UNIVERSIDAD TÉCNICA DE AMBATO

FACULTAD DE INGENIERÍA EN SISTEMAS, ELECTRÓNICA E INDUSTRIAL

CARRERA DE INGENIERÍA EN SISTEMAS COMPUTACIONALES E INFORMÁTICOS

Tema:

AUDITORIA INFORMÁTICA APLICANDO LA METODOLOGÍA COBIT 5.0 AL PROCESO DE RECAUDACIÓN DEL MODULO DE TESORERIA DEL SISTEMA CABILDO EN EL DEPARTAMENTO FINANCIERO DEL GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPALIDAD DE AMBATO

Trabajo de Graduación. Modalidad: Proyecto de Investigación, presentado previo la obtención del título de Ingeniero en Sistemas Computacionales e Informáticos.

SUBLÍNEA DE INVESTIGACIÓN: Administración de recursos

AUTOR: Carlos Andrés Ruíz López

TUTOR: Ing. Dennis Chicaiza, Mg.

Ambato – Ecuador

Enero 2020

APROBACIÓN DEL TUTOR

En mi calidad de tutor del Trabajo de Investigación sobre el tema: "AUDITORIA INFORMÁTICA APLICANDO LA METODOLOGÍA COBIT 5.0 AL PROCESO DE RECAUDACIÓN DEL MODULO DE TESORERIA DEL SISTEMA CABILDO EN EL DEPARTAMENTO FINANCIERO DEL GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPALIDAD DE AMBATO", del señor Ruíz López Carlos Andrés, estudiante de la Carrera de Ingeniería en Sistemas Computacionales e Informáticos, de la Facultad de Ingeniería en Sistemas, Electrónica e Industrial, de la Universidad Técnica de Ambato, considero que el informe investigativo reúne los requisitos suficientes para que continúe con los tramites y consiguiente aprobación de conformidad con el numeral 7.2 de los Lineamientos Generales para la aplicación de Instructivos de las Modalidades de Titulación de las Facultades de la Universidad Técnica de Ambato.

Ambato, enero de 2020

EL TUTOR

Ing. Dennis Chicaiza, Mg.

AUTORÍA

El presente trabajo de investigación titulado: "**AUDITORIA INFORMÁTICA APLICANDO LA METODOLOGÍA COBIT 5.0 AL PROCESO DE RECAUDACIÓN DEL MODULO DE TESORERIA DEL SISTEMA CABILDO EN EL DEPARTAMENTO FINANCIERO DEL GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPALIDAD DE AMBATO".**

Es absolutamente original, auténtico y personal, en tal virtud, el contenido, efectos legales y académicos que se desprenden del mismo son de exclusiva responsabilidad del autor.

Ambato, enero de 2020

Carlos Andrés Ruíz López

CC: 1804435210

DERECHOS DE AUTOR

Autorizo a la Universidad Técnica de Ambato, para que haga uso de este Trabajo de Titulación como un documento disponible para la lectura, consulta y procesos de investigación.

Cedo los derechos de mi Trabajo de Titulación, con fines de difusión pública, además autorizo su reproducción dentro de las regulaciones de la Universidad.

Ambato, enero de 2020

Carlos Andrés Ruíz López

CC: 1804435210

APROBACIÓN DEL TRIBUNAL DE GRADO

La Comisión Calificadora del presente trabajo conformada por los señores docentes Ing, Mg. Franklin Mayorga e Ing. PhD. Víctor Guachimbosa, revisó y aprobó el Informe Final del Proyecto de Investigación titulado "AUDITORIA INFORMÁTICA APLICANDO LA METODOLOGÍA COBIT 5.0 AL PROCESO DE RECAUDACIÓN DEL MODULO DE TESORERIA DEL SISTEMA CABILDO EN EL DEPARTAMENTO FINANCIERO DEL GOBIERNO AUTÓNOMO DESCENTRALIZADO MUNICIPALIDAD DE AMBATO", presentado por el señor Ruíz López Carlos Andrés, de acuerdo al numeral 9.1 de los Lineamientos Generales para la aplicación de Instructivos de las Modalidades de Titulación de las Facultades dela Universidad Técnica de Ambato

---

Ing. Elsa Pilar Urrutia Mg.

PRESIDENTA ENCARGADA DEL TRIBUNAL

Ing. Franklin Mayorga, Mg.

DOCENTE CALIFICADOR

Ing. Víctor Guachimbosa, PhD.

DOCENTE CALIFICADOR

DEDICATORIA

Primeramente, a Dios por darme los conocimientos y la fuerza para poder cumplir mis metas.

A mi madre por su sacrificio y esfuerzo, por siempre velar por mi educación y mi bienestar a lo largo de mi vida, por ser una persona incondicional y excepcional.

A mi padre Galo por todos los buenos momentos que me ofreció en mi niñez.

A mi tío Walter que siempre me ha inculcado valores y que me ha enseñado que un título no debe cambiar a una persona.

A mis primos Santiago, Darío y Gabriel por ser como mis hermanos, por enseñarme que con dedicación todo se puede cumplir.

A Byron Barreno por demostrarme un apoyo incondicional a lo largo de esta etapa.

AGRADECIMIENTO

Agradezco primeramente a Dios por brindarme la inteligencia, humildad y sabiduría necesaria para poder continuar con todas las metas que se me presentan.

A mi madre por ser el motor fundamental en mi vida, ya que sin ella nada hubiese sido posible.

A mi padre que a pesar de la distancia lo tengo siempre presente.

A mis primos y tío por estar en las buenas y en las malas, por motivarme a continuar y no rendirme.

A mi amigo Byron Barreno por brindarme la mano cuando lo he necesitado.

A mis profesores por todos los conocimientos impartidos a lo largo de la carrera ya que gracias a sus conocimientos he sabido llegar hasta el final.

ÍNDICE GENERAL DE CONTENIDOS

ÍNDICE DE TABLAS

ÍNDICE DE FIGURAS

RESUMEN EJECUTIVO

El presente trabajo de investigación se realizó con el fin de auditar al sistema Cabildo del Gobierno Autónomo Descentralizado Municipal de Ambato, al cual no se ha realizado una auditoria informática en años anteriores, el beneficio de dicha auditoria es encontrar posibles inconvenientes en el departamento de Tecnologías de la Información (TI), dicho sistema es el encargado de la recaudación de bienes financieros en la ciudad de Ambato. Con lo cual se espera aportar con nuevas ideas que proporcionen un mejor servicio a los interesados de la ciudad de Ambato.

La metodología empleada fue Cobit 5.0 la cual se utilizó para poder evaluar y encontrar las falencias en el sistema Cabildo y en las áreas con las que trabaja dicho sistema, el trabajo principalmente se basó en los cinco principios de dicha metodología, los cuales ayudaran a mantener un manejo óptimo de la información. Se realizaron pruebas las cuales fueron divididas por áreas, después dichas pruebas fueron separadas por principios dependiendo las características que cumplan.

De acuerdo con el análisis obtenido mediante las pruebas generadas se pudo presenciar las debilidades del sistema Cabildo. Una de las debilidades más visibles fue la carencia de documentación del sistema, la cual es de vital importancia en la institución, por lo cual se presentaron recomendaciones las cuales ayudarán a mantener la integridad de la información.

Para el Gobierno Autónomo Descentralizado Municipal de Ambato la elaboración de una auditoria informática basada en la metodología Cobit será de gran ayuda ya que se podrá comprobar los procesos y documentación existentes que son manejado en el departamento de Tecnologías de la Información (TI).

ABSTRACT

He present research work was carried out in order to audit the Cabildo system of the Government of Ambato, which a computer audit has not been carried out in previous years, the benefit of this audit is to find the possible inconveniences in the Information Technology department (IT), also the system is responsible for the collection of financial assets in the city. That is expected with new ideas that provide a better service to those interested in Ambato.

The methodology used was Cobit, it was used to be able to evaluate and find the flaws in the Cabildo system and in the areas with which the system works, the labor was mainly based on the five principles of said methodology, which will help to maintain a management; Optimal information. Tests were performed, they were divided by areas, then tests were separated by principles depending on the characteristics they meet.

According to the analysis obtained through the tests generated, the weaknesses of the Cabildo system could be seen. One of the most visible weaknesses was the lack of documentation of the system, recommendations were presented which will help maintain the integrity of the information.

