un nivel de dirección ejecutiva (ISACA, 2012).
2. La fase 2 define el alcance de la iniciativa de implementación utilizando el mapeo de COBIT de metas u objetivos empresariales con metas de TI. Se debe llevar a cabo una valoración del estado actual y se asemejan los problemas y deficiencias por la ejecución de un proceso de revisión de capacidad (ISACA, 2012).

3. La fase 3 durante esta etapa se forma un objetivo de mejora, continuado de un análisis detallado valiéndose de las directrices de COBIT para identificar diferencias y posibles soluciones (ISACA, 2012).
4. La fase 4 se encarga de planificar soluciones prácticas mediante la definición de proyectos respaldados por casos de negocios justificados. Además, se crea un plan de cambios para la implementación (ISACA, 2012).
5. En la fase 5 se logran definir las mediciones y establecer la supervisión empleando las metas y métricas de COBIT para conseguir y mantener la alineación con el negocio y que el rendimiento puede ser medido (ISACA, 2012).
6. La fase 6 se centra en la operación sostenible de los nuevos catalizadores y de la supervisión de la obtención de los beneficios deseados (ISACA, 2012).
7. En la fase 7 se revisa el éxito general de la iniciativa, se identifican requisitos extras para el gobierno o la gestión de la TI. Se refuerza la necesidad de mejora continua (ISACA, 2012).

CAPÍTULO 2

Desarrollo

Comparación de COSO y COBIT

COSO y COBIT son dos marcos de referencia que permiten llevar un control interno en las instituciones sobre información ya sean de gobierno, financieros o de la tecnología para prevenir fraudes y riesgos.

Los dos marcos de control son utilizados en procesos de auditoría, pero difieren en aspectos como: enfoque, propósito, alcance, detalle, finalidad entre otros.

Por lo que se realiza una comparación para elegir el modelo más apropiado para realizar una auditoría informática mediante la calificación de las métricas de evaluación planteadas de acuerdo con los principales objetivos que debe cumplir una auditoría informática en instituciones de Educación media.

Escala de evaluación

La escala de valoración permite determinar el grado de cumplimiento de parámetros, permitiendo verificar así su magnitud. Una de estas escalas es la de Likert, la cual se utiliza para una evaluación cualitativa de las métricas propuestas (Canto de Gante et al., 2020).

La escala de Likert puede presentar una escala de evaluación de al menos tres niveles y pudiendo llegar hasta cinco, siendo 1 el cual no cumple con la métrica y 5 que cumple la métrica en su totalidad, es decir que esta evaluación tiene una afirmación ya sea positiva o negativa junto con una evaluación numérica (Canto de Gante et al., 2020).

Para la escala de puntuación se manejó una escala de Likert con las ponderaciones mostradas en la Tabla 3.

Tabla 3.

Escala de Likert.

Valor	Significado
1	Totalmente en desacuerdo
2	En desacuerdo
3	Ni de acuerdo ni en desacuerdo
4	De acuerdo
5	Totalmente de acuerdo

Métricas de evaluación

El estudio comparativo de los modelos de control COSO III y COBIT V, se plantearon métricas de acuerdo con los principales objetivos que deben cumplir una auditoría informática en instituciones de educación media que son:

- Controlar la función informática de las instituciones de educación.
- Analizar la eficiencia de los Sistemas Informáticos.
- Verificar el cumplimiento de los objetivos y la Normativa general de la institución a través de la revisión eficaz de la gestión de los recursos materiales y humanos (Asociación Española de Contabilidad y Administración de Empresas, 2017).

La evaluación se realiza respecto a cada métrica planteada como se muestra en la Tabla 4, las cuales son evaluadas en base a la escala de Likert.

Tabla 4.

Métricas de evaluación planteadas para comparar los modelos de control COSO y COBIT.

Métricas	**Modelo de control**	
	COSO	**COBIT**
Propósito		
Supervisión y monitoreo		
Seguridad de la información		
Adaptación		
Total		
Promedio		

Se determinó si uno o los dos modelos de control son más apropiado utilizar en una auditoría informática, en base al promedio obtenido respecto a las métricas, para garantizar el cumplimiento de sus objetivos principales.

Comparación respecto al propósito de la auditoría informática en Instituciones de educación media.

Propósito

Tabla 5.

Comparación de COSO y COBIT respecto al propósito en auditoría informática.

Métrica		**Modelo de control**	
Propósito		**COSO**	**COBIT**
Tecnología de la información	¿Se encarga de verificar el funcionamiento de TI?	3	5
Gobernanza de los sistemas de información	¿Permite conocer la gobernanza de los sistemas de información?	5	5
Gobierno de la organización	¿Permite conocer la forma de gobierno de la institución?	5	4
	TOTAL	13	14
	PROMEDIO	4.33	4.66

Análisis Tabla 5:

- **Tecnología de la información:** COSO en sus generalidades establece que se enfoca en realizar un análisis o control a través de un marco integrado de la administración,

dirección y el personal de una empresa para prevención de riesgos (COSO, 2013), mientras que COBIT 5 está orientado en alcanzar un proceso integrado para controlar, gestionar y gobernar la tecnología de información para lograr alcanzar los objetivos planteados de una institución (ISACA, 2012b).

Justificación

En de marco de referencia COSO en el componente 'Evaluación de Riesgos' uno de los principios que hace referencia al punto a evaluar es el principio N°7 'identificar y analizar los riesgos' en el cual hace mucho énfasis en varios factores internos y externos que pueden llegar a obstruir el cumplimiento de los objetivos; por ello se debe analizar los riesgos como base para poder gestionar los mismos. Un de estos factores es el tecnológico el cual manifiesta que puede comprometer la disponibilidad y uso de la información, costos de infraestructura y la demanda de los servicios de TI (COSO, 2013).

En el marco de referencia COBIT el proceso 'APO01 Gestionar el Marco de Gestión de TI' se encarga de aclarar y mantener el gobierno de la visión y misión corporativa de TI, además este proceso se encarga de proporcionar un enfoque de gestión sólida que permita cumplir los requisitos de gobierno corporativo incluyendo procesos de gestión, estructuras, roles y responsabilidades con todo lo consecuente al ámbito TI. Otro de los procesos que ayuda a verificar el funcionamiento de TI es 'APO11 Gestionar la Calidad' el cual asegura la entrega de soluciones y servicios que cumplan con los requisitos de la organización (ISACA, 2012a).

- **Gobernanza de los sistemas de información:** La información y tecnología son dos componentes importantes que posee una institución, tanto COSO 3 y COBIT 5 auditan la gestión y control de la información así lo establece COSO 3 en su componente entorno de control que para el cumplimiento de sus 5 principios es necesario conocer como son gobernados a través de controles generales y de aplicación de los sistemas de información para incrementar la productividad de la institución, de la misma manera

COBIT 5 a través de sus cuatro dominios como planificar, construir, ejecutar y monitorear permite controlar los sistemas de información de toda una empresa (ISACA, 2012b).

Justificación

En el marco de referencia COSO en el componente 'Actividades de Control' uno de los principios que hace referencia al punto a evaluar es el principio N°11 'La organización define y desarrolla actividades de control a nivel de entidad sobre la tecnología para apoyar la consecución de los objetivos.' en el cual la organización selecciona y desarrolla actividades generales de control sobre la tecnología para apoyar el logro de los objetivos. Las actividades de control y la tecnología se relacionan de dos formas: 1) La tecnología apoya los procesos del negocio: cuando la tecnología se integra en los procesos comerciales, se requieren actividades de control para reducir el riesgo de errores. 2) La tecnología se utiliza para automatizar las actividades de control: diversas actividades de control de una organización están parcial o completamente automatizadas (COSO, 2013).

En el marco de referencia COBIT el proceso 'EDM01 Asegurar el Establecimiento y Mantenimiento del Marco de Gobierno' se encarga de analizar y articular los requisitos para el gobierno de TI y conserva efectivas las estructuras, prácticas y procesos facilitadores, con claridad de las responsabilidades y la autoridad para alcanzar la misión, las metas y objetivos de la organización (ISACA, 2012a).

- **Gobierno de la organización:** COSO III en uno de sus objetivos establece que permite conocer a través de sus componentes la forma de gobierno de toda una institución principalmente a través del análisis de todos los aspectos informes de riesgos (Dickins & Fay, 2017)y COBIT 5 se enfoca en analizar uno de los componentes de la estructura de la institución como es la tecnología de la información de manera específica (Mangalaraj et al., 2014).

  Justificación

En el marco de referencia COSO en el componente ‘Entorno de control’ uno de los principios que hace referencia al punto a evaluar es el principio N°2 ‘El consejo de administración demuestra independencia de la dirección y ejerce la supervisión del desempeño del sistema de control interno’ en el cual la Junta Directiva demuestra independencia de la administración y despliega la supervisión del desempeño y desarrollo del Control Interno. Estas expectativas y requisitos ayudan a definir los objetivos de la organización, supervisar las responsabilidades de la junta y administrar los recursos necesarios. Otro componente que también hace referencia a este punto es el principio N°3 ‘La dirección estable con la supervisión del consejo, las estructuras, líneas de reporte y los niveles de autoridad y responsabilidad apropiados para la consecución de los objetivos’, de igual forma que el anterior principio este se encarga de que la administración, bajo la supervisión de la Dirección, determine la estructura y los niveles adecuados de autoridad y responsabilidad para obtención los objetivos (COSO, 2013).

En el marco de referencia COBIT el proceso ‘APO02 Gestionar la Estrategia’ se encarga proporcionar una visión holística del entorno empresarial y de TI, la dirección futura y los planes necesarios para migrar al entorno deseado. Utiliza módulos de estructura empresarial, incluida la subcontratación y funciones relacionadas, para responder de forma flexible, fiable y eficiente a los objetivos estratégicos (ISACA, 2012a).

