UNIVERSIDAD CATÓLICA DE CUENCA

Comunidad Educativa al Servicio del Pueblo

UNIDAD ACADÉMICA DE TIC

CARRERA DE INGENIERIA DE SISTEMAS

ANALISIS COMPARATIVO DE LA NORMA 410 DE CONTROL INTERNO DE LA CONTRALORIA GENERAL DEL ESTADO CON COBIT5

TRABAJO DE TITULACIÓN O PROYECTO DE INTEGRACIÓN CURRICULAR PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN SISTEMAS

AUTOR: ROSALIA XIMENA CONTRERAS ABAD

DIRECTOR: ING. CESAR ALVARITO CORONEL GONZAEZ

AZOGUES - ECUADOR

2020

Yo me gradué en los 50 años de la Cato!
Yo me gradué en los 50 años de la Cato!

UNIVERSIDAD CATÓLICA DE CUENCA

Comunidad Educativa al Servicio del Pueblo

UNIDAD ACADÉMICA DE TIC

CARRERA DE INGENIERIA EN SISTEMA

ANALISIS COMARATIVO DE LA NORMA 410 DE CONTROL INTERNO DE LA CONTRALORIA GENERAL DEL ESTADO CON COBIT 5

TRABAJO DE TITULACIÓN O PROYECTO DE INTEGRACIÓN CURRICULAR PREVIO A LA OBTENCIÓN DEL TÍTULO DE INGENIERO EN SISTEMAS

AUTOR: ROSALÍA XIMENA CONTRERAS ABAD

DIRECTOR: ING. CESAR ALVARITO CORONEL GONZALEZ

AZOGUES - ECUADOR

2020

Yo me gradué en los 50 años de la Cato!

Agradecimientos

Mi agradecimiento a Dios, por permitirme sonreír ante todos mis logros que son resultados de tu ayuda, gracias a ti esta meta esta cumplida.

A mis padres y a mi hermano a quienes les debo todo lo que soy, por ser un pilar fundamental en mi vida y por haberme apoyado siempre, gracias por cada consejo, por cada motivación que me dan día a día; gracias por siempre desear y anhelar lo mejor para mi vida; gracias por cada una de sus palabras que me guiaron durante mi vida.

Al mi tutor Ing. Alvarito Coronel por su guía y sus concejos por cada detalle y momento dedicado para aclarar cualquier tipo de duda que me sugiera para el desarrollo de la presente tesis, al igual que a mis compañeros y docentes con los que he compartido momentos importantes en este ciclo de estudio.

Gracias a la universidad por haberme permitido formarme, a los docentes de mi facultad por invertir su tiempo y brindar su aporte a mi proyecto de tesis.

Dedicatoria

Esta tesis la dedico a mis seres más queridos mis padres Segundo y Rosa por su apoyo incondicional por ser los principales promotores de mis sueños por confiar y creer en mi y en mis sueños, que con mucho sacrificio y abnegación supieron entregar todo de si, todos sus esfuerzos para así llegar a obtener mi anhelado título.

La dedico a mi hermano Juan por estar siempre apoyándome en cada paso que doy, él es el principal cimiento para la construcción de mi vida profesional, sentó en mi la base de responsabilidad y deseos de superación, en el tengo el espejo en el cual me quiero reflejar, sus virtudes y su gran corazón me llevan a admirarle cada día más.

Resumen

La seguridad de la información permite proteger y salvaguardar la información de las organizaciones por medio de medidas preventivas y reactivas que deben estar actualizadas para poder dirigir, controlar y asegurar la información, para esto existe normativas como Cobit 5 que representa un marco de referencia donde la misión es "Investigar, desarrollar publicar y proveer un conjunto de información con autoridad, actualizados, de carácter internacional y aceptados generalmente para el uso diario de gerentes de empresas y auditores"**.** Por otro lado, la norma 410 de la Contraloría General Del Estado tiene como objetivos estratégicos "fortalecer la gestión del control, mejorar el potencial humano, optimizar la gestión Interna", dando a conocer su misión de "controlar los recursos públicos para precautelar su uso eficiente, en beneficio de la sociedad".

En la presente investigación se realizó una comparación de los procesos de Cobit 5 versus la normativa 410 de control interno administrada para el uso de tecnología de la información que utiliza la Contraloría General Del Estado, se revisó las normativas en lo inherente con la seguridad de la tecnología de la información, para determinar el porcentaje de concordancia entre la norma nacional y una norma internacional, se empleó un análisis grafico estadístico a través de un método comparativo que nos dan a conocer los resultados finales. Los más relevantes se encontraron en el plan de contingencia, la seguridad de tecnologías de información y la administración de soporte de tecnología de información de la norma 410, teniendo altas similitudes con los procesos de gestión de información de Cobit 5.

Palabras Claves: Seguridad, Información, Cobit, Control Interno, Tecnología, Contraloría General Del Estado.

Abstract

Data security make it possible to safeguard and protect the companies´ data by using both preventive and reactive actions that require updating in order to manage, control and secure the data, for this there are regulations such as Cobit 5 which provide a reference framework where the role is to "investigate, develop, publish and provide a set of authorized, updated, world-wide and widely recognized data for day-to-day use by business managers and auditors". On the hand regulation 410 of the General States Comptroller´s Office has as its strategic aims "to strengthen management control, to enlaces its human potential, and to optimize its own internal management", stating its mission to "control public resources to safeguard their efficient use, in benefit of society".

In the current research, a comparison was between the processes of Cobit 5 and the 410 regulation of internal control provided by the State Comptroller´s Office on the use of IT, and the regulation concerning IT security were reviewed, to determine the degree of agreement between national and international standards, a statistical graphical analysis was employed through the use of a comparative method which provides the final results. The most significant were found in the emergency plan, IT security and IT support administration of the 410 regulation, with high similarities to the processes of information management of Cobit 5.

KEYWORDS: Security, Information, Cobit, Internal Control, Technology, General state Comptroller´s Office.

INDICE GENERAL

Índice de Tablas

Índice de Imágenes

Índice de Anexos

Capítulo 1

1. Introducción

Hoy en día la información forma parte de los importantes recursos de una organización, con el adecuado proceso de datos que sobrelleva a producir información importante y valiosa que conlleva a una adecuada toma de decisiones obteniendo información precisa, oportuna y completa donde las organizaciones deben obtener sistemas tecnológicos renovados y preparados ya que estos consiguen favorecer a reprender un inconveniente con mayor precipitación.

La necesidad del control interno como parte de un proceso administrativo ayuda a advertir, revelar y reprender viables anormalidades en la gestión de tecnologías de la información que consiga trastornar el normal progreso de las actividades en la organización.

El control interno como parte de proceso administrativo es fundamental ya que de no existir no podría conocerse, solo planificando, organizando y ejecutando se ha realizado de manera correcta y se encuentra funcionando bien.

La normativa gubernamental es clave para que el estado pueda ejercer el control interno entidades y organismos del estado con el fin de lograr los objetivos de cada entidad con eficiencia y eficacia, establecido por la constitución de la república del Ecuador en el apartado 211, donde indica que la Contraloría General Del Estado es una corporación técnica que administra el control del manejo de recursos estables, entes jurídicos de derecho privado que dispongan de recursos públicos, ejerce el control del cumplimiento de la normativa gubernamental para garantizar la correcta utilización de los recursos públicos.

Las normas del control interno se componen de pautas generales presentadas por la contraloría general del estado, encaminadas a originar una correcta administración de los recursos públicos y el adecuado funcionamiento administrativo de las entidades y organismos del sector público, con el objetivo de analizar la efectividad, eficiencia y economía en la gestión institucional.

Considerando que las normas de control interno de información busca originar el adecuado manejo de los sistemas computarizados que procesan la información generada por las entidades, las autoridades de las entidades públicas, tienen la responsabilidad en el control interno de establecer políticas y ordenamientos para operar los inseguridades en la obtención de los objetivos institucionales, salvaguardar y mantener los activos y organizar las revisiones de acceso a los sistemas de información; las actividades de control se dan en toda la organización, en todos los niveles y en todas los cargos y funciones. (Contraloría general del estado, 2009)

"La evaluación de los recursos y procesos de TI son importantes para el buen funcionamiento de una organización y para el aseguramiento de supervivencia en el mercado"

La Contraloría General Del Estado frente a las modificaciones realizados en la legislación ecuatoriana que se ha elaborado a partir de la manifestación de la nueva constitución de la republica del ecuador, "reformas de la ley orgánica y normativas para los sectores ambiental, eléctrico, administrativo, talento humano información pública, finanzas y entre otras", considera que es oportuno reestablecer las políticas de control interno para emprender a las entidades, organismos del sector público y entes jurídicos que dispongan de un marco normativo de la cual pueda llegar a desempeñar sus objetivos, es por eso que las entidades públicas están basadas en la norma 410 orientada al control interno de tecnología de la información; dicha norma se encuentra establecida con diecisiete sub normativas cada una de ellas tiene diferente propósito para el control de la información.

Mientras que Cobit 5 "objetivos de control para la información y la tecnología relacionada" es un marco de referencia aprobado internacionalmente encaminado a las buenas prácticas para el control interno de información tecnológica conformado por un marco de dominios ayudando a las empresas a salvaguardar las brechas entre los riegos que conllevan, necesidades de

intervención y semblantes propiamente técnicos, audita la gestión de control de los sistemas de información.

Está encaminado al control interno dando protección a las funciones de gobierno de TI, está compuesto por 37 procesos de gestión y se encuentran representados en cuatro dominios **"**Planificar y Organizar, Adquirir e implementar, Entrega y soporte, Monitorizar y evaluar**."**

El modelo cobit 5 vincula tecnología informática, consolida estándares de fuentes globales, se emplea a los sistemas de información de toda la organización, que se encuentra establecido en la teoría de que los recursos de TI requieren ser gobernados por un conjunto de procesos para abastecer la información oportuna y confiable que necesita una organización. (Contraloría General Del Estado, 2016)

La gestión de procesos es un factor clave compuesto por metodologías y tecnologías para lograr los objetivos empresariales y a su vez el cumplimiento de la normativa gubernamental, implicando a una necesidad de cambio en la cultura organizacional. Mediante el acuerdo 1580 "la secretaria nacional de administración pública emite una norma técnica para la administración por procesos", esta norma puede servir como marco metodológico para todas las empresas públicas contribuyendo en el progreso de la gestión de empresas.(Escuela de Administración Finanzas, 2007)

Como se mencionó anteriormente la norma nacional de control interno 410 para las tecnologías de la información emitidas por la Contraloría General Del Estado se encarga de confrontar el apropiado uso y control de los procesos institucionales, "se encuentra relacionada con las normas internacionales como los objetivos del control para la información y tecnologías relacionadas (Cobit 5)" administrada para el manejo de las tecnologías de información que busca la implementación de un gobierno de TI que computarice los procesos de las áreas trascendentales, entrega de valor, gestión de riesgos, gestión de recursos, comprobación de desempeño.

1.1 Antecedentes

En 1967 se modificó la denominación de “Contraloría General de la Nación” por “Contraloría General del Estado”. Esta reforma se manifestó ante la insuficiencia de organizar las funciones institucionales con la determinación del estado como “organización política, se estableció como el organismo de fiscalización y contabilidad de la hacienda pública”.

En 1977 se consignó la ley orgánica de administración financiera y remplazó a la ley Orgánica de hacienda fue planeada bajo una orientación sistemática de los diferentes mecanismos de la administración financiera. Se marcaron las medidas primordiales sobre la contraloría general del estado que debía manifestar los reglamentos técnicos de control interno como parte de las normas sustitutas de los sistemas de contabilidad y de control que le pertenecía expresar al organismo de control.

En noviembre del mismo año con acuerdo # 000971, la contraloría general del estado consignó los primeros reglamentos técnicos de control interno juntamente con las “políticas de contabilidad, Normas Técnicas de Contabilidad y Políticas de Auditoria del Sector Público”. Esta normativa fue renovada en abril de 1994 con la expedición del acuerdo 017-CG

La contraloría dejo de ser la oficina de contabilidad e intervención fiscal para formar parte de un organismo superior de control de los recursos de las entidades del sector público, con la facultad de observar los procedimientos financieros y administrativos de las entidades públicas o privadas que apliquen las auditorias financieras o auditorias operacionales.

Con la intención de certificar la correcta y eficiente administración de los recursos y bienes de las entidades y organismos del sector público ecuatoriano en el año 2002, la contraloría general del estado expuso los estatutos de control interno, que establecen lineamientos encaminados al cumplimiento de dichos objetivos.

El apartado 212 de la constitución de la republica del ecuador da a conocer lo siguiente "facultad al controlador general para expedir la normativa para el cumplimiento de sus funciones, mediante el acuerdo 047-CG se expidió el reglamento de uso y control de los recursos informáticos y de telecomunicación de la contraloría general de estado". (Contraloría General Del Estado, 2016)

El manejo de los medios informáticos que se utiliza como un intermedio para procesar, recolectar, trasladar información y el uso de aplicaciones electrónicas se ha transformado en un mecanismo fundamental para el funcionamiento de la sociedad; es por eso que se debe actualizar las normativas jurídicas para salvaguardar el acceso a la información.

> "En el artículo 4 da a conocer sobre la política de seguridad de información donde la contraloría general del estado declara y establece que la información digital institucional, en soporte digital, constituye un activo institucional que debe ser administrado y protegido, garantizando su disponibilidad, confidencialidad e integridad por parte de todos sus servidores/as, en cumplimiento de las normas determinadas" (Contraloría General Del Estado, 2016)

Es por eso que El Instituto de Gobierno de TI fue desarrollado por la Auditoria de Sistema de Información y de la Asociación de Control (ISACA) y su función inscrita en 1998 para mejorar en el entendimiento y la protección de los principios de gobierno de TI, el instituto de gobierno de TI adquirió una serie de liderazgos en el rol de desarrollo de la publicación.

Cobit está basado inicialmente en los objetivos de control de ISACA que se ha ido optimizando con los actuales y procedentes modelos internacionales a nivel técnico, profesional y determinados de la industria. Los objetivos de control se han desarrollado para el estudio de sistemas de información de toda la empresa.

El proyecto Cobit se organizó por primera vez en 1995 con el fin de establecer un mayor impacto global y duradero sobre el campo de los negocios y de los controles de sistemas de información. (Cobit, 2014)

La progresiva complicación de las tecnologías de información, la dependencia de ellas por parte de las organizaciones encamina a la necesidad de disponer con un marco genérico de control, gestión y gobierno de TI independientemente de la tecnología que certifique el alcance de los objetivos de la organización, comprimiendo riesgos derivados de las propias TI.

> "La publicación de los objetos de control originales, en 1992, y las posteriores ediciones de Cobit (primera en 1996, y segunda en 1998) marcaron una época en la que la orientación principal de la asociación era el control interno y la Auditoria de sistemas" (Byron Napoleón Cadena Oleas & Irene García Rondón, 2016)

1.2 Descripción del Problema

La contraloría general del estado es la máxima corporación de control fiscal ecuatoriano encargado de la inspección y la utilización de los recursos estatales administrando el régimen de control, fiscalización y auditoria del estado con el propósito de examinar, comprobar y valorar la utilización de recursos, administración y custodia de bienes públicos. El departamento de tecnologías de información y comunicación es el responsable de mantener y proteger la información de la organización que actualmente se encuentra basada en las normas 410 denominada tecnologías de la información. No existe una comparación que se fundamente con la norma nacional que son utilizadas por las entidades públicas con una norma internacional, por lo que surge la necesidad realizar una comparación para dimensionar si los procesos que utiliza la contraloría general del estado bajo la norma 410 están en concordancia con una norma internacional. Al realizar una indagación no se obtuvo bajo que referencias de normas nacionales o internacionales para el control interno de información se realizó la norma 410.

Mientras las Normas internacionales como los Objetos De Control Para Información Y Tecnología Relacionadas que se encuentran en Cobit 5 esta norma está encaminada para la gestión de las tecnologías de información (TI) que busca la implementación de un gobierno de TI que mecanice los procesos de las áreas Estratégicas, entrega de valor, gestión de riesgos, gestión de recurso, comprobación de desempeño.

Existen otras normativas internacionales para la seguridad de la información como es la norma ISO 27001 "es un sistema basado en el ciclo de mejora continua de Deming dicho ciclo consiste en Planificar, Hacer, Verificar Actuar por lo que se conoce como ciclo PDCA". "La norma ISO 27001 se relaciona con la seguridad y Cobit 5 actúa como una especie de marco que ayuda a conectar a la norma ISO 27001 y otros marcos de gestión de TI" (ISO, 2019).

Para la comparación de las normativas utilizaremos Cobit 5 siendo la última edición del framework de un marco internacional que se publicó en el año 2012 se encuentra centrado en la tecnología de información que es el mecanismo principal para generar valor en las organizaciones, esta versión a nivel de la estructura de procesos y dominios fue agregada un nuevo dominio que esta orienta al gobierno de TI llamado "EMD- Evaluar, Dirigir, Monitorear" que remplaza el antiguo proceso ME4 DE Cobit 4.1. "Estos dominios son una evolución de la estructura de procesos y dominios de Cobit 4.1.