For the Autonomous Municipal Decentralized Government of Ambato the elaboration of a computer audit based on the Cobit methodology will be of great help since it will be possible to check the existing processes and documentation that are managed in the Information Technology (IT) department

CAPÍTULO I.- MARCO TEÓRICO

1.1 Antecedentes Investigativos

En el Gobierno Autónomo Descentralizado Municipalidad de Ambato cuenta con el sistema Cabildo el que es encargado del manejo de la información financiera de la ciudad de Ambato.

El Sistema Cabildo está conformado por un total de 1156 usuarios, divididos en diferentes módulos y cada módulo consta de diferentes funcionarios y roles, los cuales serán asignados dependiendo su cargo.

El sistema Cabildo trabaja con una base de Datos llamada Oracle, la cual es la encargada de guardar la información de todos los funcionarios y clientes de la ciudad de Ambato.

En la Universidad Politécnica de Valencia, Alberto Hervalejo Sánchez en su proyecto "Auditorías de Seguridad Informática y la OSSTMM"en el año 2009. Menciona, "Nunca se podrá crear y proteger la información que tengamos, siempre existirá atacantes y nuevas herramientas que ayuden a vulnerar la seguridad, ayudando a que los sistemas se vuelvan más sencillos al momento de generar ataques".

El proyecto realizado se centra en la Auditoría de Seguridad Informática (en especial, vulnerabilidades y test de intrusión), tomando como referencia, la metodología descrita por el Instituto para la Seguridad y Metodologías Abiertas (Institute for Security and Open Methodologies-ISECOM), la "Open Source Security Testing Methodology Manual" (OSSTMM). Teniendo en cuenta, que ésta es, quizás la metodología más extendida en el campo y ofrece métodos científicos a los tests de seguridad, pero, además, ofrece una guía a los auditores para realizar una auditoría OSSTMM certificada" **[1]**.

Según el trabajo realizado en la Universidad Técnica de Ambato, en la Facultad de Ingeniería en Sistemas Electrónica e Industrial en la tesis "Auditoria Informática para los departamentos Financiero, Tesorería, Proveeduría, Agencia Norte y agencia Sur de la Empresa municipal de agua potable y Alcantarillado de Ambato" de Maritza Andrea Espinoza Apráez, afirma haber realizado una Auditoria Informática, en la cual trata de buscar una solución a los ataques generados en la parte de Hardware y Software realizados por terceras personas **[2]**.

En la Escuela Politécnica del Litoral, Gabriela Hernández en su proyecto "Diseño de un Plan Estratégico de Seguridad de Información en una Empresa del Sector Comercial" en el año 2006. Plantea un diseño de un Plan de Seguridad Informática para poder tener sus activos seguros, los cuales beneficiaran a cumplir los procesos y objetivos de forma eficaz.

Recomienda utilizar políticas de seguridad basadas en estándares o normas los cuales se podrán implementar en el área de sistemas, beneficiando a la seguridad informática de la empresa **[3]**.

En la Universidad de las Fuerzas Armadas ESPE, Jiménez Cuestas Ana Lucía en su trabajo de titulación "Auditoria Informática del Sistema de Información de la empresa Cocinas Internacionales utilización Cobit v5", en el 2016; menciona que mediante la aplicación de la Auditoria Informática utilizando la metodología Cobit v5, verifico la carencia de un gobierno de Tecnologías de la información y de controles los cuales permiten garantizar la seguridad de la información **[4]**.

En la Universidad Nacional de Chimborazo UNACH, Patricia Alexandra Badillo Pinto en su proyecto "Guía de implementación de Tecnologías de la Información aplicando Cobit en Auditorias de entidades financieras, para disminuir errores procedimentales", en el 2016; menciona que mediante el uso del marco de trabajo Cobit 5 se logró entender el estado actual de la Cooperativa de Ahorro y Crédito Nueva Esperanza, además se pudo identificar los procesos necesarios para el manejo adecuado del Departamento de Sistemas **[5]**.

1.2. Objetivos y descripción del cumplimiento de objetivos

OBJETIVO GENERAL

Realizar una Auditoria Informática aplicando la metodología Cobit 5.0 al proceso de Recaudación del módulo de Tesorería del sistema Cabildo en el departamento Financiero del Gobierno Autónomo Descentralizado Municipalidad de Ambato en el periodo del año 2018.

OBJETIVOS ESPECÍFICOS:

1) Evaluar la situación actual del sistema informático Cabildo del GAD de Ambato, principalmente enfocándose en la realidad de Tecnologías de la Información en el Departamento Financiero en el Área de Tesorería.
2) Aplicar los estándares COBIT en la evaluación y auditoría del sistema Cabildo del Gobierno Autónomo Descentralizado Municipal de Ambato y presentar sus resultados al Departamento Financiero en el Área de Tesorería.
3) Proponer un plan de mejores prácticas para obtener una mayor integridad, confidencialidad y confiabilidad de la información, en los procesos del sistema Cabildo del Gobierno Autónomo Descentralizado Municipal de Ambato.

En lo que se refiere al cumplimiento del objetivo general se puede manifestar que se logró cumplir con totalidad, gracias al estudio e implementación de la metodología Cobit 5.0 en especial con la ejecución de los principios Cobit en el sistema Cabildo del Gobierno Autónomo Descentralizado Municipalidad de Ambato.

Lo que se refiere a los objetivos específicos se han realizado satisfactoriamente, al evaluar la situación actual del sistema Cabildo del Gobierno Autónomo Descentralizado Municipalidad de Ambato, con la ejecución de la metodología Cobit 5.0 principalmente con el manejo de los principios Cobit.

Posteriormente se sugirió la creación de políticas las cuales ayuden al manejo adecuado del sistema Cabildo y del departamento de Tecnologías de la Información (TI).

CAPÍTULO II.- METODOLOGÍA

2.1 Materiales

2.1.1 Humanos

- Docente Tutor del Proyecto
- Autor del Proyecto.

2.1.2 Institucionales

- GAD del Municipio de Ambato.
- Biblioteca Física.
- Biblioteca Digital.
- Repositorio Institucional.

2.1.3 Otros

No.	Detalle	Unidad	Cantidad	Valor Unitario	Valor Total
1	Internet	Horas	200	$ 0.80	160
2	Carpetas	c/u	3	$ 1.00	3
3	Cuaderno	c/u	2	$ 1.50	3
4	Copias	c/u	60	$ 0.03	1.80
5	Lápices	c/u	2	$ 0.60	1.20
6	Esferos	c/u	3	$ 0.75	2.25
7	Borrador	c/u	1	$ 0.30	0.30
8	Laptop	c/u	1	$ 800	800
9	Transporte	Semanal	25	$ 25	500
				Subtotal	1471.55
				Imprevisto (10%)	147.155
				Total	1618.705

2.2 Métodos

2.2.1 Sistemas de Información

Conjunto de elementos que interactúan entre sí, para que la información siempre este disponible para cumplir con los objetivos de la institución.

Un Sistema de Información realiza cuatro actividades básicas:

- Entrada de información: proceso en el cual el sistema toma los datos que requiere.
- Almacenamiento de información: pude hacerse por computadora o archivos físicos para conservar la información.
- Procesamiento de la información: permite la transformación de los datos fuente en información que puede ser utilizada para la toma de decisiones
- Salida de información: es la capacidad del sistema para producir la información procesada o sacar los datos de entrada al exterior **[6]**.

2.2.2 Seguridad informática

La seguridad informática es una disciplina que se enfoca en la protección de la información, la cual puede estar almacenada en la nube o en nuestros ordenadores.

Un sistema informático puede ser protegido desde un punto de vista lógico (con el desarrollo de software) o físico (vinculado al mantenimiento eléctrico, por ejemplo). Por otra parte, las amenazas pueden proceder desde programas dañinos que se instalan en la computadora del usuario (como un virus) o llegar por vía remota (los delincuentes que se conectan a Internet e ingresan a distintos sistemas) **[7].**

Para que un sistema se pueda definir como seguro debe tener cuatro características; como se muestra en la Tabla 1.