Supervisión y Monitoreo

Tabla 6

Comparación de COSO y COBIT respecto a supervisión y monitoreo en auditoría informática.

Métrica		**Modelo de control**	
Supervisión y monitoreo		**COSO**	**COBIT**
Cumplimiento con la ley	¿Permite verificar su uso de acuerdo y acorde a la ley?	5	5
Alineación a los objetivos de negocio	¿Su implementación permite alinear con los objetivos de negocio?	5	5
Establecimiento de Roles y responsabilidades	¿Establece roles para la organización?	5	5
	TOTAL	15	15
	PROMEDIO	5	5

Análisis Tabla 6:

- **Cumplimiento con la Ley:** Los dos modelos de control son empleados para el cumplimiento de los objetivos del control interno de una institución, por lo que los dos buscan el cumplimiento de las leyes, acuerdos, normas o políticas contractuales establecidos en los procesos de las organizaciones, COSO lo establece en sus objetivos de evaluación de riesgos y COBIT en uno de sus criterios de control como es el cumplimiento.

  Justificación

  En el marco de referencia COSO en el componente ‘Evaluación de riesgos’ uno de los principios que hace referencia al punto a evaluar es el principio N°6 ‘La organización define los objetivos con suficiente claridad para permitir la identificación y evaluación de los riesgos relacionados’ en el cual la organización define los objetivos con suficiente claridad para poder identificar y evaluar los riesgos relacionados con los objetivos. Para determinar si los objetivos son apropiados, la administración debe considerar: 1) La alineación de las metas establecidas con las prioridades estratégicas. 2) Determinar la tolerancia al riesgo del objetivo. 3) Coherencia entre los

objetivos declarados y las leyes, reglas, reglamentos y normas aplicables a la entidad (COSO, 2013).

En el marco de referencia COBIT existen varios procesos que entre sus metas están el cumplimiento y soporte de las TI al cumplimiento del negocio de las leyes y regulaciones externas. Estos procesos son: 'APO12 Gestionar el Riesgo', 'APO10 Gestionar los Proveedores' y 'BAI010 Gestionar la Configuración'; además también Son responsables de identificar, evaluar y mitigar continuamente los riesgos relacionados con TI dentro de las tolerancias establecidas por la dirección ejecutiva (ISACA, 2012a).

- **Alineación de los objetivos del negocio:** En el modelo COBIT se estructura un gobierno de TI, donde uno de sus componentes es la alineación estratégica en el cual se garantiza el alineamiento a los objetivos del negocio ya sean actuales o futuros, de la misma manera COSO alinea sus estrategias y objetivos de acuerdo a la misión, visión de la organización para supervisar los riesgos, es decir que los dos modelos plantean alinear los objetivos del negocio pero con dos enfoques diferentes, COBIT para garantizar un efectivo gobierno de TI y COSO para evaluar los riesgos.

  Justificación

  En el marco de referencia COSO en el componente 'Información y comunicación' uno de los principios que hace referencia al punto a evaluar es el principio N°14 'La organización comunica la información internamente' el cual establece Comunicar información dentro de la organización, incluidos los objetivos y responsabilidades de control interno, para respaldar la operación del sistema de control interno. Por lo tanto, la administración debe desarrollar e implementar políticas y procedimientos que promuevan una comunicación interna efectiva y siempre alineado a los objetivos de la organización.

  En el marco de referencia COBIT el proceso 'MEA01 Supervisar, Evaluar y Valorar el Rendimiento y la Conformidad' establece recolectar, validar y evaluar métricas y

objetivos de negocio, de TI y de procesos. Supervisar que los procesos se están realizando acorde al rendimiento acordado y conforme a los objetivos y métricas; es decir que estén alineados a los objetivos del negocio (ISACA, 2012a).

- **Establecimiento de los roles y responsabilidades:** En los dos modelos es indispensable establecer las responsabilidades de los funcionarios de la organización, para con la auditoría conocer el cumplimiento de estas y en caso de fallas buscar alternativas que ayuden a solventarlas minimizando los riesgos en la organización.

  Justificación

  En el marco de referencia COSO en el componente 'Evaluación de riesgos' uno de los principios que hace referencia al punto a evaluar es el principio N°6 'La organización define los objetivos con suficiente claridad para permitir la identificación y evaluación de los riesgos relacionados' afirma que la organización define los objetivos de una manera lo suficientemente clara para identificar y evaluar los riesgos asociados con los objetivos. Antes de la evaluación de riesgos, se deben identificar objetivos relacionados con los distintos niveles de la entidad, a saber, objetivos operativos, de información y de cumplimiento, que deben ser coherentes con la misión de la entidad (COSO, 2013).

  En el marco de referencia COBIT el proceso 'APO07 Gestionar los Recursos Humanos' Proporciona un enfoque estructurado para garantizar la estructura, el despliegue y la toma de decisiones óptimos de los recursos humanos. Esto incluye comunicar funciones y responsabilidades claras, planes de formación y desarrollo personal y expectativas de rendimiento con el apoyo de personas competentes y motivadas.

Seguridad de la Información

Tabla 7.

Comparación de COSO y COBIT respecto a seguridad de la información en auditoría informática.

Métrica		**Modelo de control**	
Seguridad de la información		**COSO**	**COBIT**
Administración de riesgos	¿Permite una buena gestión de riesgos?	5	5
Normas de Seguridad	¿Establece normas de seguridad para la institución respecto a TI?	3	5
Gestión de la información	¿Permite un adecuado manejo de la información respecto a TI?	5	5
	TOTAL	13	14
	PROMEDIO	4.33	4.66

Análisis Tabla 7:

- **Administración de riesgos:** Los dos modelos de control tienen un enfoque para prevención de fraudes y riesgos, es así que dentro del modelo de COSO se especifica en un componente la valoración de riesgos donde es necesario identificar cambios que afecten en el sistema de control interno de la organización, de igual forma COBIT en su dominio de planear y organizar especifica en uno de sus procesos (P09) la administración de riesgos establecido en los indicadores de control para identificar ciertas situaciones que ponen en riesgo la organización, evaluarlas y elaborar alternativas como un plan de acción que permita reducir su impacto.

  Justificación

  En el marco de referencia COSO en el componente 'Evaluación de riesgos' uno de los principios que hace referencia al punto a evaluar es el principio N°7 'identifica y analiza los riesgos' afirma que se debe considerar los factores externos e internos al identificar los riesgos que pueden afectar los objetivos. La dirección evalúa si existen

mecanismos suficientes para identificar y analizar los riesgos, analizar las posibles dependencias de los riesgos identificados, comprender la tolerancia al riesgo de la organización y determinar la respuesta a los riesgos. La evaluación de riesgos incluye la consideración de cómo manejar el riesgo y si se acepta, evita, reduce o comparte (COSO, 2013).

En el marco de referencia COBIT el proceso 'APO12 Gestionar el Riesgo' afirma que se debe Identificar, evaluar y mitigar continuamente los riesgos relacionados con TI dentro de los niveles de tolerancia definidos por la dirección ejecutiva de la organización. Los subprocesos de APO12 nos detalla los pasos que se debe seguir para un mejor tratamiento del riesgo, estos son: recopilación de datos, analizar el riesgo, mantener un perfil de riesgo, expresar el riesgo, definir un portafolio de acciones para la gestión de riesgos y responder al riesgo (ISACA, 2012a).

- **Normas de Seguridad:** En el modelo COSO en el componente actividades de control se plantea la evaluación de cambios y riesgos en el negocio, lo cual permite establecer o desarrollar actividades de control, políticas y procedimientos que garanticen que la información de la empresa sea manejada con seguridad, sin embargo son normas para toda la organización con un enfoque general, mientras que en COBIT establecer normas de seguridad de la información se relaciona con el dominio entregar y dar soporte, donde se establecen parámetros o normas a seguir para optimizar las TI y garantizar la seguridad de la información que es contemplada en uno de sus objetivos. Es decir que los dos modelos contemplan normas de seguridad de la información sin embargo dentro de las auditorías informáticas COBIT permite establecer normas específicas en el campo de TI (ISACA, 2012a).

  Justificación

  En el marco de referencia COSO en el componente 'Actividades de control' uno de los principios que hace referencia al punto a evaluar es el principio N°11 'selecciona y desarrolla controles generales sobre tecnología' afirma que la organización elige y

desarrolla actividades generales de control sobre la tecnología para apoyar el logro de los objetivos. Las acciones y métodos de control se relacionan de dos formas:1) La tecnología respalda los procesos comerciales: cuando la tecnología se integra en los procesos comerciales, se requieren actividades de control para reducir el riesgo de errores. 2) Tecnología utilizada para automatizar las actividades de control: muchas actividades de control en las organizaciones están parcial o totalmente automatizadas.

En el marco de referencia COBIT el proceso 'APO13 Gestionar la Seguridad' se encarga de Definir, operar y monitorear el sistema de gestión de seguridad de la información; el mismo que tiene como metas: 1) Disponer de un sistema para revisar y abordar de forma eficaz los requisitos de seguridad de la información de la organización. 2) El plan de seguridad es elaborado, adoptado y difundido en toda la empresa. 3) Las soluciones de seguridad de la información se implementan y operan de manera uniforme en toda la empresa.

- **Gestión de la información:** Tanto COSO como COBIT son modelos que auditan la gestión y control de la información de una organización, es decir administradores, auditores y usuarios, sin embargo, COBIT está orientado específicamente a la tecnología de la información.

  Justificación

  En el marco de referencia COSO en el componente 'Información y comunicación' uno de los principios que hace referencia al punto a evaluar es el principio N°13 'La organización obtiene o genera y utiliza información relevante y de calidad para apoyar el funcionamiento del control interno' establece que las organizaciones deben desarrollar sistemas de información para adquirir, capturar y procesar grandes cantidades de datos de fuentes internas y externas y transformarlos en información significativa y utilizable. Los sistemas de información incluyen la combinación de personas, datos y tecnología que respaldan los procesos comerciales (COSO, 2013).