Los nombres de estos dominios en Cobit 5 han sido elegidos de acuerdo a estas designaciones de áreas principales, pero contienen más verbos para describirlos:

- Alinear, Planificar y Organizar (APO)
- Construir, Adquirir e Implementar (BAI)
- Entregar, dar Servicio y Soporte (DSS)
- Supervisar, Evaluar y Valorar (Monitor, Evaluate and Assess - MEA)

Mientras que en Cobit 4.1 denominado marco de referencia cuenta con los siguientes dominios:

- Planear y Organizar (PO)
- Monitorear y Evaluar (ME)
- Adquirir e Implementar (AI)
- Entregar y dar soporte (DS)”(Gallego Juan, 2020)

Cobit 5 nos brinda una guía de prácticas detalladas para precisar, manipular, monitorear un método de gestión de seguridad y protección de la información para todos los niveles en las organizaciones constando de 37 procesos que describen actividades para la implementación del control interno de información ya que versión anterior constaba solo de 34 procesos. La seguridad de la información y los datos son indispensables hoy en día en cualquier empresa, por lo tanto Cobit 5 beneficia a las organizaciones a disminuir los perfiles de riesgos por medio de la administración apropiada de la seguridad, plantea una idea que “la seguridad de la información es una disciplina transversal, por lo que se consideran distintos aspectos de protección de datos en todas las actividades y procesos llevados a cabo por la empresa”.(Miguel Angel Mendoza, 2015)

1.3 Objetivos

1.3.1 Objetivo General

Realizar un análisis comparativo de las normas 410 de control interno de información de la Contraloría General Del Estado con Cobit 5

1.3.2 Objetivos Específicos

- Llevar a cabo una revisión de los trabajos más relevantes, relacionados con la norma Cobit y la 410 de la Contraloría General del Estado.
- Analizar las normativas de Cobit 5 relacionado con la seguridad de la información y la normativa 410 que posee la Contraloría General Del Estado.
- Realizar una comparación de las normativas analizadas, y representar gráficamente los resultados.

1.4 Contribuciones

Con este proyecto de investigación identificaremos si la norma 410 cumple con normas internacionales o está bajo la normativa de Cobit 5.

Identificar si los dominios o procesos se encuentran dentro de las normas 410 verificando si están alineados con los estándares internacionales, que permitirá mejorar, organizar, implementar seguridades de información para la institución que utiliza las normas 410.

Examinar los procesos de Cobit 5 que se encuentren relacionados con el control interno de información.

Se utilizará Cobit 5 para la comparación por que se encuentra relacionado con los procesos de TI, objetivos de negocio que determina una relación con los recursos de TI: datos, sistemas de aplicaciones, tecnología.

Obtener definiciones de procesos para diseñar una comparación de cada normativa donde se detalle estadísticamente la similitud que tiene cada proceso en el control interno de información.

Aportar información para que a futuro con la contraloría general del estado pueda complementar la norma 410 establecer en la actualidad bajo la norma Cobit 5 que es una norma internacional.

1.5 Estado del Arte

A través de los años la práctica ha justificado que una buena gestión de la información no solo puede optimizar elocuentemente el desempeño de una organización, sino que también puede convertir radicalmente los procesos de una organización. La seguridad de la información ha sido un tema muy relevante para las comunidades académicas y para las organizaciones empresariales que tienen como propósito ser más eficientes en la administración del capital intelectual realizando implementaciones de nuevos modelos, estrategias para el perfeccionamiento de la gestión de la información. para la prevención de riesgos Kevin Mitnick (2002) hizo la siguiente afirmación "Nunca se confíe de los mecanismos de seguridad en la red para proteger su información. Revise su punto más vulnerable. En la mayoría de los casos descubrirá que este se encuentra en las personas"(Johanna Cárdenas Solano, Eduardo Becerra Ardila, & Ernesto Martinez Ardila, 2013)

Según (Katiuska Espinoza, 2017), En su trabajo plantea un diagnóstico de cumplimiento de las normativas 410 de la contraloría general del estado en la empresa pública de hidrocarburos EP Petroecuador que da a conocer "contribuir a la mejora de la gestión del área de tecnología de una empresa pública generando propuestas para trabajar con procesos que coadyuven al cumplimiento de la normativa gubernamental" en la cual está basada con conceptos de auditorías en el área de tecnología y mejores prácticas para la gestión de áreas de TI como Cobit 5, teniendo como bases el desarrollo de modelos de cumplimiento de las normativas del sector financiero Publico en la gestión de servicios de TI, realiza un caso de estudio para evaluar el grado de cumplimiento de la norma 410 en la empresa EP Petroecuador. Se tiene como resultado que la mayoría de las normas de control interno están basadas en marcos de trabajo de buenas prácticas como Cobit 5.

Por otro lado (Gomez, 2016) En su trabajo de ensayo "la aplicación de cobit en las organizaciones" da a conocer que "busca dar una mirada al modelo Cobit como herramienta clave en las organizaciones para apoyar la aplicación y ejecución de todos sus procesos" las revisiones realizadas del modelo con sus respectivas ventajas, desventajas y ejemplos determinan la toma de decisiones por parte del alta gerencia, teniendo como beneficios que Cobit es un modelo de mejores prácticas que lo convierte en una elección aprobada como un estándar adaptable para compañías de cualquier país de tipo público y privado.

A demás (Rosa Andrea Rea Lozada, 2012) En su trabajo desarrollado "Normas de control interno emitidas por la contraloría general del estado, aplicadas a la dirección de tecnologías de información del Ilustre municipio de Ibarra" da a conocer el "desarrollo para organizar a la dirección de tecnologías de la información y comunicación en procesos solicitados por la Contraloría General del Estado" en la cual describe normas

internacionales que están relacionados con la tecnología de información, presenta metodologías de trabajo aplicada a fases organizativas de diagnósticos y levantamiento de procesos, propuestas de control interno con procesos levantados y creados para la dirección de TIC. En el proyecto se determina que la dirección de tecnologías de información y comunicación consta con una herramienta para el control y la ejecución de actividades que se transforman en fortalezas.

En este apartado se puede determinar la importancia de conocer las normativas de la seguridad de la información siendo una obligación legal para todas las empresas que tiene como objetivo garantizar la disponibilidad, integridad y confidencialidad utilizando como una herramienta que nos va a permitir conocer, gestionar y minimizar posibles riesgos que atenten contra la seguridad de la información en la empresa implementando las normativas de cobit 5 y del control interno 410 de la Contraloría General del Estado, hay que tener en cuenta la diferencia entre seguridad informática y seguridad de la información. La seguridad informática se refiere a la protección de las infraestructuras de las tecnologías de la información y comunicación, mientras que la seguridad de la información se refiere a la protección de los activos de información fundamentales para el éxito de cualquier organización como ejemplos de información que se puede encontrar en una empresa están los correos electrónicos, páginas web, imágenes, bases de datos, documentos, etcétera. Los trabajos dados a conocer anteriormente se encuentran alineados con el tema de desarrollo que se realizara en el presente trabajo.

CAPÍTULO 2.

2. Marco Teórico

2.1 Sistema De Gestión De Seguridad De La Información

Las siglas SGSI son empleadas para describir a un Sistema de Gestión de la Seguridad de la Información, son un conjunto de políticas de administración, mantenimiento de un conjunto de procesos para proporcionar eficientemente la accesibilidad de la información, que busca testificar la confidencialidad, integridad y disponibilidad de los activos de información disminuyendo a la vez los riesgos de seguridad de la información.

> "La información junto con los procesos y sistemas que hacen uso de ella, son activos muy importantes de una organización; La confidencialidad, integridad y disponibilidad de información puede llegar a ser muy importante para conservar los niveles de competitividad, rentabilidad, conformidad legal e imagen empresarial para conseguir los objetivos de la organización y garantizar los beneficios económicos". (SGSI, 2019)

Un SGSI ayuda a constituir reglamentos e instrucciones en correspondencia a los objetivos de negocio de la organización, con el propósito de conservar un grado de exhibición siempre menor al grado de riesgo que la propia organización ha determinado asumir.

"Con un SGSI la organización conoce los riesgos a los que está sometida su información y los asume, minimiza, transfiere o controla mediante una sistemática definida, documentada y conocida por todos, que revisa y mejora constantemente."

Según ISO 270007 "consiste en la preservación de confidencialidad, integridad y disponibilidad, así como los sistemas implicados en su tratamiento dentro de una organización. Estos tres términos constituyen la base sobre la que se cimienta todo el edificio de la seguridad de la información.

Confidencialidad: la información no debe ser puesta a disposición o revelar a individuos, entidades o procesos no autorizados.

Integridad: salvaguardar el mantenimiento de la exactitud y completitud de la información y sus métodos de proceso.

Disponibilidad: acceso y utilización de la información y los sistemas de tratamiento de la misma por parte de los individuos, entidades o procesos autorizados cuando lo requieran." (SGSI, 2019)

El Sistema de Gestión de Seguridad de la Información busca reconocer que los riesgos de la seguridad de la información sean distinguidos, asumidos, tramitados y minimizados.

"La implantación de un Sistema de Gestión de Seguridad de la Información implica las siguientes tareas:

- Compromiso de la dirección general de la organización.
- Elaboración de un plan de Gestión de Seguridad.
- Asignación de recursos, funciones y responsabilidades.
- Formación y concienciación del personal.
- Establecer controles periódicos y mejoras.

El plan de Gestión de seguridad consiste en:

- Identificar los activos del SFSI y sus propietarios
- Identificar las amenazas de cada activo
- Identificar las vulnerabilidades del sistema
- Identificar los posibles impactos de las vulnerabilidades
- Gestionar el riesgo:
  - Evitarlo: suprimir las causas del riesgo (activo, amenaza, vulnerabilidad)
  - Transferirlo: Outsourcing (subcontratación), seguro
  - Reducirlo: la amenaza, vulnerabilidad o impacto

- Aceptarlo”(Lisot, 2018)

Un Sistema de Gestión de Seguridad de la Información se constituye con otros sistemas de gestión es decir una herramienta que ubica la gerencia para administrar y examinar un especifico ámbito en este caso la seguridad de la información.

“La gestión de las actividades de las organizaciones se realiza con más frecuencia, según los sistemas de gestión basados en estándares internacionales como son:

- ISO 9001 impacto con el medio ambiente
- ISO 14001 prevención de riesgos laborales
- ISO 27001gestion de seguridad de la información”.(SGSI, 2019)

Para organizar y determinar un sistema de gestión de la seguridad de la información se manipula el ciclo de mejora continua conocido como “Circulo de Deming” basada en un concepto ideado por Walter A. Shewhart denominada PDCA, es una sistemática que ha manifestado su aplicabilidad y ha concedido construir la mejora continua en organizaciones de todas las clases.

El modelo PDCA su significado en inglés “**Plan, DO, Check, Act** (Planificar – Hacer – Verificar - Actuar)” tiene una cadena de etapas y operaciones que permite crear un modelo de indicadores y métricas semejantes en el tiempo, de modo que se pueda considerar el progreso en la mejora de la organización.

“Planificar

- Establecer el SGSI
- Planificar y diseñar la presentación normalizando las políticas a emplear en la organización, cuáles son las conclusiones a alcanzar y en que ayudaran a alcanzar los objetivos de negocio.
- Manipulación de los medios para los procesos y los activos que los soportan, verificación del enfoque de análisis de riesgos y los criterios que se alcanzarán para

gestionar las contingencias de modo vinculado con las políticas y objetivos de seguridad.

Hacer

- Implementación y funcionamiento del SGSI
- Las Políticas y controles seleccionados para cumplirlas se implementan mediante recursos técnicos, procedimientos o ambas cosas a la vez, se establecen responsables a cada tarea para comenzar a ejecutarlas según las instrucciones.

Verificar

- Monitorización y revisión del SGSI
- Control de los procesos que se ejecutan como se ha establecido de manera eficaz y eficiente alcanzando los objetivos definidos para ellos.
- Verificar el grado de cumplimiento de las políticas y procedimientos, identificando los fallos que pudieran existir y hasta donde sea posible su origen mediante revisiones y auditorias.

Actuar

- Mantenimiento y mejora del SGSI, decidiendo y efectuando las acciones preventivas y correctivas necesarias para rectificar los fallos detectados en las auditorías internas y revisiones del SGSI o cualquier otra o información relevante para permitir la mejora permanente del SGSI”

“Con un SGSI la organización conoce los riesgos a los que está vinculada su información y los asume, minimiza, transfiere o controla mediante una sistemática definida, documentada y conocida por todos, que revisa y mejora constantemente.” (Calidad & Gestión, 2014)

2.2 Normativas Internacionales

Se crearon normas internacionales que permiten resguardar temas como la confidencialidad, integridad y disponibilidad definiendo patrones y guías relacionados con el sistema de gestión y adaptables a cualquier tipo de organización internacional y mundial abordando la seguridad de la información con la intención de suministrar el comercio, el intercambio de información y favorecer a la transferencia de tecnologías.

Entre las normas internacionales se encuentran las siguientes referencias que permiten calcular con mayor o menor grado de problema de los procesos:

COBIT

Es una colección de herramientas alineadas a asegurar el control y el alcance de la gobernabilidad de sistemas de información a largo plazo a través de auditorías, en marca todos los procesos de información de la empresa. Compila y organiza desde la instauración de la información hasta su disposición final para certificar una intervención de calidad precisa.

COSO

“Está orientado al control de la administración financiera y contable de las organizaciones, dada a la gran cercanía que existe entre esta área y los sistemas de información computarizados, es que resulta importante entender el alcance y uso de esta norma.”

ITIL

Correspondientes a las siglas en inglés Information Tecnology Library (biblioteca de infraestructura de tecnología de la información) es una congregación de mejores prácticas para la administración efectiva de los sistemas de información. “Busca alinear los objetivos de

seguridad de TI con los objetivos de seguridad del negocio, asegurando la disponibilidad, confidencialidad, integridad, autenticidad y fiabilidad de la información"

LEY SOX (ley Sarbanes-Olex de EE. UU)

"Obliga a las empresas públicas nacionales o extranjeras inscritas en la Securities and Exchange Comission (comisión de valores e intercambio) a llevar un control y almacenamiento informático escrito de su actividad"

ISO 17.799

"Es un esquema para la administración de la seguridad de la información, involucra la implementación de toda una distribución fundamentada que debe contar con un fuerte soporte de la alta dirección de cualquier organización"

La seguridad de la información según ISO 27001 se basa en la protección de su confidencialidad, integridad y disponibilidad. Dentro de este conjunto están:

- "**ISO/IEC 27000:** vocabulario estándar para el SGSI para todas las normas de la familia
- **ISO/IEC 27001:** especifica los requisitos para la implantación del SGSI. Adopta un enfoque de gestión de riesgos y promueve la mejora continua de los procesos
- **ISO/IEC 27002:** Es un código de buenas prácticas para la gestión de seguridad de la información
- **ISO/IEC 27003:** Directrices para la implementación de un SGSI es el soporte de la norma ISO/IEC27001.
- **ISO/IEC 27004**: Métricas para la gestión de seguridad de información. Es la que proporciona recomendaciones de quien, cuando y como realizar mediciones de seguridad de la información.
- **ISO/IEC 27005**: Normativa dedicada exclusivamente a la gestión de riego en seguridad de la información. Proporciona recomendaciones y lineamientos de métodos y técnicas de evaluación de riesgos de seguridad en la información

- **ISO/IEC 27006**: esta norma específica los requisitos para la certificación de SGSI." (Olivares Rojas, 2009)

ISO/IEC 31000

Esta normativa proporciona pautas genéricas sobre el manejo de riesgos y se puede aplicar a cualquier sector en su totalidad o en un área, proyecto o actividad. Se aplica al nivel de madurez de la organización con el fin de desenvolver, utilizar y optimizar continuamente sus procesos.

OCTAVE

Es una técnica de seguridad y se basa en el riesgo, permite hacer análisis de riesgo informático desde el riesgo organizacional. Establece de tres métodos de implementación basándose en criterios con orientación en la práctica y valoración basada en la información de riesgo. (García, 2015)

"OSSTMM (Manual de Metodología de Prueba de Seguridad de Código Abierto)

Proporciona una metodología para una prueba de seguridad a fondo, conocida también como auditoria OSSTMM La cual provee de una medición precisa de la seguridad a nivel operacional, permite realizar pruebas más precisas, concretas y eficientes."(Leonel & Cuzme, 2017)

2.3 Introducción Cobit

Las siglas de Cobit significan Objetivo de Control para Tecnología de Información y Tecnologías Relacionada. Es una guía de mejores prácticas destacado como una herramienta de soporte creado para ayudar a la alta gerencia a garantizar el beneficio de los objetivos de la empresa mediante el control adecuado de las TI, la distribución de procesos y su orientación de alto nivel brinda una visión completa de TI y de las decisiones a tomar de la misma, se aplica a los sistemas de información de toda organización incluyendo computadoras personales y las de red, permitiendo el desarrollo de políticas para el control de TI a través de las empresas (Institute, 2007)en el cual está apoyado en una filosofía que los recursos de TI requieren para

ser dirigidos por procesos colectivos y abastecer información oportuna y confiable que la empresa requiere para obtener sus objetivos establecidos.