Tabla 1. Características de la Seguridad Informática

Característica	Descripción
Integridad	Los activos o la información solo pueden ser modificados por las personas autorizadas y de la forma autorizada.
Confidencialidad	La información o los activos informáticos son accedidos solo por las personas autorizadas para hacerlo.
Disponibilidad	Los activos informáticos son accedidos por las personas autorizadas en el momento requerido.
Irrefutabilidad (No repudio)	El uso y/o modificación de la información por parte de un usuario debe ser irrefutable, es decir, que el usuario no puede negar dicha acción.

Fuente: Elaboración propia a partir de [8]

2.2.3 Auditoria

Es el proceso por el cual un profesional trata de conocer la situación actual de la empresa. La actividad del auditor es realizar un examen exhaustivo de las actividades y de los procesos que son fijado por las leyes.

Las auditorias son confidenciales y al finalizar la persona encargada de la auditoria debe presentar un informe detallado sobre las cosas que se examinó, el diagnostico jurídico, sugerencias las que permitan a la empresa seguir evolucionando y cumpliendo los objetivos planteados **[9]**.

2.2.3.1 Tipos de Auditorias

La auditoría ha evolucionado en los últimos años dando lugar a auditar varias especialidades.

Existen varios tipos de auditorías las cuales se pueden clasificar dependiendo el tipo de área que se quiera examinar; cómo se puede observar en la Tabla 2.

Tabla 2. Tipos de Auditorias

Tipos de Auditorias	Descripción
Auditoria Financiera (Contable)	Examina de manera clara y concreta la aplicación de los registros contables y operaciones financieras, el propósito de esta auditoria es generar un dictamen concreto de los resultados financieros, los cuales serán emitidos por un profesional en un tiempo determinado.
Auditoria Administrativa	Revisa de manera exhaustiva y sistematizada la actividad de una entidad, al igual que el cumplimiento de funciones y actividades que regulen las operaciones, procedimientos, métodos y técnicas establecidas por la empresa.
Auditoria Operacional	Es una evaluación de la empresa orientada al futuro, con fines de mejorar la eficacia, suficiencia y el correcto desempeño de sus operaciones basada en los recursos disponibles de la empresa, como son lineamientos, normas, políticas.
Auditoria Integral	Se encarga de auditar de manera global todas las funciones, actividades y operaciones de todas las áreas que conforman una empresa. Para el desarrollo de esta auditoria pueden intervenir profesionales de varias especialidades.
Auditoria Gubernamental	Es la encargada de controlar que todas las gestiones públicas se hayan realizado de manera eficiente, económica y transparente
Auditoria de Sistemas	Es la revisión y evaluación de controles en los sistemas informáticos, con el fin de verificar si el sistema cumple con las necesidades de la empresa.

Fuente: Elaboración propia a partir de [10]

2.2.4 Auditoria Informática

La Auditoria informática es un proceso exhaustivo el que es ejecutado por profesionales, los cuales tratan de verificar y asegurar que los procedimientos y políticas de las Tecnologías de la Información se cumplan de manera segura y oportuna.

Auditoria Informática el proceso de recolectar, evaluar y agrupar la información de un sistema, para determinar si se mantiene la integridad de los datos, llevando a cabo eficazmente los fines de la organización y utilizando eficientemente los recursos **[11]**.

2.2.4.1 Tipos de Auditoria Informática

Existen varios tipos de auditorías informáticas, entre las cuales tenemos los siguientes tipos; cómo se puede apreciar en la Tabla 3.

Tabla 3. Tipos de Auditoria Informática

Auditoria	**Descripción**	**Revisión**
Auditoria Informática de Sistemas	Se encarga del análisis de las actividades a las cuales se las conoce como Técnicas de Sistemas.	-Sistemas operativos. -Software básico. -Administración de base de datos.
Auditoria Informática de Explotación	Encargada de generar resultados informáticos de varios tipos como: impresos, ficheros soportados, ordenes automatizadas para la creación o modificación de procesos industriales, listados, etc.	- Controlar los manuales de instrucciones y procedimientos de explotación. - Verificar la continuidad del proceso. - Realizar controles sobre la explotación remota. -Verificar los procedimientos que impidan que puedan correrse versiones de programas no activos.
Auditoria Informática de Comunicaciones	Consiste en la recolección y agrupación de información de las redes informáticas, para poder evaluar el estado actual y	- Redes locales -Estructura física/hardware

	desempeño de la red, el cual ayudara a salvaguardar los activos de la empresa.	-Estructura lógica/software del sistema.
Auditoria Informática de Desarrollos de Proyectos	Se encarga en planificar y realizar auditorías a aplicaciones que se encuentran en funcionamiento, el objetivo principal de esta auditoria es saber si cumplen con objetivos para los que fueron creados.	-Satisfacción de usuarios. -Revisión de metodologías empleadas. -Control interno de las aplicaciones. - Control de procesos y ejecución de programas críticos **[13]**.
Auditoria Informática de Seguridad	Abarca dos conceptos: seguridad física la que se encarga de la parte de hardware, e infraestructura y seguridad lógica la que se encarga del parte del software, protección de datos y acceso de los usuarios.	Seguridad Física -Hardware -Infraestructura -Sistemas de Seguridad Seguridad Lógica -Software -Servidores - Conexiones VPN

Fuente: Elaboración propia a partir de [12] y **[13]**.

2.2.4.2 Objetivos de una Auditoria Informática

- Mejorar la relación coste-beneficio de los sistemas de información.
- Incrementar la satisfacción y seguridad de los usuarios de dichos sistemas informatizados.
- Garantizar la confidencialidad e integridad a través de sistemas de seguridad y control profesionales.
- Minimizar la existencia de riesgos, tales como virus o hackers, por ejemplo.
- Optimizar y agilizar la toma de decisiones.
- Educar sobre el control de los sistemas de información, puesto que se trata de un sector muy cambiante y relativamente nuevo, por lo que es preciso educar a los usuarios de estos procesos informatizados **[14]**.

2.2.4.3 Beneficios de la auditoria

- Te da información sobre cómo funciona la empresa

- Tiene en cuenta temas legales
- Estudia aspectos clave como la seguridad
- Te ayuda a valorar los riesgos TI
- Da soluciones concretas de rentabilidad en el trabajo.
- Da consejos sobre una utilización más eficiente de los recursos.
- Te permite poner en marcha mecanismos de protección ante los riesgos derivados del uso de las nuevas tecnologías
- Mejora las relaciones entre departamentos, al proponer sinergias en cuestiones informáticas para hacer más rentable la comunicación entre diferentes trabajadores **[15]**.

2.2.5 Metodología Cobit

COBIT 5 "Control objectives for information and related technology" es una metodología basada en el manejo de buenas prácticas, la cual ayuda a llevar un control adecuado de la información, el beneficio de dicha metodología es tratar de alcanzar un nivel óptimo en las Tecnologías de la Información.

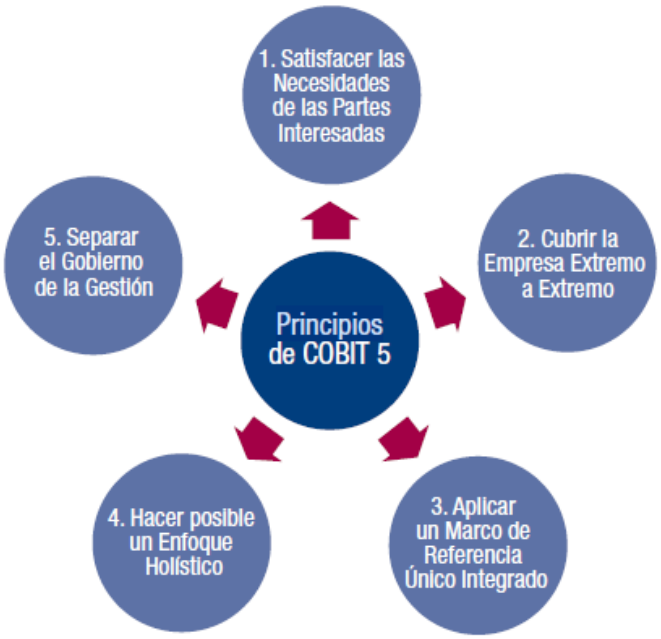
COBIT se puede aplicar a los sistemas de información de toda la empresa, incluyendo computadores y redes.