En el marco de referencia COBIT el proceso ‘BAI09 Gestionar los Activos’ se encarga de Administrar los activos de TI a lo largo de su ciclo de vida para garantizar que su uso proporcione valor a un costo óptimo, que continúen funcionando (según lo previsto), que estén físicamente contabilizados y protegidos, y que los activos críticos para respaldar las capacidades del servicio sean confiables y estén disponibles (ISACA, 2012a).

Adaptabilidad

Tabla 8.

Comparación de COSO y COBIT respecto a adaptabilidad en auditoría informática.

Métrica		**Modelo de control**	
Adaptabilidad		**COSO**	**COBIT**
Dificultad de implementación	¿Cuál tiene mayor dificultad de implementación?	5	4
Costo de implementación	¿Los costos de implementar el modelo de control son altos?	3	3
Conocimiento del personal	¿Es necesario que el personal conozca su funcionamiento para un mejor desarrollo?	5	5
	TOTAL	13	12
	PROMEDIO	4.33	4

Análisis Tabla 8:

- **Dificultad y costo de implementación:** De acuerdo con el estudio de análisis comparativo entre metodologías para la realización de auditorías de seguridad informática, aplicando el Proceso Analítico Jerárquico (AHP) se logró apreciar que el modelo COSO tiene mayor dificultad, pero menor costo en comparación a COBIT que es más fácil de implementar y tiene un costo mayor.

  Justificación

En el marco de referencia COSO en el componente ‘Actividades de supervisión y monitoreo’ uno de los principios que hace referencia al punto a evaluar es el principio N°16 ‘conduce evaluaciones continuas y/o independientes’ establece que la organización debe seleccionar, diseñar y realizar evaluaciones continuas para determinar si los componentes del sistema de control interno están implementados y funcionando. Las actividades de seguimiento y vigilancia se llevan a cabo mediante una evaluación continua e independiente. Las evaluaciones continuas se integran en los procesos de negocio en los diferentes niveles de la entidad y brindan información oportuna. El uso de la tecnología respalda la evaluación continua, tiene altos estándares de objetividad y permite una revisión eficiente de grandes cantidades de datos a bajo costo (COSO, 2013).

En el marco de referencia COBIT el proceso ‘BAI05 Gestionar la Facilitación del Cambio Organizativo’ se encarga de aumentar la capacidad de implementar cambios organizacionales de manera rápida y exitosa en toda la empresa mientras mitiga el riesgo en todo el ciclo de vida del cambio y todas las partes interesadas de negocios y TI. entre sus metas más destacadas están: 1) Comprender el deseo de cambio de sus partes interesadas. 2) El equipo de implementación puede impulsar el cambio. 3) Los cambios necesarios son entendidos y aceptados por los interesados (ISACA, 2012a).

- **Conocimiento del personal:** Es importante comprender que mientras se esté implementando cualquiera de las metodologías se ejecutan diferentes actividades que pueden llegar a ser complejas, las cuales necesitan ser regularizadas y sujetas a una supervisión previa para verificar que se cumplan los objetivos planteados. Por ello se debe tener un conocimiento previo y un acompañamiento de profesionales que lleven el proceso de la mejor manera.

Justificación

En el marco de referencia COSO en el componente ‘Actividades de supervisión y monitoreo’ uno de los principios que hace referencia al punto a evaluar es el principio N°16 ‘La organización selecciona, desarrolla y realiza evaluaciones continuas y/o independientes para determinar si los componentes del sistema de control interno están presentes y en funcionamiento’, dentro de este principio establece lo siguiente: es importante contar con personal competente que esté adecuadamente capacitado para los puestos que ocupan y las responsabilidades que asumen. En el campo de los RRHH, se debe especificar el nivel de competencia requerido para el desempeño de diversas tareas, así como las competencias (conocimientos y habilidades personales) que influyen asesoramiento profesional en el desarrollo, implementación y desarrollo de controles internos y evaluación de su eficacia. Luego de la firma del contrato, el profesional debe iniciar de manera práctica, teórica y metódica el proceso de capacitación y educación sobre su cargo, los valores de la empresa y el plan estratégico. Esto permite que el sistema de control interno funcione de manera efectiva porque cuenta con profesionales competentes que entienden las metas y objetivos de la empresa (COSO, 2013).

En el marco de referencia COBIT el proceso ‘BAI08 Gestionar el Conocimiento’ es responsable de la disponibilidad de información relevante, actualizada, validada y confiable que soporte todas las funciones del proceso y facilite la toma de decisiones. Planear la identificación, compilación, clasificación, mantenimiento, uso y retirada de conocimiento. Proporcionar la información necesaria para apoyar a los empleados en todas las actividades laborales para tomar decisiones informadas y aumentar la productividad. Otro proceso también responsable de validar esta sección es ‘MEA01 Supervisar, Evaluar y Valorar el Rendimiento y la Conformidad’ que resume, verifica y evalúa los indicadores objetivos de negocio, de TI y de gestión. Además, monitorea la implementación de los procesos contra el desempeño, las metas y las métricas establecidas (ISACA, 2012a).

Elección del modelo de control

Una vez finalizado el proceso de análisis de las tablas de puntajes de los dos modelos de control respecto a cada métrica planteada, se logra determinar el mejor para ser aplicado en una auditoría informática de educación media de acuerdo con sus objetivos.

La Tabla 9 muestra un análisis de los dos modelos con su promedio para cada métrica y la media general que sirve de base para la elección del modelo aplicable en la auditoría informática.

Tabla 9.

Matriz de resultados de cada métrica comparada.

Métricas	**Modelo de control**	
	COSO	**COBIT**
Propósito	4.33	4.66
Supervisión y monitoreo	5	5
Seguridad de la información	4.33	4.66
Adaptación	4.33	4
Total	17.99	18.32
Promedio	4.49	4.58

Se determinó que los dos modelos de control obtuvieron un valor promedio de 4 sobre 5, siendo mínima la diferencia a favor de COBIT, por lo tanto, los dos son apropiados utilizar en una auditoría informática ya que existe una superposición entre los dos modelos donde sus diferencias permite que sean complementarios en el entorno de TI, además los dos son útiles para el control interno.

CAPÍTULO 3

Resultados

Propuesta de guía metodológica basada en COBIT Y COSO para Auditorías Informáticas

En el presente capítulo se plantea una guía respecto a los resultados de la comparación de los marcos de referencia de COSO y COBIT; para facilitar la realización de una auditoría informática en las instituciones de Educación Media, en el cual se muestran las diferentes etapas que deben ser llevadas a cabo en una auditoría, así como formatos, encuestas que se debe aplicar a la institución para realizar un control interno de este departamento.

Departamento al que se dirige

La presente guía de auditoría está dirigida una institución de Educación Media de la ciudad de Ibarra, específicamente para el departamento de informática, ya que brinda lineamientos para evaluar las herramientas de hardware, software e instalaciones que son utilizados por los estudiantes, docentes y personal administrativo en el desarrollo de diferentes actividades académicas ya sea de manera dirigida o individual.

Responsables de aplicación

La guía propuesta puede ser aplicada por la persona designada por la institución de Educación, quien debe tener conocimientos básicos en la parte de administración, contabilidad e informática principalmente. Se sugiere considerar a personas como:

- Ingeniero en sistemas
- Profesor de informática
- Experiencia en el área de software, informática
- Ingeniero en software

Pueden intervenir varias personas que tengan los conocimientos planteados para la aplicación de la presente guía.

Limitantes de aplicación

a) Falta de apoyo por parte del director/rector de la institución.

b) En la institución no existen personas con los conocimientos básicos para realizar la auditoría.

c) La persona encargada del departamento de informática no brinde información verídica o necesaria de la situación actual.

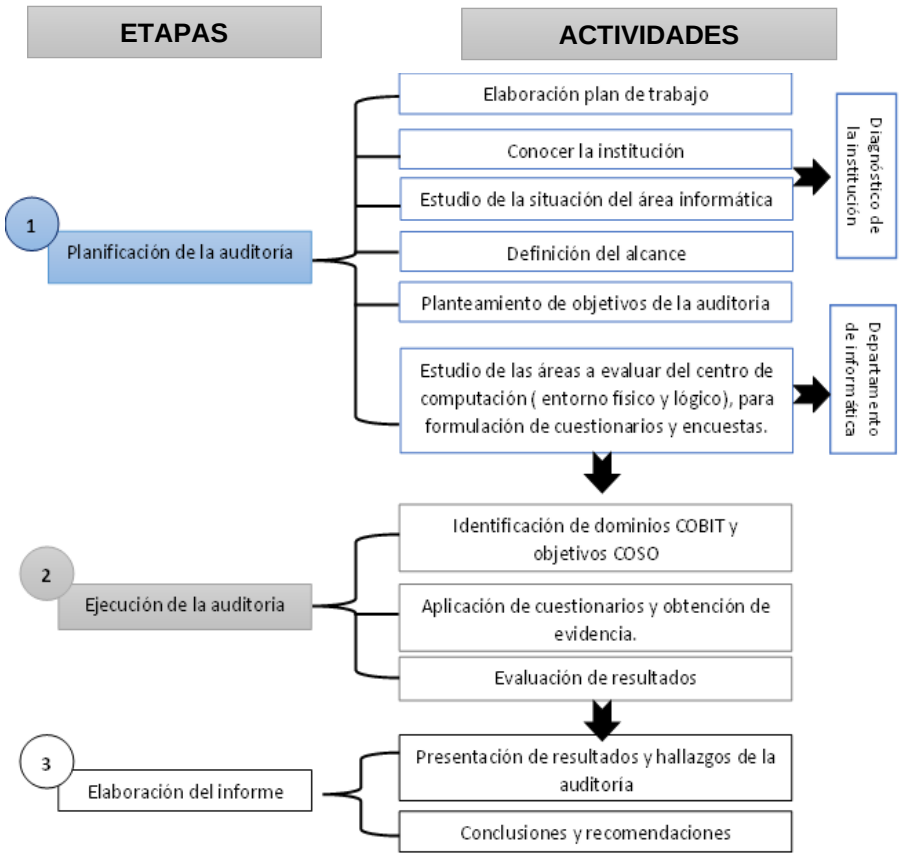
d) Falta de tiempo por parte del personal para el desarrollo de la guía.