Es un marco de referencia que tiene determinado 37 procesos de control de alto nivel que se encuentran agrupados en cuatro dominios para cada proceso de TI los cuales son: "Planear y Organizar, Adquisición e Implementación, Entrega de servicios y Monitoreo". (Sánchez, 2007)

Posee un modelo de madurez de control de procesos de TI con metodologías para calificar cada proceso centralmente de una organización, el modelo de madures es asignado a los 37 procesos de Cobit que especifica los elementos críticos de éxito, indicadores de desempeño y los indicadores de resultados de cada proceso. Tiene los siguientes componentes importantes:

Misión

"investigar, desarrollar, publicar y promover un conjunto de objetivos de control para la tecnología de información, que sea internacional y este actualizado para uso cotidiano de gerentes, auditores y usuarios."

Visión

"Ser un modelo de control para la tecnología de información"(Cobit, 2016)

"Cobit 5 es denominado como el modelo de referencia de procesos que se encuentran divididos en procesos de gobierno y de administración de la TI:

- **Gobierno** está estructurado de cinco procesos de gobierno, dentro de cada proceso se definen prácticas de evaluación.
- **Administración**: está estructurado de cuatro dominios en constancia con las áreas de responsabilidad que son: planificar, construir, ejecutar, orientación y supervisión que proporciona una cobertura de extremo a extremo de las TI." (Gallego Juan, 2020)

Cobit permite el desarrollo de buenas prácticas para control de TI a través de las políticas que posee las empresas, es el integrador de marco de referencia general para el gobierno de TI que ayuda a percibir y gestionar los riesgos y beneficios asociados con TI manteniendo la

disposición de la información para soportar decisiones de negocio logrando una excelencia operativa aplicando específicamente la tecnología, manteniendo los riesgos de TI a un nivel aceptable. Fue creado en 1996 como una herramienta de gobierno de TI relacionando con la tecnología informática permitiendo que la información y la tecnología sean gobernadas y gestionadas de manera completa para toda empresa teniendo en consideración los intereses de las partes interesadas internas y externas, puede ser manejado en la organización por los responsables de un proceso de negocio y responsables en el campo de tecnología con el compromiso de inspeccionar los aspectos de información del proceso de la empresa. (ClubEnsayos, 2012)

El gobierno de TI está orientado a proporcionar las estructuras que unen procesos con estrategias y objetivos de la empresa institucionalizando con las mejores prácticas de planificación y organización dando un alcance a los beneficios de TI para asegurarse tanto de la información de la empresa como de las tecnologías puedan ser sobrellevadas por los objetivos de la empresa consiguiendo maximizar sus beneficios alcanzando una ventaja competitiva de su información.

Cobit ha desarrollado nuevas ediciones; "la primera edición fue publicada en 1996, la segunda edición en 1998, la tercera edición en 2000 (la edición online estuvo disponible en 2003), la cuarta edición en Diciembre del 2005 la versión 4.1 está disponible desde Mayo de 2007 la versión Cobit 5 ya está disponible."(Cobit, 2014)

Los beneficios de Cobit 5 ayuda a las organizaciones de todos los tamaños a:

- "Optimizar los servicios el coste de las TI y la tecnología
- Apoyar el cumplimiento de las leyes, reglamentos, acuerdos contractuales y las políticas
- Gestión de nuevas tecnologías de información"

- “Incremento de la creación de valor a través de un gobierno y gestión efectiva de la información y de los activos.
- Incremento de la satisfacción del usuario con el compromiso de TI y sus servicios prestados
- Incremento del nivel de cumplimiento con las leyes regulaciones y políticas relevantes.”

Para que estos beneficios se logren se necesita de un buen gobierno y una buena administración de los activos de TI y de la información.

Cobit 5 es producto del progreso estratégico de ISACA impulsado a la próxima generación de enseñanzas sobre el gobierno y la administración de la información y los activos tecnológicos de las organizaciones. ISACA “desarrollo Cobit 5 para resguardar las necesidades de los interesados, que se alinean a las actuales directrices sobre técnicas de gobierno y administración relacionada con la TI”. (Evolucion c, 2015)

2.3.1 Principios de Cobit

Cobit 5 proporciona la guía de ISACA, se fundamenta en cinco principios clave para el gobierno y la gestión de las TI empresariales. En la imagen 1 se describe los cinco principios

Imagen 1 Principios cobit
Fuente (ISACA)

1. **“Satisfacer las Necesidades de las Partes Interesadas.** Las empresas existen para crear valor para sus partes interesadas manteniendo el equilibrio entre la realización de beneficios y la optimización de los riesgos y el uso de recursos.
2. **Cubrir la empresa de extremo a extremo.** Integra el gobierno y la gestión de TI en el gobierno corporativo, cubriendo todas las funciones y procesos dentro de la empresa.
3. **Aplicar un marco de referencia único e integrado.** Se alinea a alto nivel con otros estándares y marcos de trabajo relevantes, y de este modo puede hacer la función de marco de trabajo principal para el gobierno y la gestión de las TI.
4. **Hacer posible un enfoque holístico.** Un gobierno y gestión de las TI de la empresa efectivo y eficiente requiere de un enfoque holístico que tenga en cuenta varios componentes iterativos, define un conjunto de catalizadores para apoyar la implementación de un sistema de gobierno y gestión global.
5. **Separar el gobierno de la gestión.** Establece una clara distinción entre gobierno y gestión. Estas dos disciplinas engloban diferentes tipos de actividades, requieren diferentes estructuras organizativas y sirven a diferentes propósitos. ”(ISACA principios, 2012)

2.3.2 Evolución de Cobit

En la siguiente imagen se muestra la evolución que ha venido desarrollando Cobit

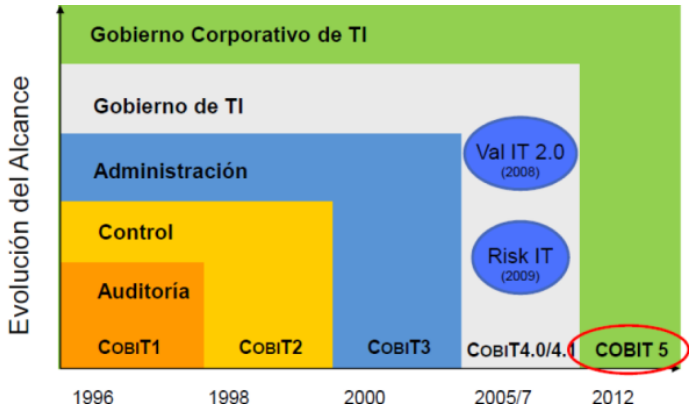


Imagen 2 Evolución de Cobit

Fuente (ISACA)

“Cobit 1

- Objetivos de control
- Guías o directrices de Auditoria

Cobit 2

- Guías de autoevaluación
- Actualización de la versión automatizada
- Referencias y material de apoyo adicional

Cobit 3

- Incorporación de las guías de controles
- Mejoras en los objetivos de control
- Identificación de indicadores de desempeño

Cobit 4.1: tiene 34 procesos que cubren 210 objetivos de control clasificados en cuatro dominios:

- Planificación y Organización (PO)
- Adquisición e Implementación (AI)
- Entrega y Soporte (DS)
- Supervisión y Evaluación (ME)

Cobit 5 proporciona una visión empresarial del gobierno de TI que tiene a la tecnología y a la información como protagonistas. Se basa en Cobit 4.1 y se amplía mediante la integración de otros importantes marcos y normas como ISO, ITIL, Val IT.”(Evolución c, 2015)

2.3.3 Cuadro de mando integral de ti (CMI IT)

"El cuadro de mando integral de TI fue detallado originalmente por Van Grembergen y Van Brugger en 1997 y Van Grembergen y Timmerman 1998. Las aplicaciones efectuadas por estos autores, formaron un cuadro de mando genérico para las TI conocido como IT BSC (IT balanced Scorecard)."

El cuadro de mando par las TI está conformado por cuatro aspectos clásicos del BSC, ya que las TI forman parte de las organizaciones y participan contribuyendo valor a la organización.

En la siguiente tabla1 se describen las cuatro perspectivas estándar del BSC TI con sus misiones y estrategias.

Orientación al usuario Representa la evaluación de las TI desde la perspectiva de usuario tanto interno como externo	
Misión	Ser los suministradores de TI preferidos.
Estrategia	Suministradores preferidos de aplicaciones o sugeridor de la mejor solución
Excelencia Operacional Representa los procesos empleados en la estrategia, diseño, transición, operación y mejora continua de los servicios y aplicaciones de TI	
Misión	Ofrecer servicios y aplicaciones TI efectivas y eficaces
Estrategia	Desarrollo y Operaciones eficientes y eficaces.
Contribución al Negocio Demuestra el valor creado desde TI para el negocio	
Misión	Obtener de la organización una inmersión razonable en TI.
Estrategia	Control de gastos en TI, valor para la organización de los procesos de TI, proveer nuevas capacidades de negocio.
Orientación futura Representa los recursos tecnológicos y humanos precisos para otorgar los servicios y aplicaciones de TI.	
Misión	Desarrollar oportunidades para contestar a desafíos futuros
Estrategia	Entretenimiento y formación del equipo TI, experiencia del equipo TI, investigación en tecnologías emergentes. Antigüedad de las aplicaciones en uso.

Tabla 1: Cuadro de Mando Integral de TI
Fuente (Ignacio G. Roberto Monfort, Albert Martinez, pag14)
Elaborado por: Rosalía Contreras

2.3.4 Métricas de Metas de TI

"Las meticas de muestra que pueden ser utilizadas para medir el logro de cada meta. Estas métricas son muestras y cada empresa debería revisar cuidadosamente la lista, decidir cuáles son métricas pertinentes y alcanzables para su propio entorno, y diseñar su propio sistema de cuadro de mando". En la tabla 2 se da a conocer detalladamente las métricas que debe cumplir cada objetivo de las TI.

Dimensión CMI	Objetivos de las TI	Métricas
Interno	Agilidad de las TI	• Nivel de satisfacción de la alta dirección del negocio con la capacidad de respuesta de TI a nuevos requerimientos • Número de procesos de negocio críticos soportados por infraestructura y aplicaciones actualizadas • Tiempo medio de conversión de objetivos TI estratégicos en una iniciativa acordada y aprobada.
	Seguridad de la información, infraestructuras de procesamiento y aplicaciones	• Número de incidentes de seguridad causantes de pérdidas financieras, interrupción del negocio o vergüenza pública • Número de servicios TI sin requerimientos de seguridad destacables. • Tiempo de concesión, cambio y eliminación de privilegios de acceso comparado con los niveles de servicio acordados. • Frecuencia de las evaluaciones de seguridad en relación a los últimos estándares y guías.
	Optimización de activos, recursos y capacidades de las TI	• Frecuencia de evaluaciones de la madurez de la capacidad y de la optimización de costes • Tendencia de los resultados de las evaluaciones • Niveles de satisfacción de la alta dirección del negocio y de TI con los costes y capacidades TI.

	Disponibilidad de información útil y relevante para la toma de decisiones	• Nivel de satisfacción del usuario del negocio con la calidad y la puntualidad (o disponibilidad) de la • información de gestión • Número de incidentes de procesos de negocio causados por la indisponibilidad de la información • Relación y alcance de decisiones de negocio erróneas donde la información errónea o no disponible fue un factor clave.
	Cumplimiento de las políticas internas por parte de las TI	• Número de incidentes relacionados con el incumplimiento de políticas • Porcentaje de interesados que entienden las políticas • Porcentaje de políticas apoyadas por estándares y prácticas de trabajo efectivas • Frecuencia de revisión y actualización de políticas

Tabla 2: Métricas de Metas de TI
Fuente (ISACA, pag17)
Elaborado por: Rosalía Contreras

2.3.5 Procesos de Gobierno de TI.

La gobernanza esta encargada de evaluar las insuficiencias, circunstancias y expectativas de las partes interesadas para establecer que se alcanzan las metas establecidas y equilibradas; estableciendo la dirección a través de la priorización y la toma de decisiones; y estimando el beneficio y el desempeño relacionado a la dirección y fines acordados.

- "Asegurar el cumplimiento de los objetivos de la empresa
- Evaluar las necesidades, condiciones y opciones de las partes interesadas.
- Supervisar el desempeño y cumplimiento de la dirección y los objetivos acordados."

En la tabla 3 se da a conocer los procesos de gobernanza especificados por Cobit 5 los cuales son los siguientes:

EMD: EVALUAR, ORIENTAR Y SUPERVISAR
EMD01 Asegurar El Establecimiento Y Mantenimiento Del Marco De Gobierno
EMD02 Asegurar La Entrega De Beneficios

EMD03 Asegurar La Optimización Del Riesgo
EMD04 Asegurar La Optimización De Los Recursos
EMD05 Asegurar La Transparencia Hacia Las Partes Interesadas

Tabla 3: Procesos de gobernanza de TI
Fuente (ISACA)
Elaborado por: Rosalía Contreras

2.3.6 Procesos de gestión de TI

Es un método fundamentada en procesos, orientada en organizar los servicios de TI proporcionado con las necesidades de las empresas.

La gestión de TI proyecta, construye, ejecuta y controla actividades distribuidas con la orientación constituida por la gobernanza, para alcanzar las metas empresariales. (ISACA, 2012). En la tabla 4 muestra el conjunto de procesos que están alineados a la gestión de TI.

ALINEAR, PLANIFICAR Y ORGANIZAR
APO01 Gestionar El Marco De TI
APO02 Gestionar La Estrategia
APO03 Gestionar La Arquitectura Empresarial
APO04 Gestionar la Innovación
APO05 Gestionar El Portafolio
APO06 Gestionar El Presupuesto Y De Los Costes
APO07 Gestionar Los Recursos Humanos
APO08 Gestionar Las Relaciones
APO09 Gestionar Los Acuerdos De Servicio
APO10 Gestionar Los Proveedores
APO11 Gestionar La Calidad
APO12 Gestionar El Riesgo
APO13 Gestionar La Seguridad
CONSTRUIR, ADQUIRIR E IMPLEMENTAR
BAI01 Gestionar Los Programas Y Proyectos
BAI02 Gestionar La Definición De Requisitos
BAI03 Gestionar La Identificación Y La Construcción De Soluciones
BAI04 Gestionar La Disponibilidad Y La Capacidad
BAI05 Gestionar La Introducción De Cambios Organizativos
BAI06 Gestionar Los Cambios
BAI07 Gestionar La Aceptación Del Cambio Y La Transición
BAI08 Gestionar El Conocimiento
BAI09 Gestionar Los Activos
BAI10 Gestionar La Configuración
ENTREGAR, DAR SERVICIO Y SOPORTE
DSS01 Gestionar Las Operaciones

DSS02 Gestionar Las Peticiones Y Los Incidentes Del Servicio
BAI03 Gestionar Los Problemas
DSS4 Gestionar La Continuidad
DSS05 Gestionar Los Servicios De Seguridad
DSS06 Gestionar Los Cambios De Los Procesos Del Negocio
SUPERVISAR, EVALUAR Y VALORAR
MEA01 Supervisar, Evaluar Y Valorar Rendimiento Y Conformidad
MEA02 Supervisar, Evaluar Y Valorar El Sistema De Control Interno
MEA03 Supervisar, Evaluar Y Valorar La Conformidad Con Los Requerimientos Externos

Tabla 4: Procesos de Gestión de TI
Fuente (ISACA)
Elaborado por: Rosalía Contreras

Al ser un marco de referencia no involucra que se deba tener todos los procesos especificados en Cobit 5, los pocos o muchos procesos que se puntualice en una empresa debe efectuar con los objetivos implantados que cubran las metas definidas en el marco de referencia.

En la imagen 1 se muestra en contexto la estructura del marco de referencia de los procesos de Cobit 5, en base al cual se propondrá el modelo para realizar el análisis de comparación con las normas que utiliza la contraloría general del estado del control interno 410.

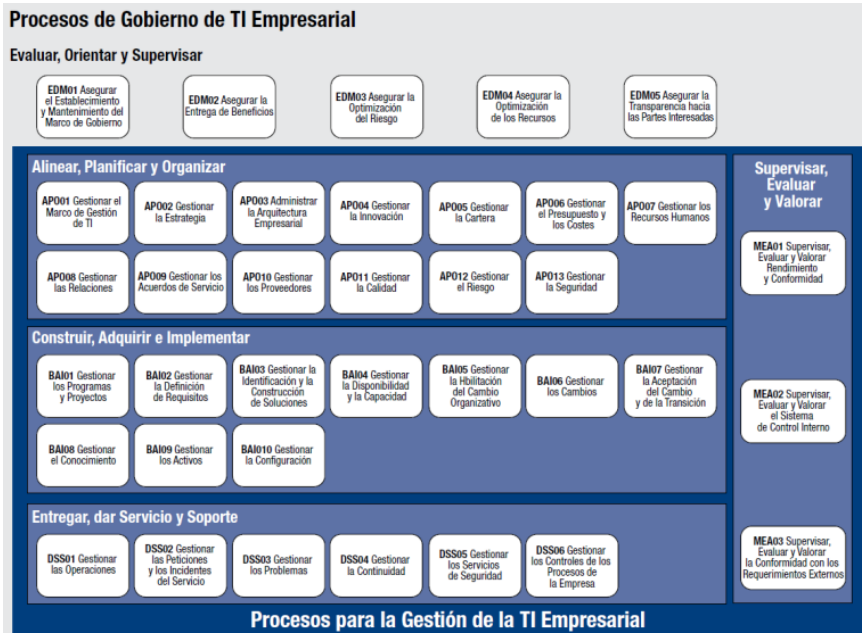


Imagen 3 Procesos de gestión de TI
Fuente (ISACA)

2.3.7 Objetivos de control para la protección de la información

Un marco de referencia puede ser manipulado por las organizaciones como una enseñanza para la composición de las operaciones concernientes con el área de información con un conjunto de propósitos definidos y revisiones de TI que tiene como objetivo principal la implementación de un marco para la gestión y el gobierno de TI.