2.2.5.1 Principios de Cobit 5.0

Los principios Cobit tratan de beneficiar a la empresa sin importar su ubicación ni tamaño, el objetivo de la utilización de los cinco principios de Cobit 5.0 es tratar de tomar mejores decisiones e inversiones las cuales estarán relacionadas con las Tecnologías de la Información (TI).

En la siguiente Figura 1 se constará los cinco principios Cobit 5.0 así como también se evidencia en la Tabla 4 detalladamente.

Figura 1. Principios Cobit 5.0



Fuente: **[17]**

Tabla 4. Principios Cobit 5.0

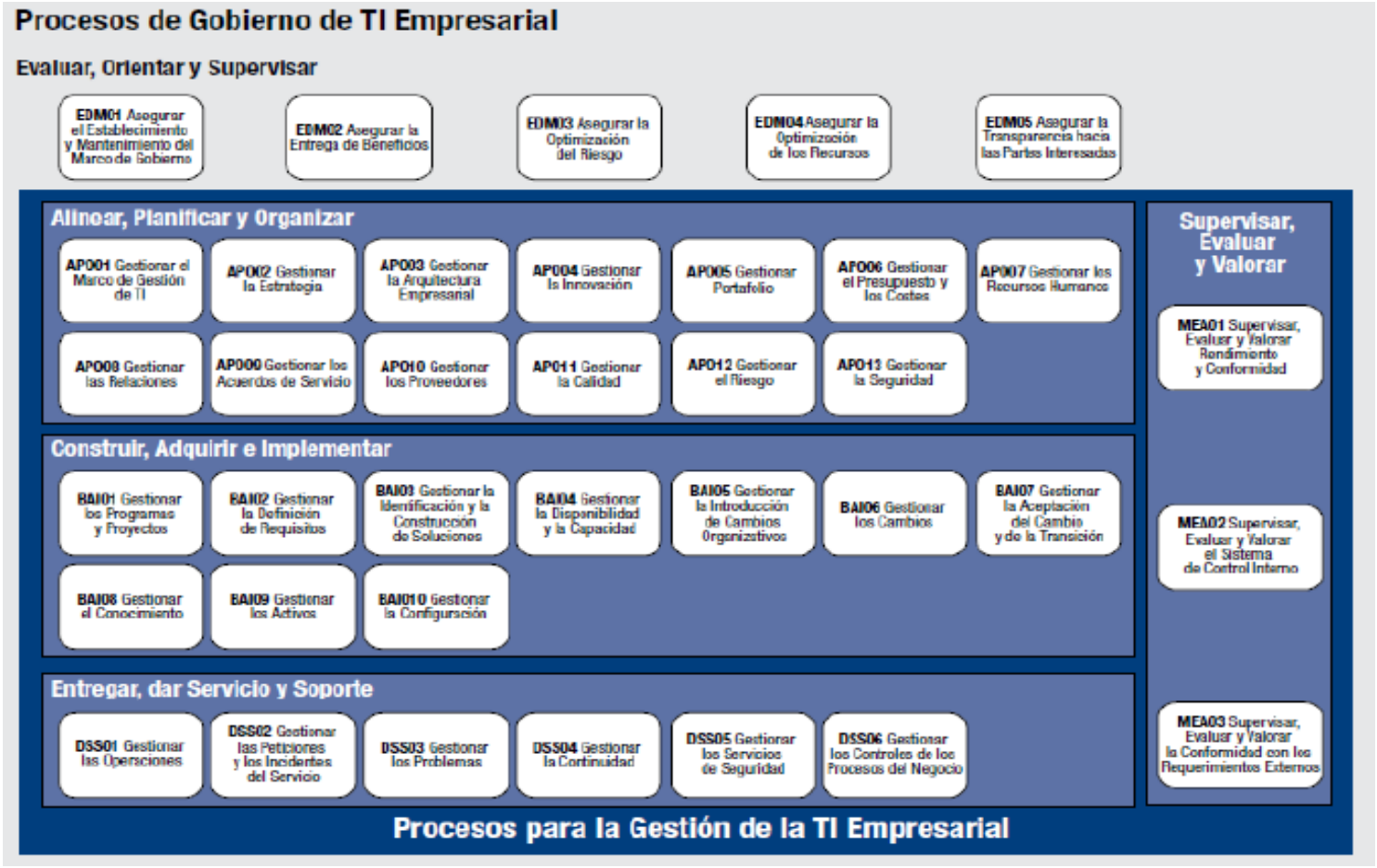
Principios COBIT	
1) Satisfacer las necesidades de las partes interesadas.	Trata de satisfacer las necesidades de todas las partes interesadas, en este caso las partes interesadas serán externas e internas. Las partes externas pueden ser clientes, contraloría, proveedores, sociedad en general. Las partes internas pueden ser los responsables de TI, auditores internos, administración de gobierno.
2) Cubrir la Empresa Extremo a Extremo.	Este principio se encarga de cubrir las funciones y procesos de toda la empresa, para el cumplimiento de ella se toma en cuenta a partes externas e internas, las cuales deberán cumplir actividades, roles y relaciones.

Principios COBIT	
3) Aplicar un Marco de Referencia Único Integrado.	Trata de verificar si en la empresa existen estándares o normativas que ayuden a cumplir los objetivos de mejor manera.
4) Hacer posible un Enfoque Holistico.	Se basa en siete catalizadores, los cuales ayudaran a que se consigan las metas de las empresas. Los siete catalizadores son: "-Principios, Políticas Y Marco de Trabajo. – Procesos – Estructuras Organizativas – Cultura, Ética y Comportamiento – Información – Servicios, Infraestructuras y Aplicaciones – Personas, Habilidades y Competencias" **[18]**.
5) Separar el Gobierno de la Gestión.	Trata de separar el Gobierno y la gestión, debido a que el gobierno se encarga de satisfacer a las partes interesadas, basándose en las condiciones y necesidades, mientras que la gestión trata de planificar y de gestionar que se cumplan las actividades establecidas las cuales son analizadas por un cuerpo de gobierno; así como se muestra en la Figura 2 y las cuales será detalladas en la Tabla 5,6,7,8 y Tabla9. El Gobierno consta con cinco procesos los cuales son evaluación, orientación y supervisión (EDM). La Gestión cuenta con cuatro dominios. – "Alinear, Planificar y Organizar (Align, Plan and Organise, APO) – Construir, Adquirir e Implementar (Build, Acquire and Implement, BAI)

	– Entregar, dar Servicio y Soporte (Deliver, Service and Support, DSS) – Supervisar, Evaluar y Valorar (Monitor, Evaluate and Assess, MEA)”**[18]**.

Fuente: Elaboración propia a partir de la Figura 1. Principios Cobit 5.0 [17] y [18]

Figura 2. Procesos de Gobierno de TI Empresarial



Fuente: [18]

Tabla 5. Procesos de Evaluación, Orientación y Supervisión (EDM)

Procesos para el Gobierno de la TI Empresarial	
Dominio de Gobierno	**Evaluar, Orientar y Supervisar (EDM):** Asegura que los objetivos planteados de la empresa sean cumplidos, estimando las necesidades de los interesados.
Procesos	
EDM01. Asegurar el establecimiento y mantenimiento del marco de referencia de gobierno: Analizar y articular los requerimientos para el gobierno de las TI de la empresa y pone en marcha y mantiene efectivas las estructuras, procesos y prácticas facilitadoras, con claridad de las responsabilidades y la autoridad para alcanzar la misión, las metas y objetivos de la empresa.	
EDM02. Asegurar la entrega de beneficios: Optimizar la contribución al valor del negocio desde los procesos de negocios, los de servicios TI y activos de las TI resultado de la inversión hecha por TI a unos costos aceptables.	
EDM03. Asegurar la optimización del riesgo: Asegurar que el apetito y la tolerancia al riesgo de la empresa son entendidos, articulados y comunicados y que el riesgo para el valor de la empresa relacionado con el uso de las TI es identificado y gestionado.	
EDM04. Asegurar la optimización de recursos: Asegurar que las adecuadas y suficientes capacidades relacionadas con las TI (personas, procesos y tecnologías) están disponibles para soportar eficazmente los objetivos de la empresa a un coste óptimo.	
EDM05. Asegurar la transparencia hacia las partes interesadas: Asegurar que la medición y la elaboración de informes en cuanto a conformidad y desempeño de las TI de la empresa son transparentes, con aprobación por las partes interesadas de las metas, las métricas y las acciones correctivas necesarias.	