Proceso de auditoría informática

La metodología se encuentra basada tanto en el modelo de control COSO como COBIT, mostrando los componentes principales que se deben abordar durante el proceso de auditoría del departamento de informática, para lo cual se plantean 3 etapas mostradas en la Figura 11:

Figura 11.

Etapas y actividades ejecutadas en la auditoría informática.



- **Planteamiento del cronograma de actividades**

Se establece las etapas de la auditoría, así como el tiempo que conlleva cada una de ellas. Se sugiere utilizar la Tabla 10.

Tabla 10.

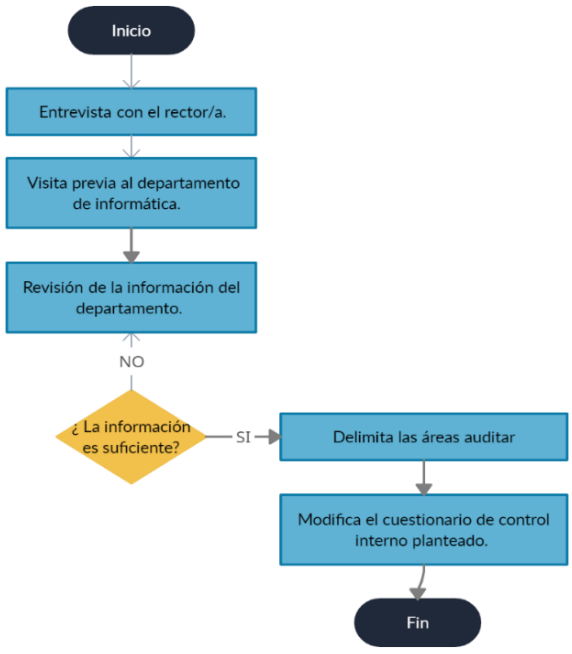
Modelo de cronograma de actividades.

N°	Actividades	Tiempo de ejecución				
		Semanas				
		S1	S2	S3	S4	S5
1	Ejecución de la matriz de planificación de auditoría					
1.1	Ejecuta la entrevista					
1.2.	Aplicación de FODA.					
1.2	Elabora o modifica el cuestionario de control interno.					
2	Ejecución de la auditoría					
2.1	Verifica los aspectos propuestos del cuestionario de control interno.					
2.2.	Elaboración de informe preliminar					
3	Elaboración de informe final					
4	Exposición de hallazgos					

ETAPA 1: Planificación de la auditoría. Para el desarrollo de la planificación de la auditoría informática se debe seguir el procedimiento detallado en la Figura 12.

Figura 12.

Proceso de la etapa de planificación de la auditoría informática.



El auditor conoce los aspectos generales de la institución educativa como: antecedentes, estructura de la organización, parte física, recursos humanos, estrategias, políticas, objetivos entre otros, así también del área específica auditar, siguiendo el procedimiento de la matriz de planificación propuesta en la Tabla 11.

Tabla 11.

Matriz de planificación.

N°	Actividad	Realizado
A	**Conocimiento y diagnóstico de la institución de Educación Media**	
A.1	Se realiza una reunión con el rector/a y se aplica una entrevista para tener conocimiento general de la misión, visión, objetivos de la institución, para ello se recomiendo aplicar la encuesta del ANEXO 1.	
A.2	Analiza la información disponible proporcionada sobre la estructura de la institución educativa.	
A.3	Conocimiento sobre las leyes, reglamentos, acuerdos relacionados con la institución educativa.	
A.4	Definición del alcance de la auditoría en la institución.	
B	**Conocimiento del departamento de informática**	
B.1	Identifica las áreas auditarse del departamento de informática.	
B.2	Analiza los informes emitidos al departamento de auditorías anteriores y el cumplimiento de las recomendaciones.	
B.3	Solicita información del inventario de hardware, software e infraestructura.	
B.4	Aplicación de FODA	
B.5	Establece los objetivos de la auditoría.	
B.6	Realización del cuestionario de control interno de auditoría al departamento de informática, se plantea utilizar el checklist propuesto en el Anexo 2.	
ELABORADO POR	**REVISADO POR**	**FECHA**

- **Aplicación de FODA**

Una herramienta utilizada para conocer la situación del departamento de informática es el FODA (Tabla 12) empleada para reconocer las fortalezas, oportunidades, debilidades y amenazas que existen en el departamento. Los elementos pueden ser tanto para hardware, software e infraestructura.

Tabla 12.
Estructura del FODA.

Fortalezas	**Debilidades**
Oportunidades	**Amenazas**

- **Planteamiento de los objetivos**

En el departamento de informática se sugiere tener en cuenta los aspectos de software, hardware, infraestructura y seguridad de la información por lo cual se proponen los siguientes objetivos para la evaluación de los siguientes parámetros.

- Verificar la seguridad de los ordenadores
- Identificar si existen políticas de acceso y protección de aplicaciones.
- Comprobar las funciones de la red.
- Comprobar que existen manuales de usuario.
- Evaluar el funcionamiento de los ordenadores.

- Comprobar que existan procedimientos para el mantenimiento de los equipos.
- Comprobar el uso apropiado de los equipos.
- Evaluar el estado y seguridad de las instalaciones.
- Evaluar la infraestructura del departamento de informática.

- **Elaboración del cuestionario de control interno**

El auditor identificará los principales objetivos de control de COBIT, para formular preguntas en base a los objetivos de la auditoría y elaborar el cuestionario de control interno. Se sugiere dividir la ejecución de la auditoría en cuatro dominios que son planteados por ISACA (2012) que son: “Alinear, planear y organizar; Construir, adquirir e implementar; Entrega, servicio y soporte; Monitorear, evaluar y valorar”.

De la misma manera el cuestionario de control interno se elaboró teniendo en cuenta los principios que establece COSO (2013). que se relacionen con el proceso de auditoría del departamento de informática, los que son: “Principio 7: Identificar y analizar los riesgos; Principio 9: Identifica y analiza cambios importantes; Principio 10: Selecciona y desarrolla actividades de control; Principio 11: Selecciona y desarrolla controles generales sobre tecnología; Principio 13: Usa información relevante; Principio 16: Conduce a evaluaciones continuas; Principio 17: Comunica y evalúa deficiencias”.

Se propone un cuestionario de control interno como se indica en el Anexo 2, en base a los 4 dominios de COBIT y de los 7 principios de COSO mencionados anteriormente y para evaluar tres componentes básicos como hardware, software e infraestructura del departamento de informática como los mostrados en la Tabla 13.

Tabla 13

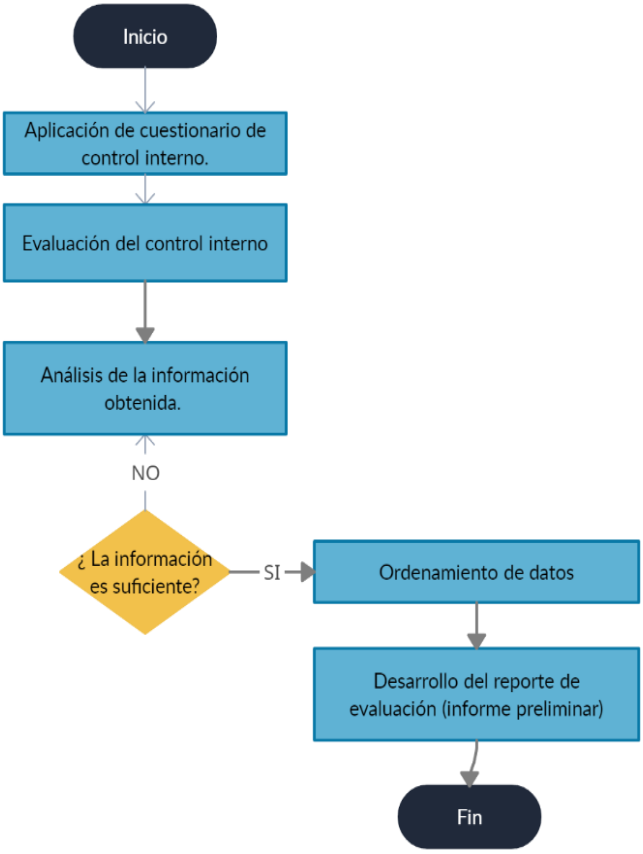
Componentes básicos para evaluar el departamento de informática de una institución de Educación media.

DEPARTAMENTO DE INFORMÁTICA	
COMPONENTE	**ASPECTOS PARA EVALUAR**
Infraestructura	❖ Condiciones eléctricas ❖ Condiciones ambientales ❖ Espacio físico ❖ Ubicación de equipos ❖ Medidas de acceso
Hardware	❖ Seguridad física ❖ Estados de los equipos ❖ Mantenimiento ❖ Actualización de equipos ❖ Frecuencia de operaciones
Software	❖ Sistemas de seguridad ❖ Operaciones ❖ Frecuencia de operaciones ❖ Identificación de archivos, registros ❖ Métodos de acceso ❖ Actualización ❖ Mantenimiento ❖ Instalación

ETAPA 2. Ejecución de la Auditoría. El proceso de ejecución de la auditoría consiste en la aplicación del cuestionario de control interno elaborado (Anexo 2), para conocer el nivel de confianza y recomendar algunas soluciones a los hallazgos. Esta etapa consiste en algunas fases como las mostradas en la Figura 13.