Cobit 5 se enfoca completamente en la seguridad de la información teniendo como base el framework de las mejores prácticas para salvaguardar la información en todos los niveles en las organizaciones, el documento de Cobit 5 "plantea que la seguridad de la información es una disciplina transversal ya que protege distintos aspectos de datos de las actividades y procesos que se realizan en una organización", Cobit 5 ofrece una enseñanza básica para definir, operar y monitorear un sistema de gestión de seguridad.

Se pretende organizar la seguridad de la información con los objetivos de la empresa, a través de las destrezas de gobierno y gestión que se encuentran orientadas a la seguridad. En la tabla 5 se muestra los procesos para la gestión de la información.

PROCESOS PARA LA GESTIÓN DE LA INFORMACIÓN
APO13: GESTIÓN DE LA SEGURIDAD
DESCRIPCIÓN DEL PROCESO Definir, operar y supervisa un sistema para la gestión de la seguridad de la información.
PROPÓSITO Mantener el impacto y ocurrencia de los incidentes de la seguridad dentro de los niveles de apetito de riesgo de la empresa.
SUBPROCESOS
APO13.01 Establecer y mantener un SGSI **(**sistema de gestión de seguridad de la información)
APO13.02 Definir y gestionar un plan de tratamiento de riesgo de la seguridad de la información
APO13.03 Supervisar y revisar el SGSI
DSS04: GESTIÓN DE LA CONTINUIDAD

DESCRIPCIÓN DEL PROCESO Establecer y mantener un plan para permitir al negocio y a TI responder a incidentes e interrupciones de servicio para la operación continua de los procesos críticos para el negocio y los servicios TI requeridos y mantener la disponibilidad de la información a un nivel aceptable para la empresa
PROPÓSITO Continuar las operaciones críticas para el negocio y mantener la disponibilidad de la información a un nivel para la empresa ante el evento de interrupción significativa
SUBPROCESOS
DSS04.01 Definir la política de continuidad de negocio, objetivos y alcance
DSS04.02 Mantener una estrategia de continuidad
DSS04.03 Desarrollar e implementar una respuesta a la continuidad del negocio
DSS04.04 Ejercitar, probar y revisar el BCP (plan de continuidad de negocio)
DSS040.05 Revisar, mantener y mejorar el plan de continuidad
DSS04.06 Proporcionar formación en el plan de continuidad
DSS04.07 Gestionar acuerdos de respaldo
DSS04.08 Ejecutar revisiones post-reanudación
DSS05: GESTIÓN DE SERVICIOS DE SEGURIDAD.
DESCRIPCIÓN DEL PROCESO Proteger la información de la empresa para mantener aceptable el nivel de riesgo de seguridad de la información de acuerdo con la política de seguridad. Establecer y mantener los roles de seguridad y privilegios de acceso de la información y realizar la supervisión de seguridad.
PROPÓSITO Minimizar el impacto en el negocio de las vulnerabilidades e incidentes operativos de seguridad en la información
SUBPROCESOS
Dss05.01 Proteger contra software malicioso (malware)
Dss05.02 Gestionar la seguridad de la red y las conexiones
Dss05.03 Gestionar la seguridad de los puestos de usuario final
Dss05.04 Gestionar la identidad del usuario y el acceso lógico
Dss05.05 Gestionar el acceso físico a los activos de ti
Dss05.06 Gestionar documentos sensibles y dispositivos de salida
Dss05.07 Supervisar la infraestructura para detectar eventos relacionados con la seguridad

Tabla 5: Procesos de Gestión de información
Fuente (ISACA)
Elaborado por: Rosalía Contreras

En estos procesos se adicionan metas y métricas determinadas a la seguridad para cada proceso determinado en los dominios de Cobit 5, estableciendo prácticas, actividades, entradas y salidas entre procesos para cada una de los que conforman el modelo de referencia. (Miguel Angel Mendoza, 2015)

2.4 Contraloría general del estado

Es una asociación técnica superior de control, con autonomía administrativa, presupuestaria y financiera, dirigido y representado por el Control General del Estado.

> "De conformidad a lo dispuesto en el artículo 1 de la ley Orgánica de la Contraloría General del Estado, su objetivo es establecer y mantener, bajo la dirección de la Contraloría General del Estado, el sistema de control, fiscalización y auditoria del Estado, y regular su funcionamiento, con la finalidad de examinar, verificar y evaluar el cumplimiento de la visión, misión y objetivos de las instituciones del estado."

La estructura organizacional de la contraloría general del estado trabaja con el estatuto orgánico de la gestión organizacional por procesos el cual consta con los siguientes instrumentos:

Misión: "Controlar los recursos públicos para precautelar su uso efectivo, en beneficio de la sociedad."

Objetivos estratégicos:

- **"**Comunicar de manera efectiva los resultados institucionales
- Fortalecer la Gestión del Control Mejorar el potencial humano
- Optimizar la gestión interna"

Visión: "Ser reconocida como un referente de excelencia en el control de los recursos públicos"

Mapa de procesos: "Representa una visión general del sistema de gestión que incorpora los procesos institucionales y sus interrelaciones."

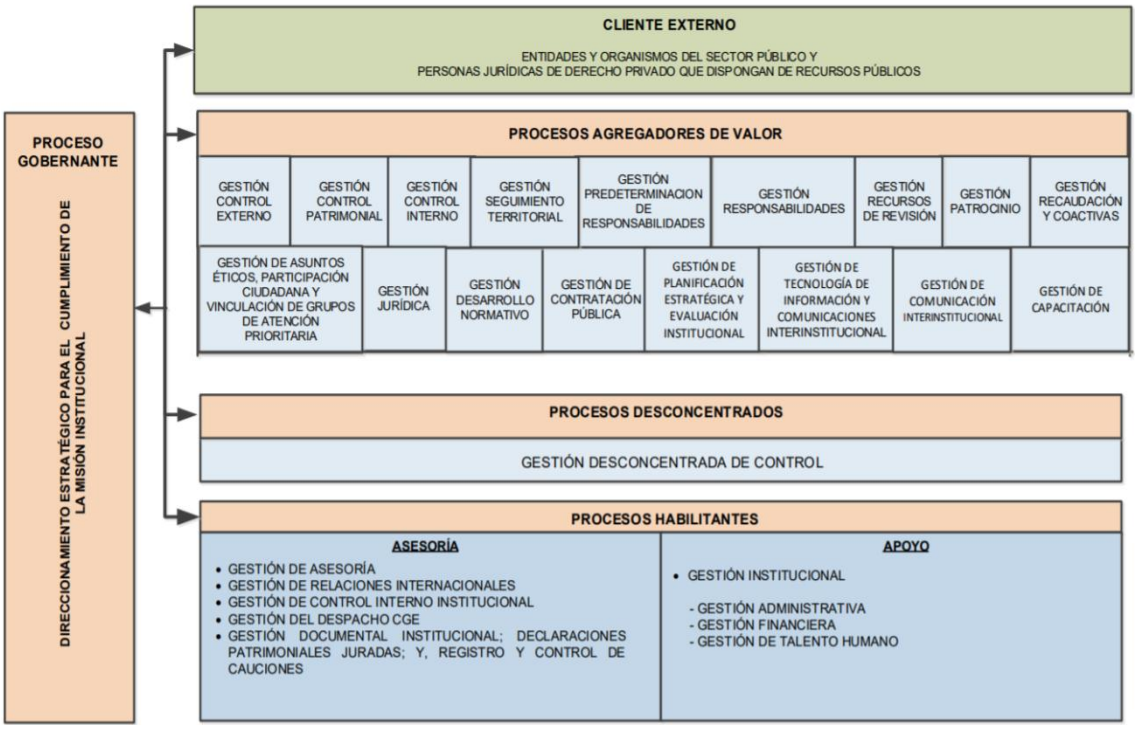


Imagen 4 Mapa de procesos de la Contraloría General Del Estado
Fuente (Contraloría general del Estado)

Las funciones que debe cumplir el establecimiento se encuentran puntualizadas en el apartado 212, del texto constitucional y son las siguientes:

1. "Dirigir el sistema de control administrativo, que se compone de auditoría interna, auditoría externa y del control interno de las entidades del sector público y de las entidades privadas que dispongan de recursos públicos.
2. Determinar responsabilidades administrativas y civiles culposas e indicios de responsabilidad penal, relacionadas con los aspectos sujetos a su control, sin perjuicio de las funciones que en esta materia sean propias de la Fiscalía General del Estado.
3. Expedir la normativa para el cumplimiento de sus funciones.
4. Asesorar a los órganos y entidades del Estado cuando se le solicite.(Contraloría General Del Estado, 2016)

2.4.1. Control interno

Se define control interno como cualquier dinamismo o labor desarrollada manual o automáticamente para notificar, restaurar errores o anormalidades, son administrados por el personal de cada entidad proporcionando seguridad para el alcance de los objetivos de la organización y el resguardo de los recursos. Los responsables del control interno de cada organización son las personas que tienen el propósito de establecer condiciones para el ejercicio del control realizan acciones y deben entender los requerimientos de diseños, implantación, operaciones y fortalecimiento de los aparatos del control interno de manera pertinente.

> Según COSO control interno es un modelo integrado a la gestión de organizaciones, ejecutado por el personal de las entidades de sus distintos niveles jerárquicos que suministran seguridad razonable en el uso de los recursos para corregir los objetivos de eficacia y eficiencia de las operaciones, confiabilidad de la información financiera, cumplimiento de leyes, reglamentos y normas que sean aplicables.(QAEC, 2019)

Las normas del control interno "constituyen un marco normativo que rige para las entidades y organismos del sector público y de los entes jurídicos de derecho privado que dispongan de recursos públicos; incluye componentes de una organización" (sistemas, procesos, recursos, cultura, metas y estructura) que ayudan al personal en el beneficio de los objetivos de la organización (Katiuska Espinoza, 2017) y la protección de los recursos, debe desempeñar con el ordenamiento jurídico, técnico y administrativo para originar eficiencia y eficacia de las operaciones de una organización y certificar la confiabilidad y oportunidad de la información, así como la implementación de reglamentos oportunos para restablecer las deficiencias de control, sus principales mecanismos está conformado por la valoración de riesgos, actividades de control, sistemas de información y comunicación.

Las normas de control interno son relacionadas con el marco legal vigente que se encuentran proyectadas bajo los elementos administrativos y normativas legales de técnicas pertinentes.

Las normas desarrolladas del control interno contienen normas generales y especificas relacionadas con “la administración financiera gubernamental, talento humano, tecnología de la información y administración de proyectos”. En el año 2002 la Contraloría General del Estado publicó las normas de control interno que constituyo con lineamiento para el cumplimiento de objetivos con la intención de garantizar la adecuada y eficiente administración de recursos y bienes de las entidades y organismos del sector público.(Contraloría General Del Estado, 2016)

El control interno está estructurado en cinco componentes funcionales:

- “Ambiente de control
- Evaluación de riesgos
- Actividades de control gerencial
- Información y comunicación
- Supervisión”(Contraloría General Del Estado, 2016)

La información es la materia prima de las organizaciones para poder desenvolverse y es necesario tenerla en cuenta para una buena toma de decisiones gerenciales.

> La información en relación con los sistemas y medios de información no son menos importantes como quiera que a través de ellos se soporta y es el insumo para planear y generar acciones de operación y como medio para tomar decisiones de tipo financiero, económico y de servicios(auditol, 2020)

El objetivo del control interno es “resguardar los recursos de la empresa o negocio evitando perdidas por fraude o negligencia, como también detectar las desviaciones que se presenten en la empresa y que puedan afectar al cumplimiento de los objetivos de la organización”.

Es por eso que el sistema de control es importante en una organización ya que es una labor necesaria para aquellos que anhelan conseguir competitividad en sus negocios ya que una

empresa que efectúa revisiones internas limita la ocurrencia de errores y fraudes en la información. Las entidades reguladoras lo catalogaran como una empresa que cumple las leyes y a su vez generan un impacto positivo en la organización. (Servin, 2018)

Para la implementación de un control interno se debe cumplir con tres fases:

Planificación:

“Alcanza acciones alineadas a la formulación de un diagnóstico de la situación en que se encuentra el sistema de control interno de la organización relacionado a las normas de control interno instituidas por la contraloría general de la republica que se utilizará de base para la preparación de un plan de trabajo que certifique la implementación y garantice la eficacia de su funcionamiento.

Ejecución:

Comprende el desarrollo de las acciones anunciadas en el plan de trabajo. Se da en dos niveles: nivel de entidad y nivel de procesos.

El primer nivel se construye políticas y normativas de control necesarias para la salvaguarda de los objetivos institucionales bajo el marco de las normas de control interno y componentes que estas establecen.

En el segundo nivel sobre la base de procesos críticos de la organización, previa identificación de los objetivos y de los riesgos que amenazan su cumplimiento, se procede a valorar los controles existentes a efectos de que estos aseguren la obtención de la respuesta a los riesgos que la administración ha optado.

Evaluación:

Comprende las acciones orientadas a lo largo de un conveniente proceso de implementación del sistema de control interno y de su eficaz funcionamiento a través de su mejora continua.”(Contraloría General Del Estado, 2016)

2.4.2 Objetivos de control interno

El control interno en las empresas u organizaciones para conseguir la misión institucional debe favorecer con el desempeño de los siguientes objetivos:

- "Promover la eficiencia, eficacia y economía de las operaciones bajo principios éticos y de transparencia.
- Garantizar la confiabilidad, integridad y oportunidad de la información
- Cumplir con las disposiciones legales y las normativas de la entidad para otorgar bienes y servicios de calidad
- Proteger y conservar el patrimonio político contra pérdida, despilfarro, uso indebido, irregularidad o acto ilegal." (Contraloría General Del Estado, 2016)

2.4.3. Normas de control interno de la contraloría general del estado

Las normas internas están orientadas a originar una apropiada administración financiera, tecnología de la información de los recursos públicos y comprobar el adecuado funcionamiento administrativo de las entidades y organismos del sector público, con el objetivo de establecer la efectividad, eficacia y economía en la gestión institucional con la finalidad de alcanzar sus objetivos.

"las normas de control interno son concordantes con el marco legal vigente y están diseñadas bajo principios administrativos, disposiciones legales y normativa técnica pertinente"

Es indispensable en toda organización ya que contribuye a notificar o restaurar errores realizados en los procesos de administración de información.

Para la realización de evaluación de proceso de control interno es preciso que las circunstancias a apreciar o inspeccionar sean cotejadas con algo que podría ser una norma, ley, reglamento estatuto, etc. Esto nos podrá dar la compostura para poder establecer el nivel de desempeño de las tareas establecidas a un sistema de información. ("Contraloría General Del Estado," 2016)

Estas normativas sirven como marco de referencia para todas las organizaciones a nivel público se encuentran categorizadas en cinco elementos que define una cadena de procedimientos que se debe de desempeñar para salvaguardarse los recursos de una organización. La representación general de las normas de control interno se muestra en la tabla 6:

CODIGO	NORMA
100	Normas generales
200	Ambiente del control
300	Evaluación de riesgos
400	Actividades del control
401	Generales
402	Administración financiera – presupuesto
403	Administración financiera – tesorería
404	Administración financiera – deuda publica
405	Administración financiera–contabilidad gubernamental
406	Administración financiera – administración de bienes
407	Administración del talento humano
408	Administración de proyectos
409	Gestión ambiental
410	Tecnología de la información
500	Información y comunicación
600	Seguimiento

Tabla 6: Normas de Control Interno
Fuente (contraloría general del estado)
Elaborado por: Rosalía Contreras

En el subgrupo 410 se dan a conocer las normas para la evaluación del control interno para la gestión de tecnología de información.

Dentro del grupo de las normativas del control interno 410 se describen 17 subgrupos de normas que cubren diferentes áreas de la gestión de tecnologías de la información que se muestra en la tabla 7.

CODIGO	NORMA
410-01	Organización informática
410-02	Segregación de funciones
410-03	Plan informático estratégico de tecnología
410-04	Políticas y procedimientos
410-05	Modelo de información organizacional
410-06	Administración de proyectos tecnológicos
410-07	Desarrollo y adquisición de software aplicativo
410-08	Adquisiciones de infraestructura tecnológica
410-09	Mantenimiento y control de la infraestructura tecnológica
410-10	Seguridad de la tecnología de información
410-11	Plan de contingencias
410-12	Administración de soporte de tecnología de información
410-13	Monitoreo y evaluación de los procesos y servicios
410-14	Sitio web, servicio de internet e intranet
410-15	Capacitación informática
410-16	Comité informático
410-17	Firmas electrónicas

Tabla 7: Normas de Tecnología de información
Fuente (Normas de Control interno pag.73)
Elaborado por: Rosalía Contreras.