Fuente: Elaboración propia a partir de [16]

Tabla 6. Procesos de Alineación, Planeación y Organización (APO)

Procesos para la gestión de la TI Empresarial	
Dominio de Gestión	**Alinear, Planear y Organizar (APO):** Este dominio cubre las estrategias y las tácticas, y tiene que ver con identificar la manera en que TI puede contribuir mejor con los objetivos del negocio. Este dominio proporciona la dirección para la entrega de soluciones y la entrega de servicios.
Procesos	
APO01. Gestionar el Marco de Gestión de TI: Aclarar y mantener el gobierno de la misión y la visión corporativa de TI.	
APO02. Gestionar la Estrategia: Proporcionar una visión holística del negocio actual y del entorno de TI, la dirección futura, y las iniciativas necesarias para migrar al entorno deseado.	
APO03. Gestionar la Arquitectura Empresarial: Establecer una arquitectura común compuesta por los procesos de negocio, la información, los datos, las aplicaciones y las capas de la arquitectura tecnológica de manera eficaz y eficiente para la realización de las estrategias de la empresa y de TI mediante la creación de modelos clave y prácticas que describan las líneas de partida y las arquitecturas objetivo.	
APO04. Gestionar la Innovación: Analizar cuáles son las oportunidades para la innovación empresarial o qué mejora puede crearse con las nuevas tecnologías, servicios o innovaciones empresariales facilitadas por TI, así como a través de las tecnologías ya existentes y por la innovación en procesos empresariales y de TI.	
APO05. Gestionar el Portafolio: Ejecutar el conjunto de direcciones estratégicas para la inversión alineada con la visión de la arquitectura empresarial, las características deseadas de inversión, los portafolios de servicios relacionados, considerar las diferentes categorías de inversión y recursos y las restricciones de financiación.	

APO06 Gestionar el Presupuesto y los Costes: Gestionar las actividades financieras relacionadas con las TI tanto en el negocio como en las funciones de TI, abarcando presupuesto, coste y gestión del beneficio, y la priorización del gasto mediante el uso de prácticas presupuestarias formales y un sistema justo y equitativo de reparto de costes a la empresa. **APO07. Gestionar los Recursos Humanos:** Proporcionar un enfoque estructurado para garantizar una óptima estructuración, ubicación, capacidades de decisión y habilidades de los recursos humanos.
AP008. Gestionar las relaciones: Gestionar las relaciones entre el negocio y TI de modo formal y transparente, enfocándolas hacia el objetivo común de obtener resultados empresariales exitosos apoyando los objetivos estratégicos y dentro de las restricciones del presupuesto y los riesgos tolerables.
AP009. Gestionar los acuerdos de servicio: Alinear los servicios basados en TI y los niveles de servicio con las necesidades y expectativas de la empresa, incluyendo identificación, especificación, diseño, publicación, acuerdo y supervisión de los servicios TI, niveles de servicio e indicadores de rendimiento.
APO10. Gestionar los Proveedores: Administrar todos los servicios de TI prestados por todo tipo de proveedores para satisfacer las necesidades del negocio, incluyendo la selección de los proveedores, la gestión de las relaciones, la gestión de los contratos y la revisión y supervisión del desempeño, para una eficacia y cumplimiento adecuados.
APO11. Gestionar la Calidad: Definir y comunicar los requisitos de calidad en todos los procesos, procedimientos y resultados relacionados de la organización, incluyendo controles, vigilancia constante y el uso de prácticas probadas y estándares de mejora continua y esfuerzos de eficiencia.
APO12 Gestionar el Riesgo: Identificar, evaluar y reducir los riesgos relacionados con TI de forma continua, dentro de niveles de tolerancia establecidos por la dirección ejecutiva de la empresa.
APO13. Gestionar la Seguridad: Definir, operar y supervisar un sistema para la gestión de la seguridad de la información.

Fuente: Elaboración propia a partir de [16]

Tabla 7. Procesos de Construcción, Adquisición e Implementación (BAI)

Procesos para la gestión de la TI Empresarial	
Dominio de Gestión	**Construir, Adquirir e Implementar (BAI):** La gerencia con este dominio pretende cubrir, que los nuevos proyectos generen soluciones que satisfagan las necesidades del negocio, que sean entregados en tiempo y dentro del presupuesto, que los nuevos sistemas una vez implementados trabajen adecuadamente y que los cambios no afecten las operaciones actuales del negocio.
Procesos	
BAI01. Gestión de Programas y Proyectos: Gestionar todos los programas y proyectos del portafolio de inversiones de forma coordinada y en línea con la estrategia corporativa. Iniciar, planificar, controlar y ejecutar programas y proyectos y cerrarlos con una revisión post-implementación.	
BAI02. Gestionar la Definición de Requisitos: Identificar soluciones y analizar requerimientos antes de la adquisición o creación para asegurar que estén en línea con los requerimientos estratégicos de la organización y que cubren los procesos de negocios, aplicaciones, información/datos, infraestructura y servicios.	
BAI03. Gestionar la Identificación y Construcción de Soluciones: Establecer y mantener soluciones identificadas en línea con los requerimientos de la empresa que abarcan el diseño, desarrollo, compras/contratación y asociación con proveedores/fabricantes.	
BAI04. Gestionar la Disponibilidad y la Capacidad: Equilibrar las necesidades actuales y futuras de disponibilidad, rendimiento y capacidad con una provisión de servicio efectiva en costes. Incluye la evaluación de las capacidades actuales, la previsión de necesidades futuras basadas en los requerimientos del negocio.	
BAI05. Gestionar la Facilitación del Cambio Organizativo: Maximizar la probabilidad de la implementación exitosa en toda la empresa del cambio	

organizativo de forma rápida y con riesgo reducido, cubriendo el ciclo de vida completo del cambio y todas las partes interesadas del negocio y de TI.
BAI06. Gestionar los Cambios: Gestiona todos los cambios de una forma controlada, incluyendo cambios estándar y de mantenimiento de emergencia en relación con los procesos de negocio, aplicaciones e infraestructura. Esto incluye normas y procedimientos de cambio, análisis de impacto, priorización y autorización, cambios de emergencia, seguimiento, reporte, cierre y documentación. **BAI07. Gestionar la Aceptación del Cambio y la Transición:** Aceptar formalmente y hacer operativas las nuevas soluciones, incluyendo la planificación de la implementación, la conversión de los datos y los sistemas, las pruebas de aceptación, la comunicación, la preparación del lanzamiento, el paso a producción de procesos de negocio o servicios TI nuevos o modificados, el soporte temprano en producción y una revisión post-implementación.
BAI08. Gestionar el Conocimiento: Mantener la disponibilidad de conocimiento relevante, actual, validado y fiable para dar soporte a todas las actividades de los procesos y facilitar la toma de decisiones. Planificar la identificación, recopilación, organización, mantenimiento, uso y retirada de conocimiento.
BAI09. Gestionar los Activos: Gestionar los activos de TI a través de su ciclo de vida para asegurar que su uso aporta valor a un coste óptimo, que se mantendrán en funcionamiento, que están justificados y protegidos físicamente, y que los activos que son fundamentales para apoyar la capacidad del servicio son fiables y están disponibles.
BAI10. Gestionar la Configuración: Definir y mantener las definiciones y relaciones entre los principales recursos y capacidades necesarios para la prestación de los servicios proporcionados por TI, incluyendo la recopilación de información de configuración, el establecimiento de líneas de referencia, la verificación y auditoría de la información de configuración y la actualización del repositorio de configuración.