Figura 13.

Proceso de la ejecución de la auditoría

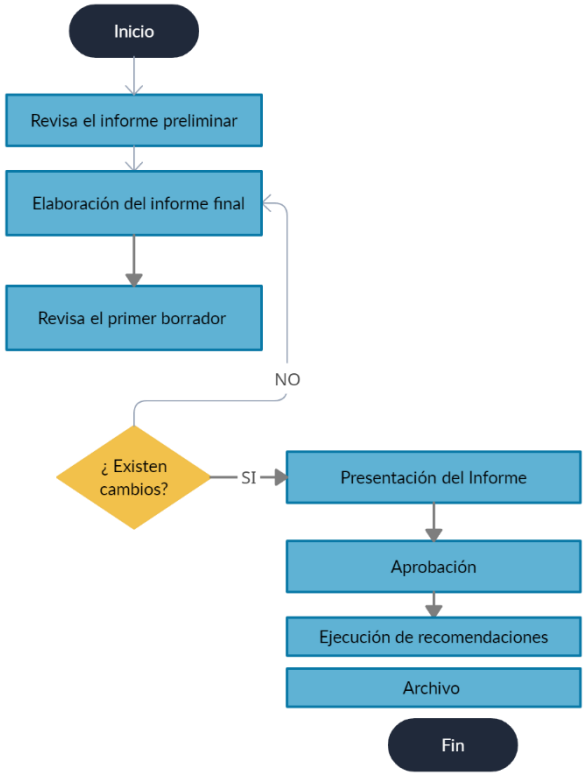


Terminada la ejecución de la auditoría, el auditor puede asignar sus datos en un reporte de evaluación como el sugerido en el Anexo 3 para cada dominio, dependiendo la tabulación de los datos, para facilitar el desarrollo de conclusiones y recomendaciones en el informe final.

ETAPA 3: Elaboración del informe final. Para la elaboración del informe final se sugiere implementar el proceso especificado en la Figura 14.

Figura 14.

Proceso de elaboración del informe final.



El auditor incluye en el informe final los aspectos que incidieron de forma negativa en el proceso de auditoría, el informe debe ser claro, preciso y concreto de los hallazgos encontrados. En el informe se deben presentar las siguientes partes:

- *Antecedentes:* Acontecimientos previos a la auditoría.
- *Situación actual:* Hallazgos encontrados, se describe el funcionamiento adecuado o inadecuado del departamento de informática.
- *Causas:* Se plantean las alternativas de porque se producen los problemas planteados.
- *Recomendaciones:* Se plantean soluciones a los problemas encontrados, siendo el director de la institución el encargado de tratar de implementar las.
- *Anexos:* Es opcional, donde se puede incluir información de los hallazgos como fotografías.

Se recomienda utilizar el modelo especificado en el Anexo 4.

Validación de la guía propuesta.

La guía propuesta para ejecutar una auditoría informática en Instituciones de educación Media es validad por el método Delphi, donde a través de encuestas se recolecta la opinión de expertos respecto a una temática, aplicando diferentes escalas como la de Likert (García et al., 2013).

Método Delphi

El método Delphi es una técnica de recopilación de información acerca de la opinión de un determinado tema en específico, para obtener una opinión en consenso a través de un análisis cualitativo y una exploración abierta de las distintas respuestas de la encuesta o cuestionario realizado (López Gómez, 2018).

Esta herramienta permite tener opiniones a partir de una temática el cual se caracteriza por ser un proceso iterativo, ya que se conoce la opinión de los expertos en diferentes ocasiones, además es importante mantener el anonimato de las respuestas basándose únicamente en las ideas, de la misma forma se puede obtener un criterio general en base a la respuesta de cada experto (Reguant Álvarez & Torrado Fonseca, 2016).

Este método tiene como proceso general 4 etapas:

1. La definición
2. Conformación del grupo de informante
3. Ejecución de rondas a consultar
4. Resultados (Reguant Álvarez & Torrado Fonseca, 2016)

Aplicación del método Delphi a la guía de auditoría informática.

Definición. La aplicación del método Delphi se basa en el problema de que las instituciones educativas no llevan un modelo de control adecuado de auditoría informática, debido a la dificultad de elegir el modelo de control más apropiado por lo cual existe una alta probabilidad de fallos en los sistemas informáticos, por lo que es necesario el planteamiento

de una guía que facilite la aplicación de la auditoría informática en base a los dos modelos de control más apropiados como son COSO y COBIT.

Conformación del grupo de informantes. Se procede a determinar el perfil de los expertos participantes en la validación, estableciéndose a expertos en el área de auditoría informática o personas interesadas en la auditoría de instituciones de educación media, es importante mencionar que la terminología de experto no se relaciona con un título sino más bien por los conocimientos que tiene sobre la temática (Almenara & Moro, 2014).

Es por ello por lo que se plantea la elección de 5 expertos, 4 relacionados con conocimientos de auditoría informática y 1 persona encargada de un departamento informático de una institución de Educación medida de la ciudad de Ibarra. No se establece los nombres de las personas encuestadas ya que el método exige confidencialidad en las respuestas.

Se planteó el acercamiento a los expertos en base a la disponibilidad de tiempo que ellos poseen actualmente para colaborar con la validación de la propuesta, la cual fue realizada a través de la plataforma de Google Forms.

Ejecución de rondas a consultar. Se elabora dos cuestionarios para evaluar la guía planteada anteriormente, valorándose en primer lugar con preguntas de criterio general que permitan validar la propuesta como las mostradas en la Tabla 14.

De la misma manera se plantean preguntas específicas acerca del cuestionario de control interno planteado en la presente guía como se muestra en la Tabla 15.

Tabla 14

Preguntas de aspecto general de la propuesta de guía de auditoría informática.

N°	Pregunta	Escala	
		Parámetro	**Abreviatura**
1	¿Considera usted que la guía contiene instrucciones claras y precisas que orientan a la persona encargada de la auditoría?	Totalmente de acuerdo	TA
		De acuerdo	DA
		Ni de acuerdo ni en desacuerdo	NAD
		En desacuerdo	D
2	¿Considera que la presente guía abarca las etapas fundamentales de la auditoría?	Totalmente de acuerdo	TA
		De acuerdo	DA
		Ni de acuerdo ni en desacuerdo	NAD
		En desacuerdo	D
3	¿Considera que el cuestionario de control interno propuesto se encuentra enmarcado dentro de los marcos de referencia COBIT y COSO (alineados)?	Totalmente de acuerdo	TA
		De acuerdo	DA
		Ni de acuerdo ni en desacuerdo	NAD
		En desacuerdo	D
4	¿Los dominios elegidos para la realización de la auditoría son los adecuados para ejecutar una auditoría informática en las unidades educativas?	Totalmente de acuerdo	TA
		De acuerdo	DA
		Ni de acuerdo ni en desacuerdo	NAD
		En desacuerdo	D
5	¿Considera que el cuestionario de control interno contiene características suficientes para obtener información esencial para un departamento de informática respecto a sus diferentes áreas?	Totalmente de acuerdo	TA
		De acuerdo	DA
		Ni de acuerdo ni en desacuerdo	NAD
		En desacuerdo	D
6	¿Los formatos planteados son adecuados para llevar a cabo la realización de la auditoría?	Totalmente de acuerdo	TA
		De acuerdo	DA
		Ni de acuerdo ni en desacuerdo	NAD
		En desacuerdo	D
7	Las partes planteadas del informe final son las correctas y suficientes para presentar de manera clara y concisa dicho informe.	Totalmente de acuerdo	TA
		De acuerdo	DA
		Ni de acuerdo ni en desacuerdo	NAD
		En desacuerdo	D
8	¿Cree usted que la guía es adecuada para aplicar en una auditoría informática de una institución de Educación Media?	Totalmente de acuerdo	TA
		De acuerdo	DA
		Ni de acuerdo ni en desacuerdo	NAD
		En desacuerdo	D

Tabla 15.

Preguntas específicas del cuestionario de control interno planteado.

N°	Pregunta	Escala
1	La actividad tiene relación con el dominio de COBIT especificado.	SI
		NO
		Observación
2	La actividad está relacionada con los principios de COSO planteados en la guía.	SI
		NO
		Observación
3	La actividad evalúa una de las áreas del departamento de informática.	SI
		NO
		Observación
4	Se debe eliminar la actividad	SI
		NO
		Observación
5	La actividad debe ser modificada	SI
		NO
		Observación

Resultados. Respecto a las preguntas de aspecto general se obtuvo los resultados mostrados en la Tabla 16 de cada uno de los expertos.

Tabla 16.

Respuestas a las preguntas de aspecto general de la guia de cada uno de los expertos.

Experto	**Pregunta**							
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**
1	TA	TA	DA	TA	DA	TA	TA	TA
2	TA	TA	TA	TA	TA	TA	TA	TA
3	TA	TA	DA	TA	DA	TA	TA	TA
4	TA	TA	TA	DA	TA	TA	TA	TA
5	DA	TA	TA	TA	DA	TA	TA	TA

Como podemos observar los expertos encuestados se encuentran de acuerdo con la guía planteada en la auditoría informática y que puede ser utilizada como guía para realizar una auditoría en el departamento de informática de una institución de educación media, se realiza las correcciones de redacción, orden y demás sugerencias planteadas obteniendo como resultado la guía presentada en la sección 3.1.

De acuerdo con el cuestionario de control interno planteado respecto a los dos marcos de referencia se obtuvieron como resultados los mostrados en la Tabla 17.

Tabla 17.

Respuestas a las preguntas específicas del cuestionario de control interno planteado.