"Estas normas son obligatorias para todas las entidades del sector público y las personas jurídicas de derecho privado que disponga de recursos públicos; estos controles tienen dos razones

- Desarrollar las actividades de manera organizada para obtener resultados esperados en los tiempos estimados con los costes planificados
- Cumplir con los procedimientos y regulaciones del estado para alcanzar los objetivos gubernamentales para el beneficio del país"

En la norma 410-10 **Seguridades De Tecnología De Información** "establece mecanismos que protejan y salvaguarden contra la perdida y fugas de los medios y la información que se procesa mediante sistemas informáticos." ("Contraloría General Del Estado," 2016)

Estas normas se pueden manipular operativamente el área de TICS y es inevitable complementarla con otros factores de gestión de TI.

2.5 Metodología

En el desarrollo de esta investigación se utilizará un enfoque cualitativo.

La investigación cualitativa implica el manejo y el almacenamiento de una gran variedad de materiales, entrevista, experiencia personal, historias de vida, observaciones, textos históricos, imágenes, sonidos que representan la rutina y las situaciones inciertas. Taylor Bogdan dice "que el investigador cualitativo pretende comprender lo que la gente dice". El objetivo de la investigación cualitativa es suministrar una metodología de investigación que admita alcanzar el complicado mundo de la experiencia vivida desde el punto de vista de las personas que la viven.(universidad de Jaén, n.d.)

Para emprender el trabajo y el desarrollo del referencial teórico se utilizaron metodologías y procedimientos que contienen el análisis y revisión de bibliografías, documentos, y fuentes secundarias. El enfoque principal está basado en la norma de control interno de información y el análisis de la misma.

La revisión de las normas de control interno 410 Tecnologías se obtendrán información de la página de la Contraloría General del Estado

Así como la revisión de los procesos se utilizará el libro de ISACA "esta publicación contiene una guía de referencia detallada de los procesos que están definidos en el modelo de procesos de referencia de Cobit".

Esta investigación está basada en un enfoque cualitativo que aporta la utilización de un procedimiento de investigación para la cual se realizó mediante el método comparativo utilizando como un medio sistemático y ordenado para examinar semejanzas que puede existir entre la normativa y los procesos, con estas bases se realizó una comparación agrupando los alcances de la normativa de control interno 410 denominada "Tecnologías de Información" de la Contraloría General del Estado y los procesos de "Gestión de Información" de Cobit 5,

teniendo como herramienta de apoyo para consolidar información en cada análisis realizado se utilizó el programa de Excel.

2.6 Propuesta

Se pretende realizar una comparación de los procesos de Cobit 5 con las normas de control interno 410, obteniendo los resultados de dicha comparación se verificará el porcentaje de las similitudes de las normas o procesos que utiliza la Contraloría General Del Estado.

Los resultados se darán a conocer a través del método comparativo de las normas con mayor similitud que existe entre las normativas de 410 y Cobit5.

CAPÍTULO 3.

3. Análisis comparativo de normativas

Para la realización del análisis de las normativas 410 de la Contraloría General Del Estado versus Cobit 5 se construyó un cuadro donde se encuentran todos los componentes del subgrupo de la normativa 410 con su respectiva información para contrastar de una forma establecida el alcance de cada uno de las normativas y proceder a realiza la comparación y el análisis con los procesos que está compuesto Cobit 5.

En la tabla 8 se da a conocer cada alcance que tiene la normativa 410 relacionada a la tecnología de la información.

ALCANCES	
Norma	Componente de la norma
410-01	**Organización informática** • Debe estar bajo la responsabilidad de una unidad que administre y gestione las tecnologías de información de la organización. • La unidad de tecnología de información está posicionada dentro de la estructura organizacional. • La unidad de tecnología de información permite asesorar y apoyar a la alta dirección participando en la toma de decisiones a la institución como en la mejora tecnológica. • La unidad de tecnología de información posee una estructura interna que satisfacen los objetivos y los avances tecnológicos. • Existe una gestión estructurada de cambios orientada a mejora tecnológica
410-02	**Segregación de funciones** • Existen funciones y responsabilidades especificadas para el personal de tecnologías de información • Existe supervisión de los roles y funciones del personal de TI en cada una de las áreas. • Existe una descripción documentada que está conformada por la unidad de tecnología de información, contemplara las responsabilidades y experiencias necesarias para cada posición.
410-03	Plan informático estratégico de tecnología

	• Existe un plan informático de tecnologías de información alineados al plan estratégico institucional. • Existen planes operativos dentro del plan informático estratégico • Posee la unidad de tecnologías de información un portafolio de proyectos y de servicios. • Existen revisiones periódicas de control del plan estratégico y del plan operativo de la unidad de tecnologías de información. • Existen revisiones de cumplimiento de los proyectos planificados en dependencia de los cronogramas establecidos
410-04	Políticas y procedimientos • Existen políticas definidas que apoyan a la gestión de las TICS • Existen procedimientos que rigen las actividades de la gestión de TICS • Las políticas y procedimientos garantizan la calidad, seguridad, confidencialidad, controles internos, propiedad intelectual, firmas electrónicas y mensajería de datos legalidad del software. • Existen controles, sistemas de aseguramiento de la calidad y gestión de riesgos, al igual que directrices y estándares tecnológicos. • Existe una socialización con los funcionarios y usuarios finales • Existen intercambios de información con otras entidades basadas en políticas de confidencialidad de la información.
410-05	Modelo de información organizacional • Existe un modelo de información definido para la creación uso y compartición de información institucional • Poseen un diccionario de datos corporativos, que incluyen reglas de validación y controles de integridad • Existe un proceso de clasificación de datos en la cual se aplique niveles de seguridad y disponibilidad
410-06	Administración de proyectos tecnológicos • Se describe el alcance, los objetivos y las relaciones con otros proyectos institucionales • Se especifica el cronograma de actividades y los recursos involucrados en la consecución del proyecto • Se considera el costo total de propiedad (CTP)con todos los costos directos e indirectos asociados • Se define un líder por proyecto • Los proyectos se los ejecuta por etapas (inicio, planeación, ejecución, control, monitoreo y cierre del proyecto) así como los entregables, aprobaciones, compromisos formales o documentos electrónicos legalizados.

	• Existe socialización al inicio de cada etapa importante del proyecto entre todos los involucrados • Existe un análisis de riesgos respectivo asociado al proyecto • Existe un monitoreo del control del avance del proyecto • Existe un plan de control de cambios y un plan de aseguramiento de la calidad • Los procesos de cierre incluyen la aceptación formal y las pruebas que certifiquen la calidad y el cumplimento de los objetivos planteados junto con los beneficios obtenidos.
410-07	Desarrollo y adquisición de software aplicativo • La adquisición de software o soluciones tecnológicas se las hace en función dl portafolio de proyectos y servicios priorizados en los planes estratégicos y operativos aprobados, considerando las políticas públicas establecidas por el estado • Existe estándares internacionales, metodologías y buenas prácticas para la codificación de software, nomenclaturas, interfaz de usuario interoperabilidad, pruebas unitarias y de integración. • Se conforman un equipo multidisciplinario enfocado al acompañamiento en todas las fases del desarrollo del software • Se manejan pistas de auditoria en los sistemas de información desarrollados • Los contratos para la adquisición de aplicaciones tecnológicas poseen el nivel de detalle suficiente que permita correlacionar las necesidades tecnológicas versus las adquiridas, así como las garantías del fabricante, licencias y actualizaciones respectivas. • Existen actas de aceptación de por parte de los usuarios del paso de los sistemas probados y aprobados desde el ambiente de desarrollo prueba al ambiente de producción • Existen manuales técnicos de instalación, configuración y de usuario de las aplicaciones y su respectiva distribución de los mismos.
410-08	Adquisiciones de infraestructura tecnológica • La adquisiciones tecnológicas se las hace en función de los objetivos de la organización, principios de calidad, portafolio de proyectos y servicios, que constan en el Plan Anual de Contratación de la institución • Existe un análisis de la capacidad tecnológica, evaluando los riesgos asociados, los costos y la vida útil de los activos tecnológicos • Los contratos para la adquisición tecnológica poseen el nivel de detalle suficiente que permita correlacionar las necesidades tecnológicas versus las adquiridas • Existen acuerdos de nivel de servicio especificados en los contratos con proveedores de servicio externos a la

	institución puntualizando los aspectos de seguridad, confidencialidad y la propiedad de la información
410-09	Mantenimiento y control de la infraestructura tecnológica • Existen definidos procedimientos de mantenimiento y liberación de software • Existe una gestión adecuada del cambio a través de un análisis de riesgos previo a la implementación en el ambiente de producción • La unidad de tecnologías de información lleva un control y registro de las versiones del software que son puestos en producción • Existe un ambiente de pruebas previo a la puesta en producción de las aplicaciones fortaleciendo el principio de confiabilidad y seguridad • Existen planes de mantenimiento preventivo y correctivo de la infraestructura tecnológica • Existe un inventario tecnológico actualizado de los bienes informáticos con el detalle de las características y responsables sobre los mismos
410-10	Seguridad de la tecnología de información • Existe una ubicación adecuada y control de acceso físico a la unidad de tecnologías de información y en especial a las áreas de servidores, desarrollo y bibliotecas • Existen procedimientos de obtención periódica de respaldos de información • Existe un almacenamiento de la información critica y sensible en lugares externos de la institución • Existe una implementación y administración de seguridades a nivel de software y hardware y la evaluación periódica de las mismas • Existen instalaciones físicas adecuadas que incluyan mecanismos y dispositivos especializados capaces de monitorear y controlar el fuego, mantener un ambiente de temperatura controlado, energía acondicionada. • Existe un centro de procesamiento alternativo • Existen definidos procedimientos de políticas y procedimientos que favorezcan la seguridad de la información
410-11	Plan de contingencias • Posee la unidad de tecnologías de información implementando un plan de contingencias • Existe implementando un plan de respuesta a riesgos en función de los bienes y servicios tecnológicos • Existe un plan de continuidad de operaciones que contemple la puesta en marcha de un centro de cómputo alterno • Existe un plan de recuperación de desastres

	• Existe un comité con roles específicos y nombres de los encargados con sus funciones especificadas en caso de suscitarse una emergencia
410-12	Administración de soporte de tecnología de información • La entidad posee un área encargada del soporte tecnológico • El soporte tecnológico se lo hace en base a un esquema de procedimientos definidos y documentados • Se efectúan análisis de capacidad de los recursos tecnológicos en pos de soportar escenarios futuros • Existe seguridad en los sistemas de la entidad bajo el otorgamiento de una identificación única a los usuarios (internos, externos y temporales) • Existen estandarizaciones de la identificación, autenticación y autorización de los usuarios, así como la administración de sus cuentas • Existe un control periódico de las cuentas de usuario y los privilegios asociados a los dueños de procesos y administradores de los sistemas de tecnologías de información • Existen medidas de prevención y corrección que protejan a los sistemas institucionales de software malicioso y virus • Existe niveles de servicio y de operación para los servicios críticos de la institución basados en los requerimientos de los usuarios y capacidades tecnológicas • Existe administración de los incidentes reportados, requerimientos de servicio y solicitudes de información y de cambios a través de una mesa de servicio • La unidad de tecnologías de información posee un repositorio centralizado de configuraciones de hardware y software que garanticen su acceso priorizado la integridad y disponibilidad de la misma
410-13	Monitoreo y evaluación de los procesos y servicios • La unidad de tecnología pese un proceso definido y una metodología que permita monitorear su impacto en la institución • Existen indicadores sobre la base de las operaciones de la entidad de desempeño y métricas que permitan monitorear la gestión en pos de una correcta toma de decisiones • Existe una evaluación de mejora continua de los servicios • Existe una evaluación de la satisfacción del cliente una vez que los servicios han sido entregados.
410-14	Sitio web, servicio de internet e intranet • Existen normas, procedimientos e instructivos de instalación, configuración y utilización de los servicios de internet, intranet, correo electrónico y sitio web • La unidad de tecnología de información ha implementado aplicaciones web, servicios web y móviles que han contribuido a la automatización de procesos de la institución

410-15	Capacitación informática • Existe un plan de capacitación informático en la institución • Existe un análisis de requerimientos de capacitación para el personal de TI • Existe capacitación a los usuarios de la institución que acceden a los servicios en coordinación con el área de Talento Humano
410-16	Comité informático • Existe un comité informático en la organización • Se especifica la reglamentación, las funciones, a las atribuciones y responsabilidades de comité informático • Se ejecutan evaluaciones sobre las mejoras de los servicios implementados y sobre la creación de nuevas implementaciones
410-17	Firmas electrónicas • El certificado digital de la firma electrónica es emitido por una entidad certificadora acreditada • Los archivos electrónicos firmados digitalmente se encuentran en un estado de integridad y disponibles al usuario propietario de la información • Existen políticas internas establecidas para el manejo y administración de la firma electrónica.

410-16	Comité informático • Existe un comité informático en la organización • Se especifica la reglamentación, las funciones, a las atribuciones y responsabilidades de comité informático • Se ejecutan evaluaciones sobre las mejoras de los servicios implementados y sobre la creación de nuevas implementaciones
410-17	Firmas electrónicas • El certificado digital de la firma electrónica es emitido por una entidad certificadora acreditada • Los archivos electrónicos firmados digitalmente se encuentran en un estado de integridad y disponibles al usuario propietario de la información • Existen políticas internas establecidas para el manejo y administración de la firma electrónica.

tabla 8: Alcances de la normativa 410
Fuente: Normas de control interno para las entidades, organismos del sector público y de las personas jurídicas de derechos privados que dispongan de recursos públicos
Realizado por: Rosalía Contreras

3.1. Análisis Cobit 5 vs la normativa de control interno 410 de la contraloría general del estado

Con el objetivo de reconocer que procesos y subprocesos de Cobit 5 se relaciona con las normativas 410 que utiliza la Contraloría General Del Estado en relación con el control interno de seguridad de información se procede a comparar la tabla 8 alcances de la normativa 410, con la Tabla 5 Procesos de Gestión de información. Realizando la unión de las tablas para efectuar la comparación y visualizar que procesos están relacionados. Los resultados de la comparación se encuentran en la tabla 9.

3.1.1 Resultados de comparación de la normativa 410 vs Cobit 5

Como se puede observar en la tabla 9, algunos alcances de la normativa 410 no se relaciona en su totalidad con los procesos de Cobit 5 basado únicamente en el control interno de información, estos son los siguientes:

- “410-01 Organización informática
- 410-04 Políticas y procedimientos
- 410-05 Modelo de información organizacional
- 410-06 Administración de proyectos tecnológicos
- 410-07 Desarrollo de adquisición de software aplicativo
- 410-08 Adquisiciones de infraestructura tecnológica
- 410-09 Mantenimiento y control de la infraestructura tecnológica
- 410-13 Monitoreo y evaluación de los procesos y servicios
- 410-14 Sitio web, servicio de internet e intranet
- 410-15 Capacitación informática
- 410-16 Comité informático
- 410-17 Firmas electrónicas”

Los alcances de estas normativas no se relacionan con ninguno de los tres procesos de Cobit5, ya que esta comparación está centrada únicamente en el control interno de la información.

Para realizar el análisis de comparación de la tabla 9 se implementó el método de comparación o llamada análisis comparativo que consiste en la utilización de observaciones extraídas de normativas y procesos para examinar sus semejanzas para lo cual se empleó una herramienta de benchmarking (evaluación comparativa), como lo estamos realizando en este tema de investigación con la comparación de los procesos de Cobit 5 que tienen relación con las normativas 410.

Para realizar el análisis grafico entre las normativas se extrajo solo las normas que tienen semejanza con los procesos para obtener el número de coincidencias y así obtener un porcentaje.

En el proceso **APO13 GESTION DE LA SEGURIDAD** las normativas que tienen coincidencias son las siguientes:

- "410-02 Segregación de funciones
- 410-03 Plan informático estratégico de tecnología.
- 410-10 Seguridades de la tecnología de información.
- 410-12 Administración de soporte de tecnología de información"

410-02 Segregaciones de funciones

La normativa tiene tres alcances y se encontró una coincidencia con un porcentaje del 12% y es la siguiente:

- "Existe supervisión de los roles y funciones del personal de TI en cada una de las áreas", tiene relación con el subproceso APO13.01 "establecer y mantener un SGSI, se establece y mantiene un SGSI que proporcione un enfoque estándar , formal y continuo a la gestión de seguridad para la información, tecnología y procesos de negocio que

estén alineados a los requerimientos de negocio y la gestión de seguridad en la organización, definir y comunicar roles y las responsabilidades de la gestión de la seguridad de la información".

410-03 Plan informático estratégico de tecnología.

La normativa consta de cinco alcances de los cuales se obtuvo dos coincidencias y su porcentaje es de 25%.