Fuente: Elaboración propia a partir de [16]

Tabla 8. Procesos de Entrega, Dar Servicio y Soporte (DSS)

Procesos para la gestión de la TI Empresarial	
Dominio de Gestión	**Entregar, Dar Servicio y Soporte (DSS):** Involucra la entrega en sí de los servicios requeridos, incluyendo la prestación del servicio, la administración de la seguridad y de la continuidad, el soporte a los usuarios del servicio, la administración de los datos y de las instalaciones operativas.
Procesos	
DSS01. Gestionar Operaciones: Coordinar y ejecutar las actividades y los procedimientos operativos requeridos para entregar servicios de TI tanto internos como externalizados, incluyendo la ejecución de procedimientos operativos estándar predefinidos y las actividades de monitorización requeridas.	
DSS02. Gestionar Peticiones e Incidentes de Servicio: Proveer una respuesta oportuna y efectiva a las peticiones de usuario y la resolución de todo tipo de incidentes. Recuperar el servicio normal; registrar y completar las peticiones de usuario; y registrar, investigar, diagnosticar, escalar y resolver incidentes.	
DSS03. Gestionar Problemas: Identificar y clasificar problemas y sus causas raíz y proporcionar resolución en tiempo para prevenir incidentes recurrentes. Proporcionar recomendaciones de mejora.	
DSS04. Gestionar la Continuidad: 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.	
DSS05. Gestionar Servicios de Seguridad: 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 la seguridad.	

DSS06. Gestionar Controles de Proceso de Negocio: Definir y mantener controles apropiados de proceso de negocio para asegurar que la información relacionada y procesada dentro de la organización o de forma externa satisface todos los requerimientos relevantes para el control de la información.

Fuente: Elaboración propia a partir de [16]

Tabla 9. Procesos de Supervisión, Evaluación y Valoración (MEA)

Procesos para la gestión de la TI Empresarial	
Dominio de Gestión	S**upervisar, Evaluar y Valorar (MEA):** La totalidad de los procesos de TI deben de ser evaluados regularmente en el tiempo, para conocer su calidad y cumplimiento de los requerimientos de control. Este dominio incluye la administración del desempeño, el monitoreo del control interno, el cumplimiento regulatorio y la aplicación del gobierno.
Procesos	
MEA01. Supervisar, Evaluar y Valorar el Rendimiento y la Conformidad: Recolectar, validar y evaluar métricas y objetivos de negocio, de TI y de procesos. Supervisar que los procesos se están realizando acorde al rendimiento acordado y conforme a los objetivos y métricas y se proporcionan informes de forma sistemática y planificada.	
MEA02. Supervisar, Evaluar y Valorar el Sistema de Control Interno: Facilitar a la Dirección la identificación de deficiencias e ineficiencias en el control y el inicio de acciones de mejora. Planificar, organizar y mantener normas para la evaluación del control interno y las actividades de aseguramiento.	
MEA03. Supervisar, Evaluar y Valorar la Conformidad con los Requerimientos Externos: Evaluar el cumplimiento de requisitos regulatorios y contractuales tanto en los procesos de TI como en los procesos de negocio dependientes de las tecnologías de la información. Obtener garantías de que se han	

identificado, se cumple con los requisitos y se ha integrado el cumplimiento de TI en el cumplimiento de la empresa general

Fuente: Elaboración propia a partir de [16]

2.2.5.2 Adaptación de COBIT 5.0

La metodología COBIT 5 puede ser utilizada en dos partes individuales, la primera parte es el manejo de los Principios de COBIT, la cual cuenta de cinco principios los cuales serán aplicados en el presente trabajo.

La segunda parte es el manejo de procesos los cuales no se manejarán en este caso, debido a que no se trabajara con niveles de madurez.

La utilización de los Principios COBIT 5.0 lleva consigo beneficios que nos permitirá entender el funcionamiento actual del departamento de Tecnologías de la Información, para de esta manera poder evidenciar si dicho departamento trabaja con políticas, metodologías o estándares los cuales ayuden a un manejo adecuado del sistema Cabildo y de la información.

CAPITULO III.- RESULTADOS Y DISCUSIÓN

3.1 Análisis y discusión de los resultados

3.1.1 Evaluación de la situación actual del sistema informático Cabildo

3.1.1.1 Situación Actual del Gobierno Autónomo Descentralizado Municipal de Ambato

El Gobierno Autónomo Descentralizado Municipalidad de Ambato es el encargado de administrar los recursos de la ciudad de Ambato, su finalidad es promover el empleo, bienestar social y desarrollo de las necesidades de los ciudadanos y de sus parroquias que la conforma.

El Gobierno Autónomo Descentralizado Municipalidad de Ambato es el encargado de controlar el presupuesto de recaudaciones y las líneas de crédito, tanto en la parte nacional como internacional.

Esta institución pública se rige por tres funciones, la Función Legislativa, Función Ejecutiva y la Función Participación Ciudadana y Control Social, en este caso la Función Legislativa es representada por el Concejo Municipal, la Función Ejecutiva es representada por el señor alcalde de la ciudad y la Función Participación Ciudadana y Control Social es representado por la Asamblea Nacional

La institución cuenta con varios sistemas los cuales ayudan al desenvolvimiento de varias actividades, pero el sistema más utilizado es el sistema llamado CABILDO el cual es el encargado de la recaudación de la ciudad de Ambato.

En la actualidad el Gobierno Autónomo Descentralizado Municipalidad de Ambato también brinda servicios a los contribuyentes como

1. Promover la participación ciudadana.
2. Fortalecer la seguridad ciudadana.
3. Mantener los parques y jardines.
4. Garantizar el control sanitario.
5. Conservar el medio ambiente.
6. Promover el bienestar social.
7. Fomentar la cultura, el deporte y el turismo.
8. Proveer limpieza pública.
9. Mantener la infraestructura vial.

10. Administrar el Tránsito y Transporte Terrestre.
11. Planificar el desarrollo ordenado del territorio.**[23]**

3.1.1.1.1 Análisis General

3.1.1.1.2 Direccionamiento Estratégico

El Gobierno Autónomo Descentralizado Municipalidad de Ambato tiene los siguientes elementos; que se muestran el Tabla 10.

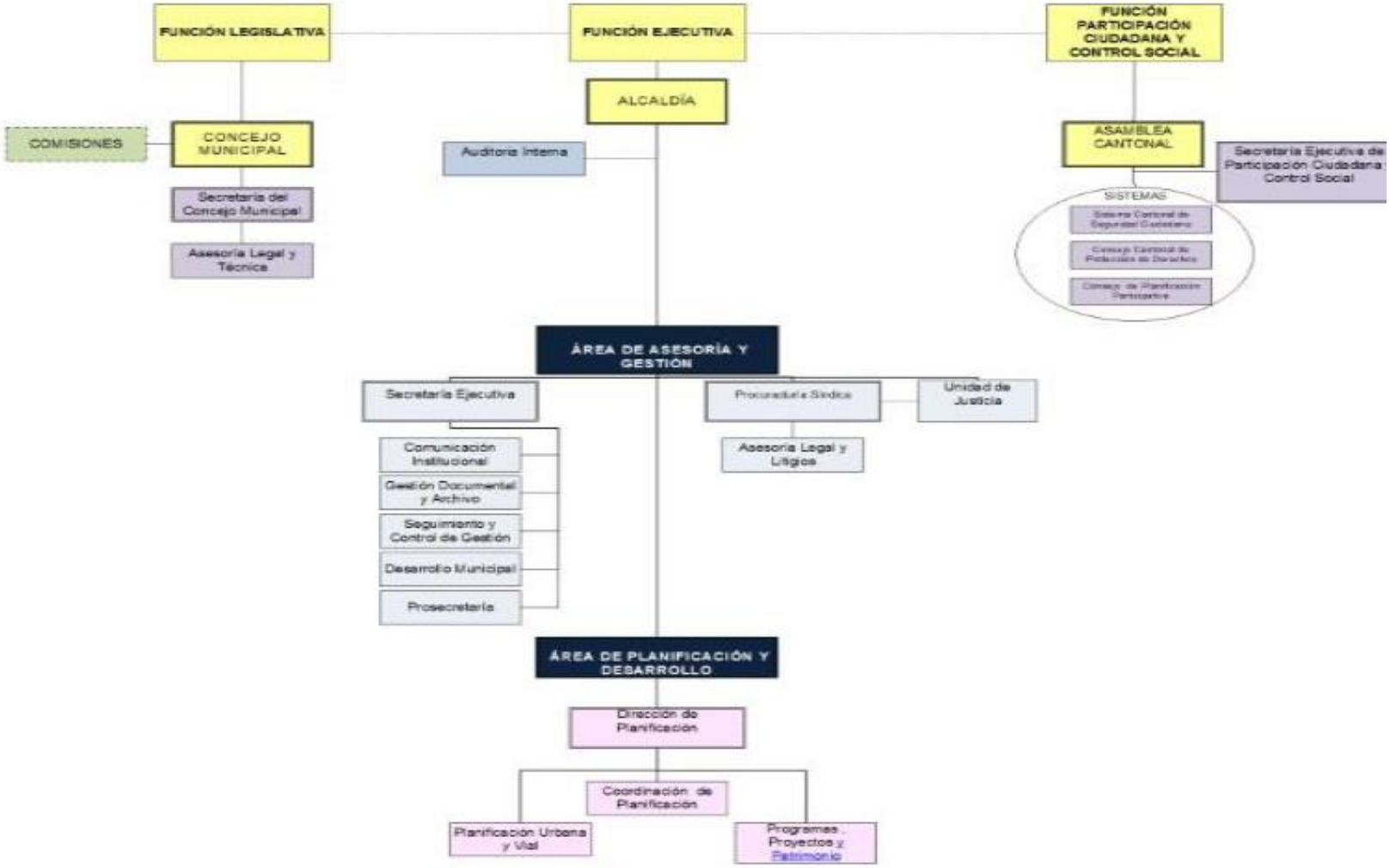
Tabla 10. Direccionamiento Estratégico del Gobierno Autónomo Descentralizado Municipalidad de Ambato