Aspecto evaluado	**Preguntas**					**Observaciones**
	1	**2**	**3**	**4**	**5**	
La institución posee una evaluación de riesgos de las actividades que se realizan en el departamento de informática.	SI	SI	SI	NO	NO	Corregir redacción
Ha existido una gestión adecuada en el inventario del departamento por parte del administrador.	SI	SI	SI	NO	NO	
Se cuenta con un plan de mitigación de riesgos.	SI	SI	SI	NO	NO	
Existen medidas de seguridad para proteger los recursos tecnológicos del departamento de informática.	SI	SI	SI	NO	NO	
Se ha implementado una gestión administrativa en el departamento de informática.	SI	SI	SI	NO	NO	
La institución cuenta con cronograma de mantenimiento de hardware para mitigar los riesgos.	SI	SI	SI	NO	NO	
Considera que existe un adecuado mantenimiento para el software.	SI	SI	SI	NO	NO	
Se han implementado procesos para evitar el congestionamiento de la información.	SI	SI	SI	NO	NO	
El software de los ordenadores fue instalado de acuerdo con el marco de adquisición.	SI	SI	SI	NO	NO	
Se han implementado mecanismos que aseguren el buen funcionamiento de los ordenadores tanto para hardware como software.	SI	SI	SI	NO	NO	
Existe una plataforma que maneje los incidentes de seguridad computacional.	SI	SI	SI	NO	NO	

Se han implementado supervisiones a las actividades de los usuarios para conocer las acciones que se ejecutan.	SI	SI	SI	NO	NO	Corregir redacción
Existe una política de cambio de credenciales en un determinado periodo.	SI	SI	SI	NO	NO	Cambiar de dominio
Existe medidas de control para el manejo de malware.	SI	SI	SI	NO	NO	
Existen manuales de procedimiento para la administración.	SI	SI	SI	NO	NO	
El personal del departamento se encuentra capacitado y entrenado para la seguridad informática.	SI	SI	SI	NO	NO	
Existe un control de activos en el departamento de informática de la institución.	SI	SI	SI	NO	NO	Corregir redacción
La institución ha cuantificado los riesgos.	SI	SI	SI	NO	NO	
El departamento de informática tiene inventarios actualizados.	SI	SI	SI	NO	NO	Cambiar de dominio
Existen sitios de almacenamiento seguro para los respaldos de información física y virtual.	SI	SI	SI	NO	NO	
Los problemas tanto de hardware como de software son resueltos inmediatamente.	SI	SI	SI	NO	NO	
El hardware existente es el adecuado para los usuarios.	SI	SI	SI	NO	NO	
Existe un protocolo establecido para el mantenimiento de los ordenadores.	SI	SI	SI	NO	NO	
El equipo tecnológico se encuentra actualizado.	SI	SI	SI	NO	NO	
Existe un usuario backup que remplace al administrador del departamento.	SI	SI	SI	NO	NO	
Tanto los usuarios como los administradores tienen capacitaciones para el uso eficiente de los recursos.	SI	SI	SI	NO	NO	

Existen equipos de cómputo adicionales que remplacen los dañados.	SI	SI	SI	NO	NO	
Existe un protocolo de mantenimiento para el mobiliario de equipos.	SI	SI	SI	NO	NO	
La institución tiene medidas de seguridad para protección del equipo.	SI	SI	SI	NO	NO	
La distribución de los ordenadores se encuentra de acuerdo con las necesidades de los usuarios.	SI	SI	SI	NO	NO	
Existe un marco de referencia que defina la segmentación de funciones.	SI	SI	SI	NO	NO	
Existe un contrato formal para la prestación de servicios con proveedores externos.	SI	SI	SI	NO	NO	
Se mantienen actualizados los manuales de procedimientos de los usuarios.	SI	SI	SI	NO	NO	Corregir redacción
Existen procedimientos de control de cambios que aseguren la actualización del plan de continuidad con requerimientos actuales.	SI	SI	SI	NO	NO	Corregir redacción
Se cuenta con mecanismos de tolerancia de fallos para utilizar de forma adecuada la disponibilidad de los recursos.	SI	SI	SI	NO	NO	
Los usuarios cuentan con procesos alternativos en caso de emergencia.	SI	SI	SI	NO	NO	
Se encuentra restringidos el acceso a través de la autenticación de usuarios.	SI	SI	SI	NO	NO	
Existe una persona encargada para el manejo de incidentes.	SI	SI	SI	NO	NO	
Existe soporte para los usuarios.	SI	SI	SI	NO	NO	
Existen sanciones al no cumplir con las políticas de los manuales de administración.	SI	SI	SI	NO	NO	

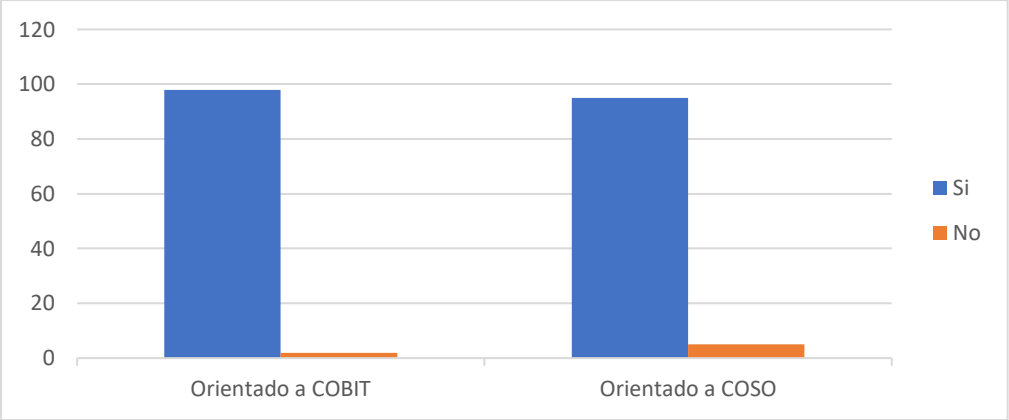
Existe una bitácora de incidentes que se generan en el departamento de informática.	SI	SI	SI	NO	NO	
Considera que la ubicación del departamento de informática es el adecuado en la institución.	SI	SI	SI	NO	NO	
El espacio físico del departamento de informática es el adecuado.	SI	SI	SI	NO	NO	
Se cuenta con un plan para monitorear y controlar los servicios de la información.	SI	SI	SI	NO	NO	
Se han efectuado procesos para detectar defectos del sistema valorando el hardware y software	SI	SI	SI	NO	NO	
Existen procedimientos que aseguren la precisión de los reportes de los datos.	SI	SI	SI	NO	NO	
Se plantean procedimientos de la divulgación de la información.	SI	SI	SI	NO	NO	Cambiar de dominio
Se comunica los hallazgos encontrados.	SI	NO	SI	SI	NO	
La institución cuenta con un protocolo que asegure la integridad y confidencialidad de los datos cuando son transmitidos a través de la red.	SI	SI	SI	NO	NO	
La institución cuenta con medidas de control de acceso al departamento de informática.	SI	SI	SI	NO	NO	
El encargado del departamento de informática mantiene un control de los equipos	SI	SI	SI	SI	SI	Eliminar aspecto a evaluar
Existen equipos para controlar y monitorear el ambiente.	NO	SI	SI	NO	NO	

Respecto a los resultados obtenidos de las encuestas a los expertos sobre el cuestionario de control interno (Figura 15) si los aspectos a evaluar se encuentran alineados a los dos modelos de control de estudio como COSO Y COBIT, se encontró que solo un 2% de los aspectos planteados no se encuentran alineados dentro del dominio correcto del marco

COBIT y COSO, por lo que estos aspectos fueron eliminados o modificados del cuestionario del cuestionario.

Figura 15.

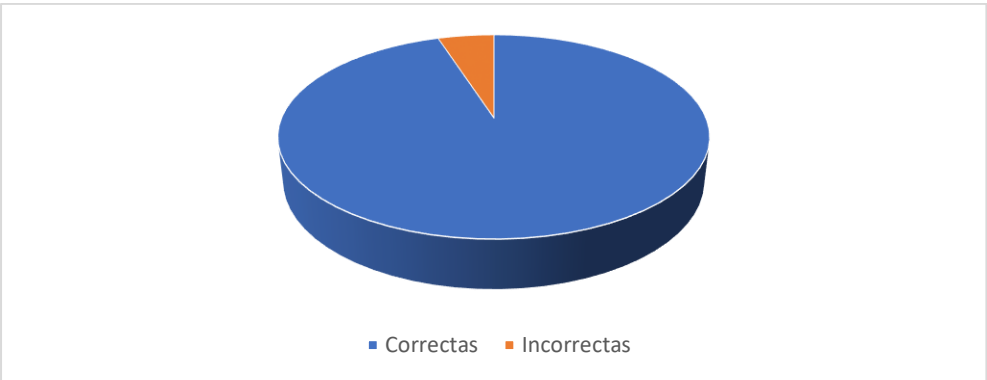
Porcentaje de actividades del cuestionario de control interno alineadas al marco COSO y COBIT.



Además de los aspectos planteados del checklist se obtiene que un 95% (Figura 16) son apropiadas para evaluar en un proceso de auditoría de un departamento de informática, además se eliminó aquellos aspectos que se sugirió que debían ser eliminados y se modificó respecto a la redacción.

Figura 16.

Porcentaje de aspectos a evaluar que son apropiados para obtener información en una auditoría del departamento de informática.



CONCLUSIONES

Por medio del análisis bibliográfico realizado se concluye que el uso de métodos de control como COSO y COBIT en la auditoría informática permite a las instituciones educativas encontrar el origen de los problemas tecnológicos que se presenten dentro de la institución y buscar diferentes soluciones, a través de un manejo adecuado de los procesos permitiendo mitigar los riesgos.