- "Existe un plan informático de tecnología de información alineados al plan estratégico institucional", su relación es con el subproceso APO13.02 "definir y gestionar un plan de tratamiento de riesgo de la seguridad de la información, se mantiene un plan de seguridad de información que describa como se gestionan y alinean los riesgos de seguridad de información con la estrategia y la arquitectura de la organización. Se asegura que las recomendaciones para implementar las mejoras en seguridad se basan en casos de negocios aprobados, se implementan como parte integral de desarrollo de soluciones y servicios y se operan después como parte integral de las operaciones del negocio".
- "Existen revisiones periódicas de control del plan estratégico y del plan operativo de la unidad de tecnologías de información", se relaciona con el subproceso APO 13.03 "supervisar y revisar el SGSI, se comunica regularmente la necesidad y los beneficios de la mejora continua de la seguridad de información. Recolectar y analizar datos sobre el SGSI y la mejora de su efectividad, corregir las no conformidades para prevenir recurrencias, realizar revisiones periódicas del SGSI incluyendo aspectos de política, objetivos y prácticas de seguridad del SGSI".

410-10 Seguridades de la tecnología de información.

Esta normativa consta de siete alcances y se obtuvo una coincidencia con un porcentaje de 13%, Las coincidencias son las siguientes:

- "Existe una ubicación adecuada y control de acceso físico a la unidad de tecnologías de información y en especial a las áreas de servidores, desarrollo y bibliotecas", se relaciona con el subproceso APO13.01 "establecer y mantener un SGSI, se establece un SGSI proporcionando un enfoque estándar, formal y continuo para la seguridad de la información, alineando el SGSI con el enfoque global de la gestión de seguridad en la organización."

410-12 Administraciones de soporte de tecnología de información

Esta normativa consta de diez alcances de los cuales se encontró cuatro coincidencias obteniendo un porcentaje de 50%. Las coincidencias son las siguientes:

- "Existe seguridad en los sistemas de la entidad bajo el otorgamiento de una identificación única a los usuarios (internos, externos y temporales)," se relaciona con el subproceso "**APO13.01** Establecer y mantener un SGSI; se alinea bajo un enfoque global de la gestión de seguridad en la empresa, manteniendo la seguridad de la asignación de roles y responsabilidades".
- "Existen estandarizaciones de la identificación, autenticación y autorización de los usuarios así como la administración de sus cuentas;" se relaciona con el subproceso "**APO13.01** Establecer y mantener un SGSI; se define roles y responsabilidades para la gestión de la seguridad de la información, definiendo alcances y límites del SGSI en términos de las características de la empresa, organización, localización, activos y tecnología, se incluyen detalles y justificación para cualquier actividad que realicen."
- "Existe un control periódico de las cuentas de usuario y los privilegios asociados a los dueños de procesos y administradores de los sistemas de tecnologías de información;"

se relaciona con el subproceso "**APO13.03** Supervisar y revisar el SGSI; se realiza revisiones periódicas y prácticas de seguridad del SGSI, registrando las acciones y eventos que podrían tener un impacto en la efectividad o el desempeño del SGSI."

- "Existen medidas de prevención y corrección que protejan a los sistemas institucionales de software malicioso y virus;" se relaciona con el subproceso "**APO13.02** Definir y gestionar un plan de tratamiento de riesgo de la seguridad de la información; se formula y se mantiene un plan de tratamiento de riesgos de seguridad de la integrando y planificando el diseño, implementación y supervisión de los procedimientos de seguridad de información y otros controles que permitan la prevención y detección temprana de eventos de seguridad así como la respuesta a incidentes de seguridad."

En el proceso **DSS04 GESTION DE LA CONTINUIDAD** las normativas que tienen coincidencias son las siguientes:

- "410-10 Seguridad de la tecnología de información
- 410-11 Plan de contingencias
- 410-12 Administración de soporte de tecnología de información"

410-10 Seguridad de la tecnología de información

Esta normativa se encontró tres coincidencias y su porcentaje es de 37%. Las coincidencias son las siguientes:

- "Existen procedimientos de obtención periódica de respaldos de información;" su relación es con el subproceso "**DSS04.07** Gestionar acuerdos de respaldo; mantiene la disponibilidad de la información crítica del negocio manteniendo legibles las copias de seguridad y las archivadas periódicamente."
- "Existe un almacenamiento de la información crítica y sensible en lugares externos de la institución"; se relaciona con el subproceso "**DSS04.07** Gestionar acuerdos de

respaldo; se definen los requerimientos del almacenamiento de las copias de seguridad, dentro y fuera de la propia ubicación, que satisfaga los requerimientos del negocio. Considerar la accesibilidad requerida a las copias de seguridad."

- "Existe un centro de procesamiento alternativo" se relaciona con el subproceso "**DSS04.03** Desarrollar e implementar una respuesta a la continuidad del negocio; se desarrolla un plan de continuidad de negocio (BCP) basado en la estrategia que documente los procedimientos y la información lista para el uso en un incidente para facilitar que la empresa continúe con sus actividades críticas."

410-11 Plan de contingencias

En esta normativa se encontró tres coincidencias con un porcentaje de 38%. Las coincidencias son las siguientes:

- "Posee la unidad de tecnologías de información implementando un plan de contingencias"; se relaciona con el subproceso "**DSS04.02** Mantener una estrategia de continuidad; se evalúa las opciones de gestión de la continuidad del negocio y se escoge una estrategia de continuidad viable y efectiva que pueda asegurar la continuidad y recuperación de la empresa frente a un desastre u otro incidente mayor u o disrupción."
- "Existe un plan de continuidad de operaciones que contemple la puesta en marcha de un centro de cómputo alterno;" se relaciona con el subproceso "**DSS04.03** Desarrollar e implementar una respuesta a la continuidad del negocio; se define las condiciones y procedimientos de recuperación que permita la reanudación de los procesos de negocio, incluyendo la actualización y conciliación de las bases de datos para preservar la integridad de la información."
- "Existe un plan de recuperación de desastres"; ser relaciona con el subproceso "**DSS04.04** Ejercitar, proba y revisar el BCP; probar los acuerdos de continuidad regularmente para ejercitar los planes de recuperación respecto a unos resultados

predeterminados, para permitir el desarrollo de soluciones innovadoras y para ayudar a verificar que el plan funcione en el tiempo como se espera."

410-12 Administración de soporte de tecnología de información

En esta normativa se encontró dos coincidencias y su porcentaje es de 25%. Las coincidencias son las siguientes:

- "Se efectúan análisis de capacidad de los recursos tecnológicos en pos de soportar escenarios futuros"; se relaciona con el subproceso "**DSS04.05** Revisar, mantener y mejorar el plan de continuidad; se revisa el plan de continuidad regularmente para considerar el impacto de cambios nuevos o mayores en: organización de la empresa, procesos de negocio, acuerdos de externalización, tecnologías, infraestructura, sistemas operativos y sistemas de aplicaciones."
- "Existe niveles de servicio y de operación para los servicios críticos de la institución basados en los requerimientos de los usuarios y capacidades tecnológicas"; se relaciona con el subproceso "**DSS04.03** Desarrollar e implementar una respuesta a la continuidad del negocio; se mantiene planes de continuidad de negocio operativos que contengan los procedimientos que deben ser seguidos para permitir continuar operando los procesos críticos del negocio."

En el proceso **DSS05 GESTION DE SERVICIOS DE SEGURIDAD** las normativas que tienen coincidencias son las siguientes:

- "410-02 Segregación de funciones
- 410-10 Seguridad de la tecnología de información
- 410-12 Administración de soporte de tecnología de información"

410-02 Segregación de funciones

En esta normativa se obtuvo dos coincidencias y su porcentaje es de 40%. Las coincidencias son las siguientes:

- "Existen funciones y responsabilidades definidas para el personal de tecnologías de información" se relaciona con el subproceso "**DSS05.04** gestionar la identidad del usuario y el acceso lógico; se asegura que todos los usuarios (internos, externos y temporales) y su actividad en sistemas de TI son identificables unívocamente. Identificar unívocamente todas las actividades de proceso de información por usuario."
- "Existe supervisión de los roles y funciones del personal de TI en cada una de las áreas"; se relaciona con el subproceso "**DSS05.04** Gestionar la identidad del usuario y el acceso lógico; se identifica todas las actividades de proceso de la información por roles funcionales, coordinando con las unidades de negocio y asegurando que todos los roles estén definidos consistentemente."

410-10 Seguridad de la tecnología de información

En esta normativa se encontraron dos coincidencias su porcentaje es de 40%. Las coincidencias son las siguientes:

- "Existe una implementación y administración de seguridades a nivel de software y hardware y la evaluación periódica de las mismas"; se relaciona con el subproceso "**DSS05.02** Gestionar la seguridad de la red y las conexiones; se utiliza medidas de seguridad y procedimientos de gestión relacionados para proteger la información en todos los modos de conexión realizando pruebas periódicas de la seguridad del sistema para determinar la adecuación de la protección del sistema."
- "Existen definidos procedimientos de políticas y procedimientos que favorezcan la seguridad de la información"; se relaciona con el subproceso "**DSS05.01** proteger

contra software malicioso (malware); se implementa y se mantiene efectivas medidas preventivas de detección y correctivas a lo largo de la empresa para proteger los sistemas de información, revisando y evaluando regularmente la información sobre posibles amenazas."

410-12 Administración de soporte de tecnología de información

En esta normativa se encontró una coincidencia con un porcentaje de 20%. La coincidencia es la siguiente:

- "Existen medidas de prevención y corrección que protejan a los sistemas institucionales de software malicioso y virus;" se relaciona con el subproceso "**DSS05.01** proteger contra software malicioso (malware); se implementa efectivas medidas preventivas de detección y correctivas a lo largo de la empresa para proteger los sistemas de información y tecnología. Instalación y activación de herramientas de protección frente a software malicioso en todas las instalaciones de proceso, con ficheros de definición de software malicioso que se actualicen según se requiera (automático o semiautomáticamente)." Los resultados se dan a conocer en la tabla 9.

Tabla 9 Comparación de normativas 410 vs Cobit 5

410 Tecnologia de la Informacion	APO 13 GESTION DE LA SEGURIDAD			DSS04: GESTIÓN DE LA CONTINUIDAD								DSS05: GESTIÓN DE SERVICIOS DE SEGURIDAD						
	APO13.01 Establecer y mantener un SGSI	APO13.02 Definir y gestionar un plan de tratamiento de riesgo de la seguridad de la información	APO13.03 Supervisar y revisar el SGSI	DSS04.01 Definir la política de continuidad de negocio, objetivos y alcance	DSS04.02 Mantener una estrategia de continuidad	DSS04.03 Desarrollar e implementar una respuesta a la continuidad del negocio	DSS04.04 Ejercitar, probar y revisar el BCP (plan de continuidad de negocio)	DSS040.05 Revisar, mantener y mejorar el plan de continuidad	DSS04.06 Proporcionar formación en el plan de continuidad	DSS04.07 Gestionar acuerdos de respaldo	DSS04.08 Ejecutar revisiones post-reanudación	DSS05.01 proteger contra software malicioso (malware)	DSS05.02 gestionar la seguridad de la red y las conexiones	DSS05.03 gestionar la seguridad de los puestos de usuario final	DSS05.04 gestionar la identidad del usuario y el acceso lógico	DSS05.05 gestionar el acceso físico a los activos de TI	DSS05.06 Gestionar Documentos Sensibles Y Dispositivos De Salida	DSS05.07 Supervisar la infraestructura para detectar eventos relacionados con la seguridad
410-01 Organización informatica																		
Debe estar bajo la responsabilidad de una unidad que administre y gestiónes las tecnologías de información de la organización.																		
La unidad de tecnología de información está posicionada dentro de la estructura organizacional.																		
La unidad de tecnología de información permite asesorar y apoyar a la alta dirección participando en la toma de decisiones a la institución como en la mejora tecnológica																		
La unidad de tecnología de información posee una estructura interna que satisfacen los objetivos y los avances tecnológicos.																		
Existe una gestión estructurada de cambios orientada a mejora tecnológica																		

410-02 Segregación de funciones																	
Existen funciones y responsabilidades definidas para el personal de tecnologías de información	x													x			
Existe supervisión de los roles y funciones del personal de TI en cada una de las áreas														x			
Existe una descripción documentada que está conformada por la unidad de tecnología de información, contemplara las responsabilidades y experiencias necesarias para cada posición.																	
410-03 Plan informático estratégico de tecnología																	
Existe un plan informático de tecnologías de información alineados al plan estratégico institucional.		x															
Existen planes operativos dentro del plan informático estratégico																	
Posee la unidad de tecnologías de información un portafolio de proyectos y de servicios																	
Existen revisiones periódicas de control del plan estratégico y del plan operativo de la unidad de tecnologías de información			x														
Existen revisiones de cumplimiento de los proyectos planificados en dependencia de los cronogramas establecidos																	
410-04 Políticas y procedimientos																	
Existen políticas definidas que apoyan a la gestión de las TICS																	
Existen procedimientos que rigen las actividades de la gestión de TICS																	
Las políticas y procedimientos garantizan la calidad, seguridad, confidencialidad, controles internos, propiedad intelectual, firmas electrónicas y mensajería de datos legalidad del software.																	
Existen controles, sistemas de aseguramiento de la calidad y gestión de riesgos, al igual que directrices y estándares tecnológicos																	
Existe una socialización con los funcionarios y usuarios finales																	
Existen intercambios de información con otras entidades basadas en políticas de confidencialidad de la información.																	

410-05 Modelo de información organizacional																		
Existe un modelo de información definido para la creación uso y compartición de información institucional																		
Poseen un diccionario de datos corporativos, que incluyen reglas de validación y controles de integridad																		
Existe un proceso de clasificación de datos en la cual se aplique niveles de seguridad y disponibilidad																		
410-06 Administración de proyectos tecnológicos																		
Se describe el alcance, los objetivos y las relaciones con otros proyectos institucionales																		
Se especifica el cronograma de actividades y los recursos involucrados en la consecución del proyecto																		
Se considera el costo total de propiedad (CTP)con todos los costos directos e indirectos asociados																		
Se define un líder por proyecto																		
Los proyectos se los ejecuta por etapas (inicio, planeación, ejecución, control, monitoreo y cierre del proyecto) así como los entregables, aprobaciones, compromisos formales o documentos electrónicos legalizados																		
Existe socialización al inicio de cada etapa importante del proyecto entre todos los involucrados																		
Existe un análisis de riesgos respectivo asociado al proyecto																		
Existe un monitoreo del control del avance del proyecto																		
Existe un plan de control de cambios y un plan de aseguramiento																		
Los procesos de cierre incluyen la aceptación formal y las pruebas que certifiquen la calidad y el cumplimento de los objetivos planteados junto con los beneficios obtenidos.																		

410-07 Desarrollo y adquisición de software aplicativo																			
La adquisición de software o soluciones tecnológicas se las hace en función del portafolio de proyectos y servicios priorizados en los planes estratégicos y operativos aprobados, considerando las políticas públicas establecidas por el estado																			
Existe estándares internacionales, metodologías y buenas prácticas para la codificación de software, nomenclaturas, interfaz de usuario interoperabilidad, pruebas unitarias y de integración.																			
Se conforman un equipo multidisciplinario enfocado al acompañamiento en todas las fases del desarrollo del software																			
Se manejan pistas de auditoria en los sistemas de información desarrollados																			
Los contratos para la adquisición de aplicaciones tecnológicas poseen el nivel de detalle suficiente que permita correlacionar las necesidades tecnológicas versus las adquiridas, así como las garantías del fabricante, licencias y actualizaciones respectivas.																			
Existen actas de aceptación de por parte de los usuarios del paso de los sistemas probados y aprobados desde el ambiente de desarrollo prueba al ambiente de producción																			
Existen manuales técnicos de instalación, configuración y de usuario de las aplicaciones y su respectiva distribución de los mismos.																			
410-08 Adquisiciones de infraestructura tecnológica																			
La adquisiciones tecnológicas se las hace en función de los objetivos de la organización, principios de calidad, portafolio de proyectos y servicios, que constan en el Plan Anual de Contratación de la institución																			
Existe un análisis de la capacidad tecnológica, evaluando los riesgos asociados, los costos y la vida útil de los activos tecnológicos																			
Los contratos para la adquisición tecnológica poseen el nivel de detalle suficiente que permita correlacionar las necesidades tecnológicas versus las adquiridas																			
Existen acuerdos de nivel de servicio especificados en los contratos con proveedores de servicio externos a la institución puntualizando los aspectos de seguridad, confidencialidad y la propiedad de la información																			

410-09 Mantenimiento y control de la infraestructura tecnológica																	
Existen definidos procedimientos de mantenimiento y liberación de software																	
Existe una gestión adecuada del cambio a través de un análisis de riesgos previo a la implementación en el ambiente de producción																	
La unidad de tecnologías de información lleva un control y registro de las versiones del software que son puestos en producción																	
Existe un ambiente de pruebas previo a la puesta en producción de las aplicaciones fortaleciendo el principio de confiabilidad y seguridad																	
Existen planes de mantenimiento preventivo y correctivo de la infraestructura tecnológica																	
Existe un inventario tecnológico actualizado de los bienes informáticos con el detalle de las características y responsables sobre los mismos																	
410-10 Seguridad de la tecnología de información																	
Existe una ubicación adecuada y control de acceso físico a la unidad de tecnologías de información y en especial a las áreas de servidores, desarrollo y bibliotecas	x																
Existen procedimientos de obtención periódica de respaldos de información										x							
Existe un almacenamiento de la información critica y sensible en lugares externos de la institución										x							
Existe una implementación y administración de seguridades a nivel de software y hardware y la evaluación periódica de las mismas																x	
Existen instalaciones físicas adecuadas que incluyan mecanismos y dispositivos especializados capaces de monitorear y controlar el fuego, mantener un ambiente de temperatura controlado, energía acondicionada.																	
Existe un centro de procesamiento alternativo						x											
Existen definidos procedimientos de políticas y procedimientos que favorezcan la seguridad de la información												x					