Direccionamiento Estratégico del Gobierno Autónomo Descentralizado Municipalidad de Ambato	
Misión	La misión actual del Gobierno Autónomo Descentralizado Municipal de Ambato es el desarrollo sustentable basándose en la gestión integral municipal, esta se guiará en procesos y políticas locales para la innovación del cantón.
Visión	El Gobierno Autónomo Descentralizado Municipal de Ambato es una institución pública equitativa y publica, la cual es caracterizada por su efectividad y excelencia del cumplimiento de los derechos humanos fundamentalmente basado en el desarrollo.
Valores	Transparencia Y Honestidad Eficacia Respeto Equidad Compromiso
Principios	Justicia Social Pluralismo Responsabilidad Comunitaria Vocación De Servicio
Fines	• El desarrollo equitativo y solidario mediante el fortalecimiento del proceso de autonomías y descentralización;

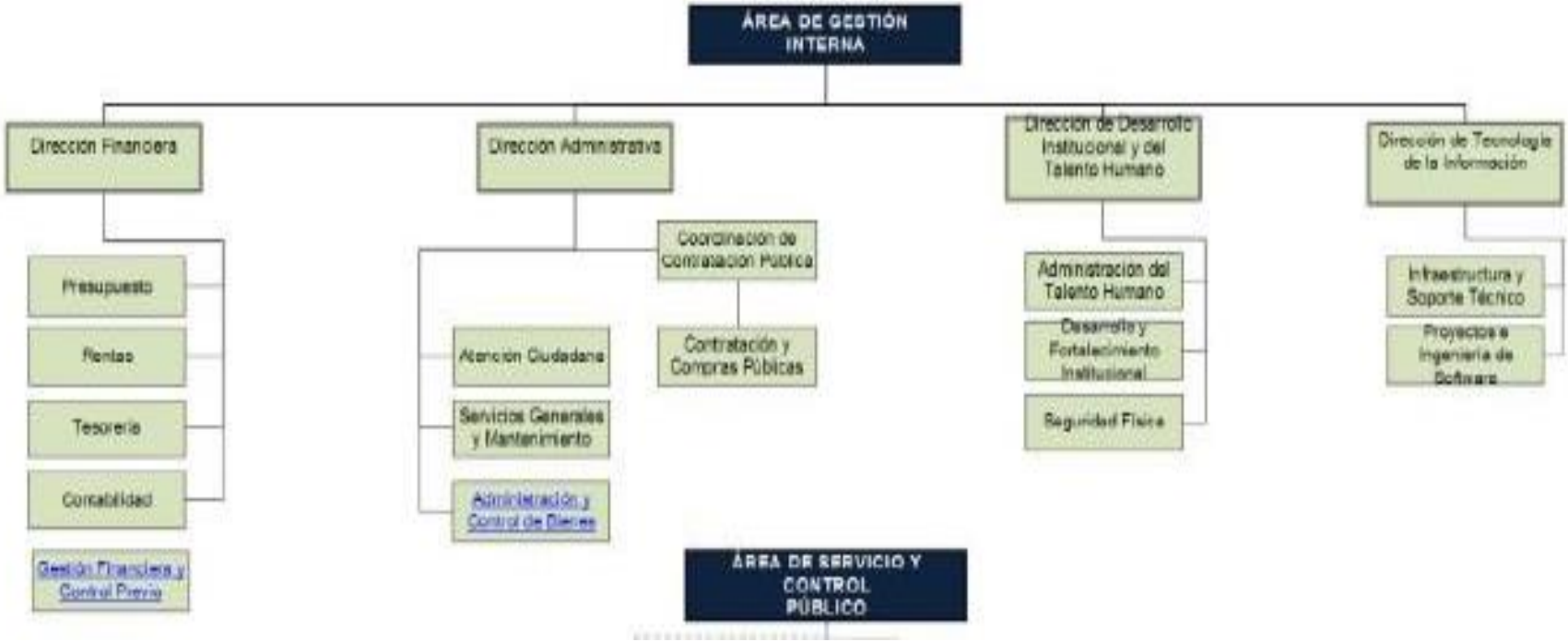
	• La garantía, sin discriminación alguna y en los términos previstos en la Constitución de la República, de la plena vigencia y el efectivo goce de los derechos individuales y colectivos constitucionales y de aquellos contemplados en los instrumentos internacionales; • El fortalecimiento de la unidad nacional en la diversidad; • La recuperación y conservación de la naturaleza y el mantenimiento de un ambiente sostenible y sustentable; • La protección y promoción de la diversidad cultural y el respeto a sus espacios de generación e intercambio; la recuperación, preservación y desarrollo de la memoria social y el patrimonio cultural; • La obtención de un hábitat seguro y saludable para los ciudadanos y la garantía de su derecho a la vivienda en el ámbito de sus respectivas competencias; • El desarrollo planificado participativamente para transformar la realidad y el impulso de la economía popular y solidaria con el propósito de erradicar la pobreza, distribuir equitativamente los recursos y la riqueza, y alcanzar el buen vivir; • La generación de condiciones que aseguren los derechos y principios reconocidos en la Constitución a través de la creación y funcionamiento de sistemas de protección integral de sus habitantes

Fuente: Elaboración propia a partir de [19] y [20]