El estudio comparativo, permitió determinar que el uso de los dos modelos de control como COSO y COBIT son apropiados para utilizar en una auditoría informática, ya que al tener una superposición entre los dos modelos permite que sus diferencias complementen en el entorno de TI, siendo más efectivo integrar los dos modelos de control en una auditoría informática en instituciones de educación media.

Se estandarizó una guía de auditoría informática para instituciones de educación Media en base a los modelos de control COSO y COBIT, en la cual se indica el proceso a seguir, aspectos a evaluar, recursos, así como los formatos o documentos que se deberían utilizar en el proceso de auditoría.

A través del método de Delphi utilizando la opinión de diferentes expertos se concluye que la guía de auditoría informática propuesta y el cuestionario de control interno son apropiados para ser utilizados en un proceso de auditoría en una institución de Educación Media, obteniendo así una propuesta teórica y práctica.

RECOMENDACIONES

La comparativa de los marcos de referencia COSO y COBIT sirvió para complementar los dos modelos y poder generar una guía práctica en la que las instituciones educativas se puedan basar, por ello se recomienda que para realizar la auditoría informática se debe encargar a una persona que tenga un conocimiento técnico mínimo en todo lo que refiere a tecnología y gestión. La guía contiene aspectos específicos y simples para que la ejecución de la auditoría se lleve de la manera más compresible para el auditor.

Se recomienda que por lo menos una vez al año se realice una auditora informática ya que con el checklist establecido se pretende cubrir la mayoría de los aspectos de los dos marcos de referencia y en base al mismo implementar controles que permitan mitigar y corregir cualquier tipo de riesgo que esté presente o se pueda presentar en un futuro.

REFERENCIAS

Aguirre, C. (2015). *Elaboración e implementación de una metodología de control interno en el área informática para la Cooperativa de Ahorro y Crédito Ltda. "Loja Internacional*.

Alayo, Z. (2016). *El Marco Integrado de Control Interno COSO 2013 y su influencia en la Gestión Empresarial de las pequeñas empresas mineras en el Perú*. http://hdl.handle.net/10757/621003

Alcedo, C. (2018). *PROPUESTA DE MEJORAMIENTO DEL SISTEMA DE CONTROL INTERNO ADMINISTRATIVO-FINANCIERO APLICADO COSO III DE LA EMPRESA NONOLÁCTEOS CIA*.

Almenara, J. C., & Moro, A. I. (2014). Empleo del método Delphi y su empleo en la investigación en comunicación y educación. *EDUTEC. Revista electrónica de tecnología educativa*, *48*, a272–a272.

Asociación Española de Contabilidad y Administración de EmpresasServicio Infoaeca. (2017). *Auditoria Informática*.

Baldeón, J., & Coronel, A. G. (2012). *PLAN MAESTRO DE SEGURIDAD INFORMÁTICA PARA LA UTIC DE LA ESPE CON LINEAMIENTOS DE LA NORMA ISO/IEC 27002*.

Basantes, A., Gallegos, M., Guevara, C., Jácome, A., Posso, Á., Quiña, J., & Vaca, C. (2016). *Comercio electrónico*.

Bendermacher, J. (2017). *Auditoría interna y auditoría externa Funciones distintivas para la administración de una organización*. www.theiia.org/gpi.

Biler-Reyes, S. A. (2017). Auditoria. Elementos esenciales. *Dominio de las Ciencias*, *3*(1), 138–151.

Calderón, L. (2018). *Suguridad informática y seguridad de la información*.

Canto de Gante, Á. G., Sosa González, W. E., Bautista Ortega, J., Escobar Castillo, J., & Santillán Fernández, A. (2020). Escala de Likert: Una alternativa para elaborar e interpretar un instrumento de percepción social. *Revista de la alta tecnología y sociedad*, *12*(1).

Chávez, S. (2018). El Concepto de Riesgo. En *Recursos Naturales y Sociedad* (Vol. 4, Número 1). https://doi.org/10.18846

Chisag, V. (2017). *Realización de Beneficios Obtimización del Riesgo*.

Chuquimarca, M., Narvaez Zurita, C., Ormaza Andrade, J., & Erazo Álvarez, J. (2020). El futuro de la auditoría y las innovaciones tecnológicas. *Especial*, *6*(1), 316–339.

Committee of Sponsoring Organizations of the Treadway Commission. (2013). *Control interno - Marco Integrado*.

Consejo de Auditoría Interna del Gobierno de Chile. (2016). *IMPLANTACIÓN, MANTENCIÓN Y ACTUALIZACIÓN DEL PROCESO DE GESTIÓN DE RIESGOS EN EL SECTOR PÚBLICO*.

COSO. (2013). *MODELO COSO III--MARCO INTEGRADO DE CONTROL INTERNO*. www.auditool.org

de Haes, S., Van, W., & Debreceny, R. (2013). COBIT 5 and enterprise governance of information technology: Building blocks and research opportunities. *Journal of Information Systems*, *27*(1), 307–324. https://doi.org/10.2308/isys-50422

Dickins, D., & Fay, R. G. (2017). COSO 2013: Aligning internal controls and principles. *Issues in Accounting Education*, *32*(3), 117–127.

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

Figueroa-Suárez, J. A., Rodríguez-Andrade, R. F., Bone-Obando, C. C., & Saltos-Gómez, J. A. (2018). La seguridad informática y la seguridad de la información. *Polo del conocimiento*, *2*(12), 145–155.

Florian. (2015). *LA AUDITORIA, ORIGEN Y EVOLUCION ¿POR QUE EN COLOMBIA SOLO SE CONOCE A TRAVÉS DE LEYES?*

García, M. M., Suárez, M., & li, M. (2013). El método Delphi para la consulta a expertos en la investigación científica Delphi method for the expert consultation in the scientific research. En *Revista Cubana de Salud Pública* (Vol. 39, Número 2). http://scielo.sld.cu

Giraldo, S. (2015). *Modelo de medición bajo la metodología ajustada PAM de la implementación del Capítulo IV Título I Parte I de la circular básica Jurídica 29 de 2014 de la superintendencia financiera mapeado bajo el modelo COSO y COBIT 5*. *53*(9), 1689–1699.

Gonzales, R. (2013). *Marco Integrado de Control Interno. Modelo COSO III Manual del Participante*.

Granda, P. D., Imbaquingo, D. E., Ortega, C. M., Guevara, C. P., & Pusdá, M. R. (2017). *Innovación Tecnológica*.

Imbaquingo, D. E. (2017). *Tecnologías Aplicadas a la Ingeniería. III Jornadas de Ingeniería*.

ISACA. (2012a). *Procesos Catalizadores*. http://linkd.in/ISACAOfficial

ISACA. (2012b). *Un Marco de Negocio para el Gobierno y la Gestión de las TI de la Empresa*. http://linkd.in/ISACAOfficial

ISO. (2013). *GUÍA DE IMPLANTACIÓN PARA LA SEGURIDAD DE LA INFORMACIÓN*.

ISO/IEC. (2016). *TECNOLOGÍAS DE LA INFORMACIÓN — TÉCNICAS DE SEGURIDAD — SISTEMAS DE GESTIÓN DE SEGURIDAD DE LA INFORMACIÓN – DESCRIPCIÓN GENERAL Y VOCABULARIO.*

Jácome, A., Herrera, E., Herrera, I., Caraguay, J., Basantes, A., & Ortega, M. (2019). *Análisis temporal y pronóstico del uso de las TIC, a partir del instrumento de evaluación docente de una Institución de Educación Superior*. https://bit.ly/350Feve

Jácome, J., Pusdá, M., & Imbaquingo, D. (2017). *Fundamentos de Auditoría Informática basada en riesgos*.

Jafeth, A., & Mosquera, M. (2018). *Current status of the security audit in higher education information systems*.

Jara Pérez, D. F. (2018). *Valoración y Plan de Tratamiento de Riesgos de Seguridad de la Información para los Procesos Incluidos en el Alcance del SGSI del Cliente TGE de la Empresa ASSURANCE CONTROLTECH*.

León, A. J. v., Mora, A. J. E., Huilcapi, M. M. R., Tamayo, H. A. del P., & Armijos, M. C. A. (2018). COBIT como modelo para auditorías y control de los sistemas de información. *Polo del Conocimiento*, *3*(4), 17. https://doi.org/10.23857/pc.v3i4.439

Londoño, L., & Nuñez, M. (2010). *Desarrollo de la administración de riesgos. Diagnóstico en grandes empresas del Área Metropolitana del Valle de Aburrá*. http://www.redalyc.org/src/inicio/ArtPdfRed.jsp?iCve=21520993004

López Gómez, E. (2018). El método Delphi en la investigación actual en educación: una revisión teórica y metodológica. *Educación XX1: revista de la Facultad de Educación*.

Luna, O. F. (2013). *Sistemas de Control Interno Para Organizaciones*. Instituto de Investigación en Accountability y Control. https://books.google.com.ec/books?id=plsiU8xoQ9EC

Mangalaraj, G., Singh, A., & Taneja, A. (2014). *IT governance frameworks and COBIT-a literature review*.

Manrique, J. (2019). *Introducción a la auditoría*.

Méndez, H. (2017). La auditoría: concepto, clases y evolución. En *Auditoria, grado Superior* (McGraw Hill, Vol. 1).

Minchala, P. (2016). *Estudio comparativo de las metodologías COBIT 5 y COSO III para la gestión del riesgo de TI*. *4*(4).

Ministerio de Finanzas. (2017). *METODOLOGÍA PARA LA GESTIÓN INTEGRAL DE RIESGOS*.

Moeller, R. R. (2013). *Executive's guide to Coso internal controls: understanding and implementing the new framework*. John Wiley & Sons.

Montes Villanueva, L. M. (2018). *Auditoría financiera interna y externa*.