410-11 Plan de contingencias																		
Posee la unidad de tecnologías de información implementando un plan de contingencias					x													
Existe implementado un plan de respuesta a riesgos en función de los bienes y servicios tecnológicos																		
Existe un plan de continuidad de operaciones que contemple la puesta en marcha de un centro de cómputo alterno						x												
Existe un plan de recuperación de desastres							x											
Existe un comité con roles específicos y nombres de los encargados con sus funciones especificadas en caso de suscitarse una emergencia																		
410-12 Administración de soporte de tecnología de información																		
La entidad posee un área encargada del soporte tecnológico																		
El soporte tecnológico se lo hace en base a un esquema de procedimientos definidos y documentados																		
Se efectúan análisis de capacidad de los recursos tecnológicos en pos de soportar escenarios futuros								x										
Existe seguridad en los sistemas de la entidad bajo el otorgamiento de una identificación única a los usuarios (internos, externos y temporales)	x																	
Existen estandarizaciones de la identificación, autenticación y autorización de los usuarios así como la administración de sus cuentas	x																	
Existe un control periódico de las cuentas de usuario y los privilegios asociados a los dueños de procesos y administradores de los sistemas de tecnologías de información			x															
Existen medidas de prevención y corrección que protejan a los sistemas institucionales de software malicioso y virus		x									x							
Existe niveles de servicio y de operación para los servicios críticos de la institución basados en los requerimientos de los usuarios y capacidades tecnológicas						x												
Existe administración de los incidentes reportados, requerimientos de servicio y solicitudes de información y de cambios a través de una mesa de servicio																		
La unidad de tecnologías de información poseen un repositorio centralizado de configuraciones de hardware y software que garanticen su acceso priorizado la integridad y disponibilidad de la misma																		

410-13 Monitoreo y evaluación de los procesos y servicios																		
La unidad de tecnología pese un proceso definido y una metodología que permita monitorear su impacto en la institución																		
Existen indicadores sobre la base de las operación de la entidad de desempeño y métricas que permitan monitorear la gestión en pos de una correcta toma de decisiones																		
Existe una evaluación de mejora continua de los servicios																		
Existe una evaluación de la satisfacción del cliente una vez que los servicios han sido entregados.																		
410-14 Sitio web, servicio de internet e intranet																		
Existen normas, procedimientos e instructivos de instalación, configuración y utilización de los servicios de internet, intranet, correo electrónico y sitio web																		
La unidad de tecnología de información ha implementado aplicaciones web, servicios web y móviles que han contribuido a la automatización de procesos de la institución																		
410-15 Capacitación informática																		
Existe un plan de capacitación informático en la institución																		
Existe un análisis de requerimientos de capacitación para el personal de TI																		
Existe capacitación a los usuarios de la institución que acceden a los servicios en coordinación con el área de Talento Humano																		
410-16 Comité informático																		
Existe un comité informático en la organización																		
Se especifica la reglamentación, las funciones, a las atribuciones y responsabilidades de comité informático																		
Se ejecutan evaluaciones sobre las mejoras de los servicios implementados y sobre la creación de nuevas implementaciones																		
410-17 Firmas electrónicas																		
El certificado digital de la firma electrónica es emitido por una entidad certificadora acreditada																		
Los archivos electrónicos firmados digitalmente se encuentran en un estado de integridad y disponibles al usuario propietario de la información																		
Existen políticas internas establecidas para el manejo y administración de la firma electrónica.																		

Tabla 9: Comparación de normativas

Realizado por: Rosalía Contreras

CAPITULO 4

4. Conclusiones Y Recomendaciones

4.1 Conclusiones

- En esta investigación se cumplió el primer objetivo "Llevar a cabo una revisión de los trabajos más relevantes, relacionados con la norma Cobit 5 y la 410 de la Contraloría General del Estado." Se encontró información de trabajos que están relacionados a las dos normativas y se encuentran implementadas en distintas organizaciones donde realizan diagnósticos, verifican el cumplimiento de las normativas y utilizan como una herramienta clave para verificar si existe debilidades o fortalezas y poder mejorar los procesos de la organización.

- Cumpliendo con el segundo objetivo específico es "Analizar las normativas de Cobit 5 relacionado con la seguridad de la información y la normativa 410 que posee la Contraloría General Del Estado" Este análisis se encuentra en el capítulo 2 Marco teórico. En este capítulo se identifica cuáles son los procesos que están relacionados a la gestión de información, se define la importancia de la gestión y el gobierno de TI. En conclusión, al primer objetivo es:

- En el área de tecnología es importante trabajar con el gobierno de TI ya que al implementarlo permite alinearnos a los objetivos, estrategias, permitiendo proporcionar el mejor uso de la tecnología y de las estructuras organizativas en coordinación con la alta dirección para generar recursos de forma eficiente, valorar a los procesos que reflejaran en servicios tecnológicos.
- Al trabajar con la gestión de TI nos permite estar alineados a los servicios de TI proporcionados con las necesidades de la organización, involucrándose el uso de

outsourcing (subcontratación) y servicios compartidos manteniendo una base de conocimientos amplia dentro de la empresa paras que las prácticas sean exitosas.

- Cobit 5 es conocida como una guía de las mejores prácticas presentada como Framework que está dirigida al control y supervisión de tecnología de la información, consta de una serie de recurso que sirve de modelo de referencia para la gestión de TI, es un marco integral que está compuesto de 37 procesos, normativas de seguridad, servicios tecnológicos, gestión de proyectos, arquitectura empresarial; como se da a conocer en el capítulo 2.
- Los procesos de gestión de información están enfocados en la seguridad de la información teniendo como base el framework de las mejores prácticas implementado guías para la protección de la información para todos los niveles de la organización con procesos que brindan una guía básica para monitorear un sistema de gestión de la seguridad como se da a conocer en el capítulo 2

Respecto a "Analizar las normativas que posee la Contraloría General Del Estado". Para analizar de forma detallada se construyó dos matrices.

- La primera matriz se encuentra todas las normas de la contraloría general del estado que se utiliza como marco de referencia para todas las organizaciones, están orientadas a originar una apropiada administración financiera, tecnología de la información de los recursos públicos y evidenciar el correcto funcionamiento administrativo de las entidades y organismos del sector público.
- La segunda matriz se visualiza el subgrupo 410 donde se encuentra las normas para la valoración del control interno para la gestión de tecnología de información que cubre temas variados como: la organización Informática, segregación de funciones, plan informático, políticas y procedimientos, modelos de información organizacional,

administración de proyectos tecnológicos, desarrollo y adquisición de software aplicativo, adquisiciones de infraestructura tecnológica, mantenimiento de la infraestructura, seguridad de la tecnología de información, plan de contingencia, administración y soporte tecnológico, monitoreo y evaluación de procesos, sitios web, capacitación, comité informático, firmas electrónicas, como se da a conocer en el capítulo 2.

- En referente al tercer objetivo "Realizar una comparación de las normativas analizadas, y representar gráficamente los resultados". En el capítulo 3 se obtuvo el análisis comparativo de la norma 410 que corresponde a tecnología de información vs los procesos de Cobit 5 implementando el método de comparación.

  - El método comparativo nos ayuda a examinar la semejanza que puede existir entre la normativa y los procesos.
  - Mediante la comparación se obtuvo 12 normativas que no están relacionados con los procesos de Cobit ya que la comparación se centra únicamente en control interno de seguridad de la información.
  - También se obtuvo normativas que si están relacionadas con los procesos de Cobit 5 las cuales están enlazados con los temas de: segregación de funciones, plan informático estratégico de tecnología, seguridades de la tecnología de información, plan de contingencias, administración de soporte de tecnología de información.

La representación gráfica de los resultados de la comparación de las normativas se realizó la extracción de las normas que tienen similitudes con los procesos que da a conocer el porcentaje de coincidencias que existen en cada normativa. Este análisis se encuentra en el apartado de Anexos.

- En cada normativa se obtuvo un número de coincidencias las cuales son representados gráficamente dando a conocer su porcentaje.

4.2 Recomendaciones

- Si se pretende desarrollar normas o políticas del control interno de seguridad de la información bajo la norma 410 y cobit 5 se recomienda revisar cada proceso que tiene Cobit 5 por lo que están orientados a distintas áreas para una organización.
- Para obtener resultados certeros de una comparación se recomienda realizar con un método comparativo en el que interviene un conjunto de técnicas para llegar a obtener semejanzas o diferencias entre dos o más casos.

A la contraloria general del estado

- Se debe supervisar periódicamente los procedimientos de seguridad de información conjuntamente con otros controles que permitan la prevención y detección temprana de eventos maliciosos registrando las acciones y eventos que puedan tener un impacto en la efectividad o en el desempeño del SGSI.
- Tener un inventario de posibles soluciones revisadas por la dirección para asegurar que el alcance sea adecuado y que se puedan implementar para gestionar los riesgos identificando procesos de soporte y servicios de TI.
- Analizar los requerimientos actuales y futuros de elaboración de informes considerando canales de comunicación sugerencias y retroalimentación de las partes interesadas.
- Establecer un tiempo mínimo necesario para recuperar un proceso y su soporte de TI basándose en una duración de interrupción de actividades máxima tolerable.
- Es importante realizar un estudio de implementación de las buenas prácticas de TI que cubran los procesos más importantes en el área de seguridad de tecnología de información, administración de soporte de tecnología de información, plan de contingencias ya que estas normativas establecen mecanismos para proteger y salvaguardar la información que se procesan mediante sistemas informáticos facilitando

una adecuada administración en el soporte tecnológico garantizando la seguridad, confidencialidad y disponibilidad de la información.

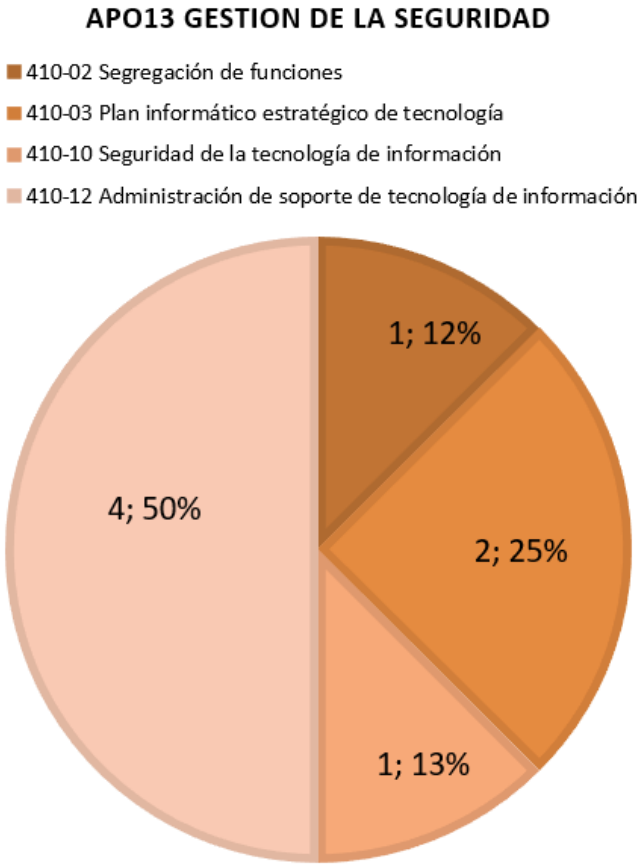
- Los análisis realizados deben ser interpretados únicamente como una guía para saber que procesos de Gestión de Información no están siendo considerados en la norma de control interno 410 “Tecnologías de Información”.

ANEXOS

COINCIDENCIAS Y PROMEDIOS DE NORMATIVAS Y PROCESOS

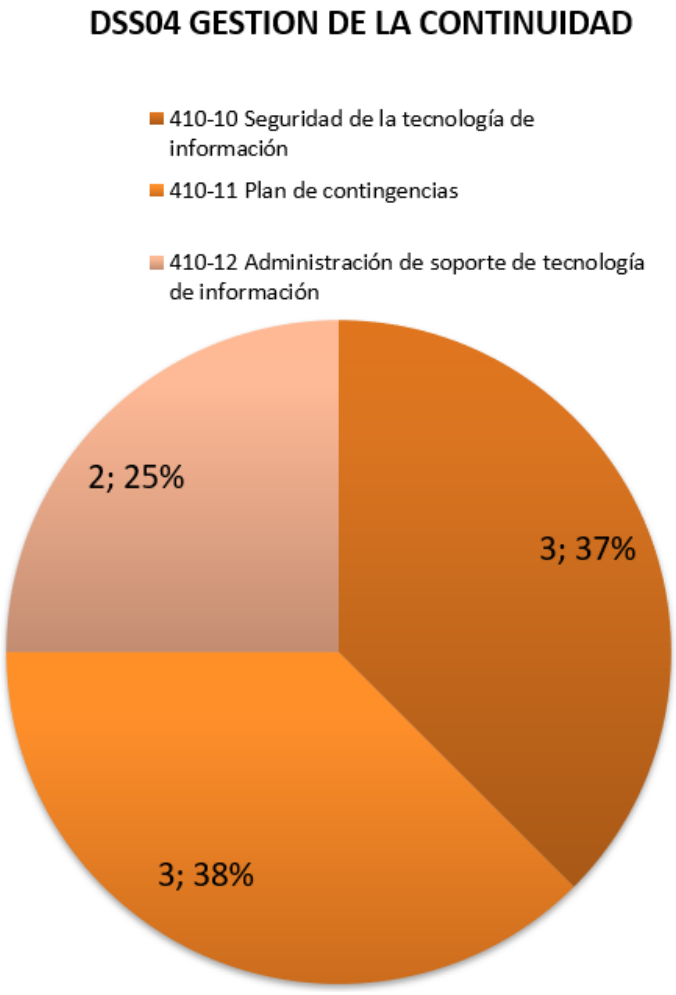
Anexo 1 Promedio APO13 gestión de la seguridad

NORMAS	APO13 GESTION DE LA SEGURIDAD
410-02 Segregación de funciones	1
Funciones y responsabilidades definidas para el personal de TI	
410-03 Plan informático estratégico de tecnología	2
Plan informático de TI alineados al plan estratégico institucional.	
Revisiones periódicas de control del plan estratégico y del plan operativo de la unidad deTI	
410-10 Seguridad de la tecnología de información	1
Ubicación adecuada y control de acceso físico a la unidad de tecnologías de información	
410-12 Administración de soporte de tecnología de información	4
Seguridad en los sistemas de la entidad de una identificación única a los usuarios	
Estandarizaciones de la identificación, autenticación y autorización de los usuarios	
Control periódico de las cuentas de usuario, procesos y administradores de los sistemas de TI	
Medidas de prevención y corrección que protejan a los sistemas institucionales de software malicioso y virus	



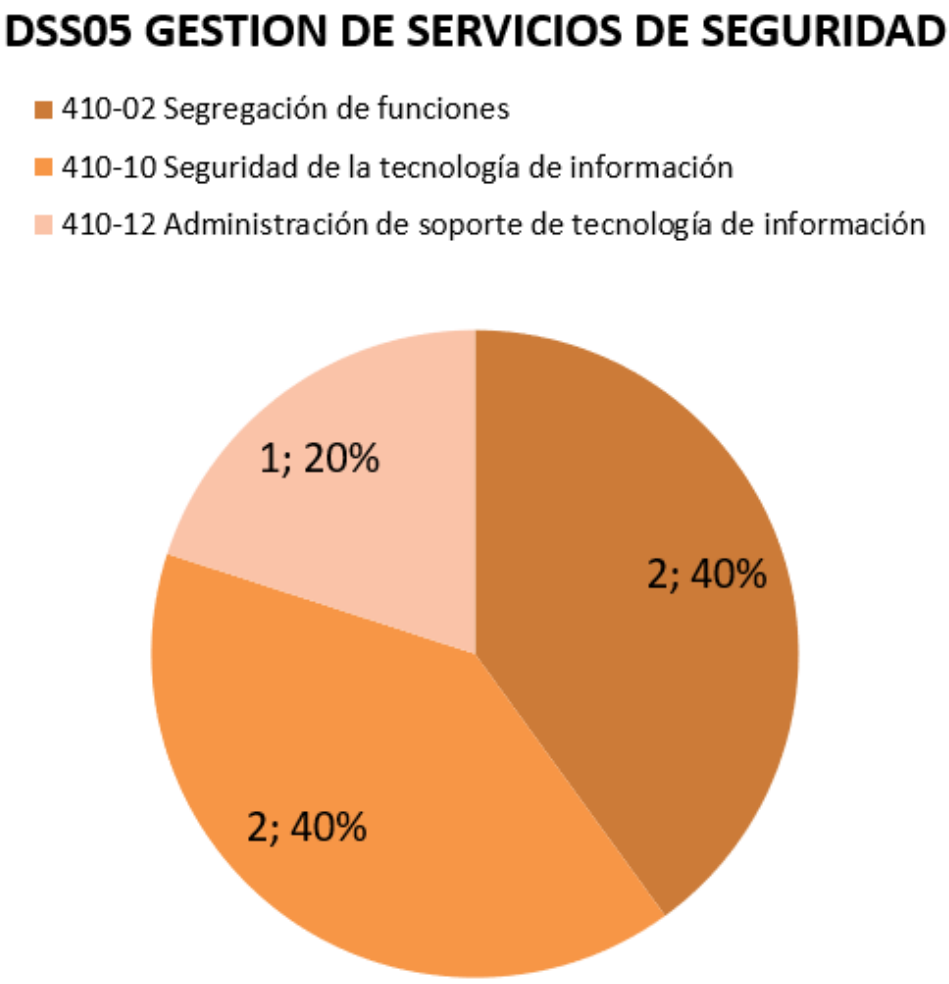
Anexo 2 Promedio DSS04 gestión de la continuidad

NORMAS	DSS04 GESTION DE LA CONTINUIDAD
410-10 Seguridad de la tecnología de información	
Funciones y responsabilidades definidas para el personal de TI Almacenamiento de la información críticaen lugares externos de la institución Existe un centro de procesamiento alternativo	3
410-11 Plan de contingencias	
Posee la unidad de TI implementando un plan de contingencias Plan de continuidad de operaciones que contemple la puesta en marcha de un centro de cómputo Plan de recuperación de desastres	3
410-12 Administración de soporte de tecnología de información	
Análisis de capacidad de los recursos tecnológicos Niveles de servicio y de operación para los servicios críticos de la institución	2



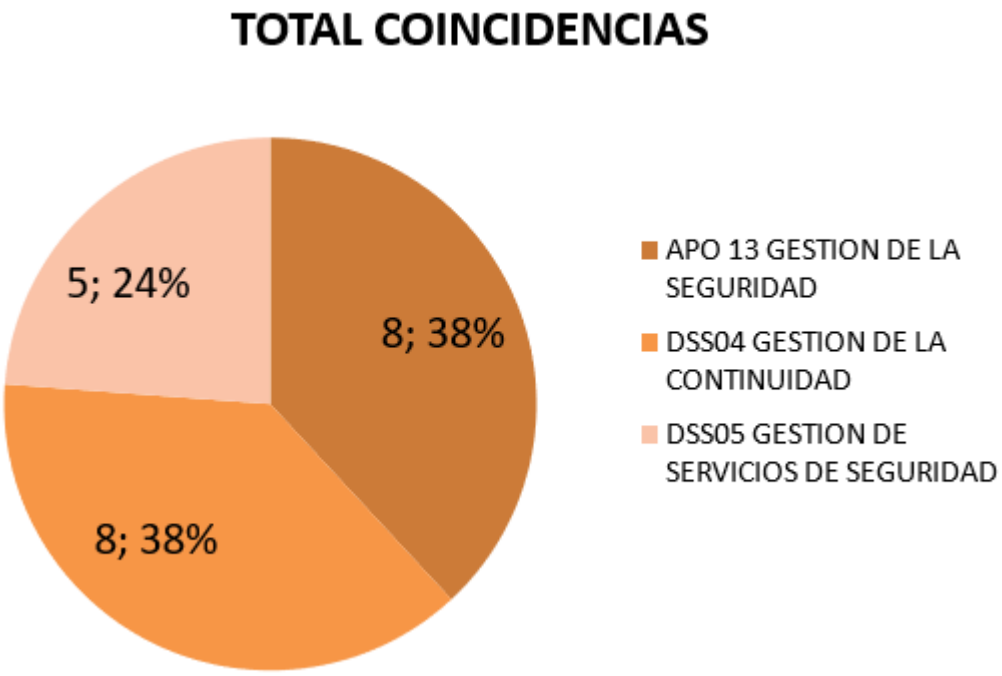
Anexo 3 Promedio DSS05 gestión de servicios de seguridad

NORMAS	DSS05 GESTION DE SERVICIOS DE SEGURIDAD
410-02 Segregación de funciones	
Funciones y responsabilidades definidas para el personal de TI	
Supervisión de los roles y funciones del personal de TI	2
410-10 Seguridad de la tecnología de información	
Implementación y administración de seguridades a nivel de software y hardware	2
Procedimientos de políticas que favorezcan la seguridad de la información	
410-12 Administración de soporte de tecnología de información	
Medidas de prevención y corrección que protejan a los sistemas institucionales de software malicioso y virus	1



Anexo 4 Total de coincidencias de cada proceso

PROCESOS	Nº COINCIDENCIAS
APO 13 GESTION DE LA SEGURIDAD	8
DSS04 GESTION DE LA CONTINUIDAD	8
DSS05 GESTION DE SERVICIOS DE SEGURIDAD	5



ANÁLISIS COMPARATIVO DE LA NORMA 410 DE CONTROL INTERNO DE LA CONTRALORÍA GENERAL DEL ESTADO CON COBIT5

INFORME DE ORIGINALIDAD

6%	6%	0%	0%
INDICE DE SIMILITUD	FUENTES DE INTERNET	PUBLICACIONES	TRABAJOS DEL ESTUDIANTE

FUENTES PRIMARIAS

1	m.isaca.org Fuente de Internet	2%
2	www.contraloria.ec-gov.net Fuente de Internet	1%
3	www.dnv.cl Fuente de Internet	1%
4	www.justiciaviva.org.pe Fuente de Internet	<1%
5	www.auditoria.gov.co Fuente de Internet	<1%
6	nic.odadata.eu Fuente de Internet	<1%
7	F.J. Pino. "Adaptation of the standards ISO/IEC 12207:2002 and ISO/IEC 15504:2003 for the assessment of the software processes in developing countries", IEEE Latin America	<1%

	Transactions, 4/2006 Publicación	
8	www.cinemania.co.cr Fuente de Internet	<1 %
9	contraloriagdeant.gov.co Fuente de Internet	<1 %
10	www.rediris.es Fuente de Internet	<1 %
11	www.cali.gov.co Fuente de Internet	<1 %
12	www.idesac.gov.co Fuente de Internet	<1 %
13	www.legal-protect.com Fuente de Internet	<1 %
14	www.gobatl.gov.co Fuente de Internet	<1 %
15	who.unep.ch Fuente de Internet	<1 %
16	www.socialistasdefuenlabrada.org Fuente de Internet	<1 %
17	www.madrimasd.org Fuente de Internet	<1 %
18	www.desarrolloweb.com Fuente de Internet	<1 %

19	www.cedelmc.com Fuente de Internet	<1%
20	www.mexder.com Fuente de Internet	<1%
21	revistas.ucp.edu.co Fuente de Internet	<1%
22	www.audisis.com Fuente de Internet	<1%
23	www.findeter.gov.co Fuente de Internet	<1%
24	bip.mideplan.cl Fuente de Internet	<1%
25	minfinanzas.ec-gov.net Fuente de Internet	<1%
26	www.ccc.uprh.edu Fuente de Internet	<1%
27	www.enba.sep.gob.mx Fuente de Internet	<1%
28	www.ieid.org Fuente de Internet	<1%
29	www.educadis.uson.mx Fuente de Internet	<1%
30	gestiondenegocios-peru.blogspot.com Fuente de Internet	<1%

31	www.javahispano.org Fuente de Internet	<1 %
32	www.donana.es Fuente de Internet	<1 %
33	www.empresa.org Fuente de Internet	<1 %
34	www.contraloriagen.gov.co Fuente de Internet	<1 %
35	www.almendron.com Fuente de Internet	<1 %
36	www.chiletech.cl Fuente de Internet	<1 %
37	www.wareprise.com Fuente de Internet	<1 %
38	www.isocio.com Fuente de Internet	<1 %
39	www.boliviagay.com Fuente de Internet	<1 %
40	bibliotecadigital.conevyt.org.mx Fuente de Internet	<1 %
41	www.acis.org.co Fuente de Internet	<1 %
42	www.conesup.net	

Fuente de Internet

<1%

43 www.iadb.org
Fuente de Internet
<1%

44 www.mastermagazine.info
Fuente de Internet
<1%

Excluir citas	Apagado	Excluir coincidencias	Apagado
Excluir bibliografía	Activo		

Universidad Católica de Cuenca

PERMISO DEL AUTOR DE TESIS PARA SUBIR AL REPOSITORIO INSTITUCIONAL

Yo, ROSALIA XIMENA CONTRERAS ABAD, portador (a) de la cédula de ciudadanía Nro. 0302205943. En calidad de autor/a y titular de los derechos patrimoniales del trabajo de titulación **"ANÁLISIS COMPARATIVO DE LA NORMA 410 DE CONTROL INTERNO DE LA CONTRALORÍA GENERAL DEL ESTADO CON COBIT 5"** de conformidad a lo establecido en el artículo 114 Código Orgánico de la Economía Social de Los Conocimientos, Creatividad e Innovación, reconozco a favor de la Universidad Católica de Cuenca una licencia gratuita, intransferible y no exclusiva para el uso no comercial de la obra, con fines estrictamente académicos, Así mismo; autorizo a la Universidad para que realice la publicación de éste trabajo de titulación en Repositorio Institucional de conformidad a lo dispuesto en el artículo 144 de la Ley Orgánica de Educación Superior.

Azogues, 07 de julio de 2020

F: .....

ROSALIA XIMENA CONTRERAS ABAD

0302205943

El Bibliotecario de la Sede Azogues

CERTIFICA:

Que: **CONTRERAS ABAD ROSALÍA XIMENA,** con cédula de ciudadanía Nro. **0302205943,** de la Carrera de: **INGENIERÍA EN SISTEMAS**

No adeuda libros, a esta fecha: **22 de junio del 2020**.

Byron Alonso Torres Romo

Bibliotecario

5 Siglas y Acrónimos

COBIT: objetivos de control para la información y la tecnología relacionada.

ISACA: Sistema de Información y de la Asociación de Control.

TI: Tecnologías De Información.

BCP: Plan de continuidad de negocio.

ISO: Organización Internacional de Estandarización.

TICS: Tecnología de Información y Comunicación.

SGSI: Sistema de Gestión de la Seguridad de la Información.

ITIL: Biblioteca de Infraestructuras de Tecnologías de Información.

OSSTMM: Manual de Metodología de Prueba de Seguridad de Código Abierto.

COSO: Comité de Organizaciones Patrocinadoras de Treadway.

CMI IT: Cuadro de Mando Integral de TI.

Benchmarking: Evaluación Comparativa.

6 Bibliografía

Auditool. (2020). La Comunicación y la Información, como componentes del Control Interno. Retrieved October 3, 2019, from https://www.auditool.org/blog/control-interno/292-la-comunicacion-y-la-informacion-como-componentes-del-control-interno

Byron Napoleón Cadena Oleas, & Irene García Rondón. (2016). El control interno para la gestión de tecnologías de la información. *Octubre 2016*. Retrieved from http://www.eumed.net/rev/caribe/2016/10/informacion.html

Calidad & Gestión. (2014). Ciclo Pdca - Estrategia Para La Mejora Continua. Retrieved September 30, 2019, from http://www.calidad-gestion.com.ar/boletin/58_ciclo_pdca_estrategia_para_mejora_continua.html

ClubEnsayos. (2012). IMPORTANCIA NORMAS COBIT - Ensayos y Trabajos - aurorita2012. Retrieved April 11, 2019, from https://www.clubensayos.com/Tecnología/IMPORTANCIA-NORMAS-COBIT/243243.html

Cobit. (2014). COBIT. Retrieved April 13, 2019, from http://implementaciondecobit.blogspot.com/p/antecedentes.html

Cobit. (2016). COBIT. Retrieved April 13, 2019, from http://implementaciondecobit.blogspot.com/p/blog-page.html

Contraloría general del estado. (2009). NORMAS DE CONTROL INTERNO DE LA CONTRALORIA GENERAL DEL ESTADO Estado: Vigente. Retrieved March 5, 2020, from https://www.oas.org/juridico/PDFs/mesicic5_ecu_ane_cge_12_nor_con_int_400_cge.pdf

Contraloría General Del Estado. (2016). Retrieved March 6, 2020, from https://www.contraloria.gob.ec/

Escuela de Administración Finanzas, e I. T. (2007). *Cobit Modelo para Auditoria y Control de Sistemas de Información*. *Consultorio Contable* (Vol. 1). Retrieved from http://www.eafit.edu.co/escuelas/administracion/consultorio-contable/Documents/boletines/auditoria-control/b13.pdf

Evolucion c. (2015). evolución de Cobit. Retrieved October 3, 2019, from https://chae201511700812108.wordpress.com/2015/05/24/evolucion-de-cobit/

Gallego Juan. (2020). Diferencias entre Cobit 4.1 Cobit 5 – Auditoria Informatica- Juan David gallego. Retrieved October 3, 2019, from https://chaui201711701121665.wordpress.com/2017/06/08/diferencias-entre-cobit-4-1-cobit-5/

García, Y. C. (2015). Modelo de Gestión de la Seguridad de Información en los procesos críticos de las áreas financieras universitarias. Caso PUCE, 132. Retrieved from http://bibdigital.epn.edu.ec/bitstream/15000/10537/1/CD-6237.pdf&usg=AFQjCNFimEroi2VMQGm9e480XENIf_U9cA

Gomez, A. I. A. (2016). *Tabla de Contenido*. *Investigación & Desarrollo*. https://doi.org/10.14482/i&d.v23i2.8303

Institute, G. (2007). *COBIT 4.1 Spanish*. Retrieved from www.itgi.org

ISACA. (2012). *Procesos Catalizadores: Usando COBIT5*.

ISACA principios. (2012). *Un Marco de Negocio para el Gobierno y la Gestión de la Empresa*. Retrieved from http://linkd.in/ISACAOfficial

ISO. (2019). ISO 27001. Aspectos claves y relación con las normas ISO 22301 e ISO/IEC 20000. Retrieved September 25, 2019, from https://www.pmg-ssi.com/2019/08/iso-27001-aspectos-claves-y-relacion-con-las-normas-iso-22301-e-iso-iec-20000/

Johanna Cárdenas Solano, L., Eduardo Becerra Ardila, L., & Ernesto Martinez Ardila, H. (2013). GESTIÓN DE LA SEGURIDAD DE LA INFORMACIÓN (pp. 1–21). Mexico. Retrieved from http://congreso.investiga.fca.unam.mx/docs/xviii/docs/2.04.pdf

Katiuska Espinoza. (2017). *normativa gubernamental*. Escuela Politecnica Ncional.

Leonel, B. C., & Cuzme. (2017). *Diseño de políticas de seguridad de la información basado en el marco de referencia COBIT 5 EN EL MARCO DE REFERENCIA COBIT 5 FRAMEWORK Cuzme Fabián1 , Suárez Luis1 , Bracho Cristian1 y Pupiales Carlos1 1 Carrera de Ingeniería en Electrónica y Redes de Co*. UniversidadTecnica del Norte. Retrieved from https://www.researchgate.net/publication/318509533_Diseno_de_politicas_de_seguridad_de_la_informacion_basado_en_el_marco_de_referencia_COBIT_5

Lisot. (2018). ¿Qué es un sistema de Gestión de la Seguridad de la información (SGSI)? Retrieved September 30, 2019, from https://www.lisot.com/que-es-un-sistema-de-gestion-de-la-seguridad-de-la-informacion-sgsi/

Miguel Angel Mendoza. (2015). COBIT para la seguridad en las organizaciones | WeLiveSecurity. Retrieved September 25, 2019, from https://www.welivesecurity.com/la-es/2015/08/04/practicas-cobit-seguridad-organizaciones/

Olivares Rojas, J. C. (2009). *Seguridad de la Información en general*. Universidad del Bío-Bío. Retrieved from http://ceur-ws.org/Vol-488/paper13.pdf

QAEC. (2019). COSO. Retrieved August 20, 2019, from https://www.aec.es/web/guest/centro-conocimiento/coso

ROSA ANDREA REA LOZADA. (2012). *"NORMAS DE CONTROL INTERNO EMITIDAS POR LA CONTRALORÍA GENERAL DEL ESTADO, APLICADAS A LA DIRECCIÓN DE TECNOLOGÍAS DE INFORMACIÓN DEL ILUSTRE MUNICIPIO DE IBARRA" AUTORA: ROSA ANDREA REA LOZADA*. UNIVERSIDAD TÉCNICA DEL NORTE, Ibarra.

Sanches, J. C. M. (2007). *COBIT ® e ITIL ®. Service Management*. Retrieved from https://prezi.com/uf4bi6hwtpyg/21-definicion-y-antecedentes-cobit-e-itil/

Servin, L. (2018). Por qué es importante el control interno en las empresas. Retrieved October 3, 2019, from https://www2.deloitte.com/py/es/pages/audit/articles/opinion-control-interno-empresas.html%0Ahttps://www2.deloitte.com/py/es/pages/audit/articles/opinion-control-interno-empresas.html#

SGSI. (2019). SGSI. Retrieved September 30, 2019, from http://www.iso27000.es/page7.html

universidad de Jaén. (n.d.). metodologia cualitativa. Retrieved March 5, 2020, from

http://www.ujaen.es/investiga/tics_tfg/enfo_cuali.html