Muñoz, C. (2012). *Auditoria En Sistemas Computacionales*. www.pearsonedlatino.com

Nuñez, K. (2014). *Diseño de un programa de auditoría tributaria preventiva igv-renta para empresas comercializadoras de combustible líquido en la ciudad de Chiclayo*.

Parra, C. R. (2018). La Agenda 2030 y sus Objetivos de Desarrollo Sostenible. En *Revista de Derecho Ambiental* (Número 10). https://doi.org/10.5354/0719-4633.2018.52077

Pérez, S., Granados, S., & Estupiñán, P. (2018). *Lo que usted debe saber sobre riesgo tecnológico*. www.gestiondelriesgo.gov.co

Piattini, M. (2016). *AUDITORIA INFORMÁTICA (Jn enfoque práctico 2" EDICIÓN AMPLIADA Y REVISADA*. www.FreeLibros.me

Pin, J. (2020). *AUDITORÍA INFORMÁTICA A LA UNIDAD EDUCATIVA "GENERAL ANTONIO ELIZALDE BUCAY, DEL CANTÓN BUCAY", PROVINCIA DEL GUAYAS, PERÍODO 2018*.

Prieto, C. B. J. (2018). El uso de los métodos deductivo e inductivo para aumentar la eficiencia del procesamiento de adquisición de evidencias digitales. *Cuadernos de Contabilidad*, *18*(46). https://doi.org/10.11144/javeriana.cc18-46.umdi

Quinaluisa Morán, N. V., Ponce Álava, V. A., Muñoz Macías, S. C., Ortega Haro, X. F., & Pérez Salazar, J. A. (2018). El control interno y sus herramientas de aplicación entre COSO y COCO. *Cofin Habana*, *12*(1), 268–283.

Ramos, M. (2018). *Auditoría Informática*.

Reguant Álvarez, M., & Torrado Fonseca, M. (2016). El método delphi. *REIRE. Revista d'Innovació i Recerca en Educació, 2016, vol. 9, num. 2, p. 87-102*.

Sendón, J., Herrera-Tapia, J., Fernández-Capestany, L., Del, M., Felipe, R. C., Chancay-García, L., & García-Quilachamín, W. (2020). *Análisis comparativo entre distintas metodologías para la realización de auditorías de seguridad informática, aplicando el Proceso Analítico Jerárquico (AHP)*.

Silva, A., & Mata, M. (2015). *La llamada Revolución Industrial*. Universidad Católica Andrés Bello. https://books.google.com.ec/books?id=YmbEneoFEI0C

Vega, E. (2021). *SEGURIDAD DE LA INFORMACIÓN*.

Zambrano, S. M. Q., & Valencia, D. G. M. (2017). Seguridad en informática: consideraciones. *Dominio de las Ciencias*, *3*(3), 676–688.

ANEXOS

Anexo 1. Encuesta al rector/a de la institución.

DIAGNÓSTICO DE LA INSTITUCIÓN	
Nombre de la persona encargada de proporcionar la información:	
Nombre institución auditada:	
Ciudad:	**Departamento:** Informática

ASPECTOS GENERALES DE LA INSTITUCIÓN.

1. **¿Cuál es la historia de la institución educativa?**

_____
_____

2. **¿Cómo está organizada la institución?**

_____
_____

MISIÓN

3. **¿Cuál es la misión de la institución?**

_____
_____

VISIÓN

4. **¿Cuál es la visión de la institución?**

_____
_____

OBJETIVOS

5. **¿Qué objetivos tiene la institución?**

_____
_____

ESTRUCTURA ORGANIZATIVA DEL CENTRO DE INFORMÁTICA

6. **¿Cuál es la estructura organizativa del centro de computación?**

_____
_____

7. **Solicitar el inventario del departamento de informática de:**

   Infraestructura:

   Hardware:

   Software:

Anexo 2. Modelo de cuestionario de control interno para auditoría informática en instituciones de Educación Media.

Nombre de la Institución:					
Fecha de la auditoría					
Departamento auditado		Informática			
DURACIÓN DE LA AUDITORÍA					
DESCRIPCIÓN	El presente documento tiene como finalidad encontrar y analizar controles específicos en las unidades académicas de educación media.				
ALCANCE	Se analizará y evaluará aspectos referentes a cuatro dominios de COBIT 5 y COSO.				
CUESTIONARIO DE CONTROL INTERNO					
Nro.	**DESCRIPCIÓN**	**SI**	**NO**	**AUDITOR**	**OBSERVACIONES**
1	**ALINEAR, PLANEAR Y ORGANIZAR**				
1.1	La institución posee una evaluación de riesgos de las actividades que se realizan en el departamento de informática.				
1.2	La institución ha cuantificado los riesgos.				
1.3	Se cuenta con un plan de mitigación de riesgos.				
1.4	Existen medidas de seguridad para proteger los recursos tecnológicos del departamento de informática.				
1.5	Se ha implementado una gestión administrativa en el departamento de informática.				
TOTAL					
2	**CONSTRUIR, ADQUIRIR E IMPLEMENTAR**				
2.1	La institución cuenta con cronograma de mantenimiento de hardware para mitigar los riesgos				
2.2	Considera que existe un adecuado mantenimiento para el software				
2.3	Se han implementado procesos para evitar el congestionamiento de la información.				
2.4	El software de los ordenadores fue instalado de acuerdo con el marco de adquisición.				

2.5	Se han implementado mecanismos que aseguren el buen funcionamiento de los ordenadores tanto para hardware como software.				
2.6	Existe una plataforma que maneje los incidentes de seguridad computacional.				
2.7	Se han implementado supervisiones a las actividades de los usuarios para conocer las acciones que se ejecutan.				
TOTAL					
3	**ENTREGA, SERVICIO Y SOPORTE**				
3.1	Existen una política de cambio de credenciales en un determinado periodo				
3.2	Existe medidas de control para el manejo de malware.				
3.3	Existen manuales de procedimiento para la administración				
3.4	El personal del departamento se encuentra capacitado y entrenado para la seguridad informática.				
3.5	Existen un control de activos en el departamento de informática de la institución				
3.6	Ha existido una gestión adecuada en el inventario del departamento por parte del administrador.				
3.7	El departamento de informática tiene inventarios actualizados				
3.8	Existen sitios de almacenamiento seguro para los respaldos de información física y virtual.				
3.9	Los problemas tanto de hardware como de software son resueltos inmediatamente.				
3.10	El hardware existente es el adecuado para los usuarios.				
3.11	Existe un protocolo establecido para el mantenimiento de los ordenadores.				
3.12	El equipo tecnológico se encuentra actualizado.				

3.13	Existe un usuario backup que remplace al administrador del departamento.				
3.14	Tanto los usuarios como los administradores tienen capacitaciones para el uso eficiente de los recursos.				
3.15	Existen equipos de cómputo adicionales que remplacen los dañados.				
3.16	Existe un protocolo de mantenimiento para el mobiliario de equipos.				
3.17	La institución tiene medidas de seguridad para protección del equipo.				
3.18	La distribución de los ordenadores se encuentra de acuerdo con las necesidades de los usuarios.				
3.19	Existe un marco de referencia que defina la segmentación de funciones.				
3.20	Existe un contrato formal para la prestación de servicios con proveedores externos.				
3.21	Se mantienen actualizados los manuales de procedimientos de los usuarios.				
3.22	Existen procedimientos de control de cambios que aseguren la actualización del plan de continuidad con requerimientos actuales.				
3.23	Se cuenta con mecanismos de tolerancia de fallos para utilizar de forma adecuada la disponibilidad de los recursos.				
3.24	Los usuarios cuentan con procesos alternativos en caso de emergencia.				
3.25	Se encuentra restringidos el acceso a través de la autenticación de usuarios.				
3.26	Existe una persona encargada para el manejo de incidentes.				
3.27	Existe soporte para los usuarios.				
TOTAL					

4	**MONITOREAR, EVALUAR Y VALORAR**				
4.1	Existen sanciones al no cumplir con las políticas de los manuales de administración.				
4.2	Existe una bitácora de incidentes que se generan en el departamento de informática.				
4.3	Considera que la ubicación del departamento de informática es el adecuado en la institución.				
4.4	El espacio físico del departamento de informática es el adecuado.				
4.5	Se cuenta con un plan para monitorear y controlar los servicios de la información.				
4.6	Se han efectuado procesos para detectar defectos del sistema valorando el hardware y software				
4.7	Existen procedimientos que aseguren la precisión de los reportes de los datos.				
4.8	Existen procedimientos de la divulgación de la información.				
4.9	La institución cuenta con un protocolo que asegure la integridad y confidencialidad de los datos cuando son transmitidos a través de la red.				
4.10	La institución cuenta con medidas de control de acceso al departamento de informática.				
4.11	Existen equipos para controlar y monitorear el ambiente.				
TOTAL					

Elaborado por:	**Revisado por:**	**Fecha:**

Anexo 3. Modelo de informe preliminar.

Nombre de la Institución:							
Fecha de la auditoría							
Departamento auditado							
DURACIÓN DE LA AUDITORÍA:							
DESCRIPCIÓN:							
INFORME PRELIMINAR							
N°	**Hallazgo**	**Causas del hallazgo**	**Repercusiones**	**Alternativas de Solución**	**Recomendaciones**	**Fecha probable de implementación**	**Responsable de la recomendación**
Elaborado por			**Revisado por**			**Fecha**	

Anexo 4. Modelo de informe final.

INFORME FINAL

SEÑOR(a) RECTOR(a)
INFORMA:
EVALUACIÓN DE CONTROL INTERNO

1. ANTECEDENTES

……
……..

2. OBJETIVOS

……
……

3. ALCANCE

……

……

4. LIMITACIONES

……

……

5. COMENTARIOS

Observaciones (numeradas):

Situación actual:

……

……

Causas:

……

……

6. Recomendaciones:

……

……

Firma auditor