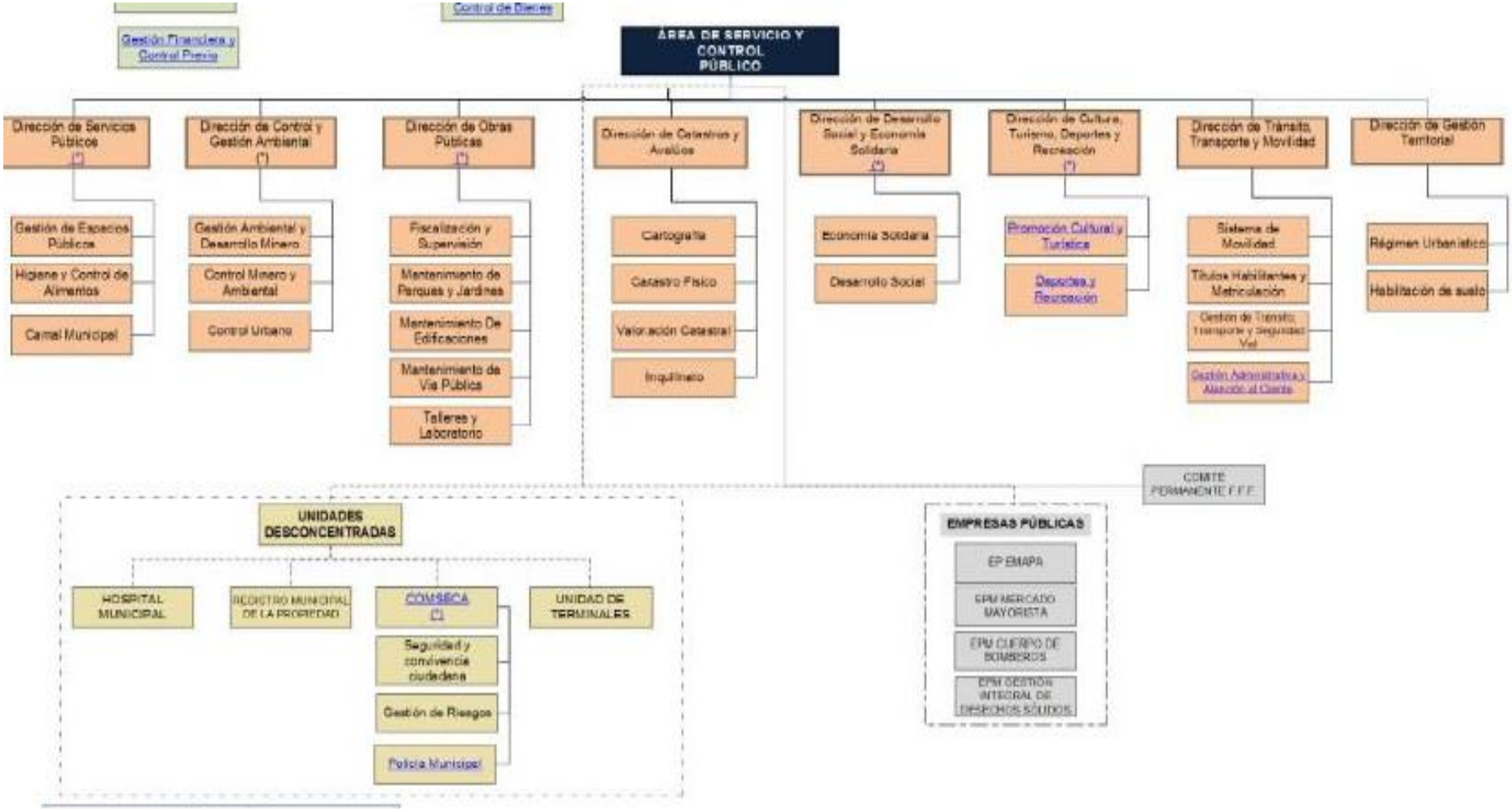
3.1.1.1.3 Organigrama del Gobierno Autónomo Descentralizado Municipal de Ambato (1/3)



(2/3)


ÁREA DE GESTIÓN INTERNA
Dirección Financiera
Presupuesto
Rentas
Tesorería
Contabilidad
Gestión Financiera y Control Previo
Dirección Administrativa
Coordinación de Contratación Pública
Atención Ciudadana
Contratación y Compras Públicas
Servicios Generales y Mantenimiento
Administración y Control de Bienes
Dirección de Desarrollo Institucional y del Talento Humano
Administración del Talento Humano
Desarrollo y Fortalecimiento Institucional
Seguridad Física
Dirección de Tecnología de la Información
Infraestructura y Soporte Técnico
Proyectos e Ingeniería de Software
ÁREA DE SERVICIO Y CONTROL PÚBLICO

(3/3)


Gestión Financiera y Control Previo
Control de Datos
ÁREA DE SERVICIO Y CONTROL PÚBLICO
Dirección de Servicios Públicos (*)
Dirección de Control y Gestión Ambiental (*)
Dirección de Obras Públicas (*)
Dirección de Catastros y Avalúos
Dirección de Desarrollo Social y Economía Solidaria (*)
Dirección de Cultura, Turismo, Deportes y Recreación (*)
Dirección de Tránsito, Transporte y Movilidad
Dirección de Gestión Territorial
Gestión de Espacios Públicos
Higiene y Control de Alimentos
Camal Municipal
Gestión Ambiental y Desarrollo Minero
Control Minero y Ambiental
Control Urbano
Fiscalización y Supervisión
Mantenimiento de Parques y Jardines
Mantenimiento De Edificaciones
Mantenimiento de Vía Pública
Talleres y Laboratorio
Cartografía
Catastro Físico
Valoración Catastral
Inquilinato
Economía Solidaria
Desarrollo Social
Promoción Cultural y Turística
Deportes y Recreación
Sistema de Movilidad
Títulos Habilitantes y Matriculación
Gestión de Tránsito, Transporte y Seguridad Vial
Gestión Administrativa y Atención al Cliente
Régimen Urbanístico
Habilitación de suelo
COMITÉ PERMANENTE F.F.F.
UNIDADES DESCONCENTRADAS
HOSPITAL MUNICIPAL
REGISTRO MUNICIPAL DE LA PROPIEDAD
COMISCA (*)
UNIDAD DE TERMINALES
Seguridad y convivencia ciudadana
Gestión de Riesgos
Policía Municipal
EMPRESAS PÚBLICAS
EP EMAPA
EPM MERCADO MAYORISTA
EPM CUERPO DE BOMBEROS
EPM GESTIÓN INTEGRAL DE DESECHOS SÓLIDOS

Fuente: [21]

3.1.1.2 Departamento de Tecnologías de la Información

El Departamento de Tecnologías de la Información es el encargado de proveer servicios tecnológicos de alta calidad, los cuales se basarán en herramientas actualizadas y confiables, estas ayudarán a mantener los procesos y actividades fiables en la institución y en la comunidad.

En la actualidad no se han realizado auditorias informáticas, pero cuentan con documentación donde establecen sus funciones también cuentan con Planes de Contingencia los cuales se crean para poder prevenir accidentes o fallos en aplicaciones informáticas, equipos tecnológicos y otros sistemas que maneje la institución.

En el último inventario realizado a todo el Municipio de Ambato y a sus entidades externas se puedo contabilizar un total de 549 equipos de cómputos; cómo se puede apreciar en la Tabla 11.

Tabla 11. Inventario de maquinas

MANTENIMIENTO DE MAQUINAS	
MUNICIPIO HUACHI	359
SERVICIOS PUBLICOS	28
JUNTA CANT. DE LA NIÑEZ	8
MUNICIPIO CENTRO	38
DTTM	38
CENTRO CULTURA	20
TRANSITO	8
BODEGA	12
CAMAL	11
LAPTOP	27
	549

Fuente: Elaboración propia

3.1.1.2.1 Objetivos de Tecnologías de la Información

Incrementar el conocimiento del personal del Gobierno Autónomo Descentralizado Municipalidad de Ambato en los sistemas informáticos propios del municipio.

Incrementar la eficacia del servicio de tecnología a usuarios mediante la utilización de conceptos y buenas prácticas para la gestión de servicios de Tecnología de la Información, así como la elaboración y difusión de políticas de uso de los recursos.

Incrementar la eficacia y eficiencia en la gestión de infraestructura y servicios tecnológicos mediante la definición de procesos y la generación de nuevos servicios para los funcionarios del Gobierno Autónomo Descentralizado Municipalidad de Ambato.

Incrementar la eficacia y eficiencia en la gestión de infraestructura y servicios tecnológicos mediante la definición de procesos y la generación de nuevos servicios para los funcionarios del Gobierno Autónomo Descentralizado Municipalidad de Ambato.

Incrementar la seguridad informática interna y externa. **[22]**

En la actualidad el Departamento de Tecnologías de la Información maneja varios sistemas, los cuales se pueden evidenciar en la Tabla 12.

Tabla 12. Sistemas Informáticos de TI

SISTEMAS INFORMÁTICOS DE TI
CABILDO
VIF
DOCFLOW
GIS
SISCAR
REGIS
GESTION DOCUMENTAL
GAD DE AMBATOTIC

SISTEMAS INFORMÁTICOS DE TI
NORMAS PARTICULARES
PAGINA WEB

Fuente: Elaboración propia a partir de [23]

El departamento de Tecnologías de la Información (TI) también es el encargado de la administración de otros sistemas informáticos, los cuales son de gran utilidad en la institución; cómo se puede observar en la Tabla 13.

Tabla 13. Otros Sistemas Informáticos

OTROS SISTEMAS INFORMATICOS	
SISTEMAS INFORMATICOS	**DESCRIPCIÓN**
Sistemas Operativos	Microsoft Windows Server
	Microsoft windows 7
	Redhat Linux
Bases de Datos	Oracle Server Data Base
	MySQL
Software de diseño	Autodesk swit
	Adobe cloud
Sistema de Seguridad	Firewall Checkpoint
Sistema de Comunicación	Correo electronico Outlook
	Skype
	SysAid
	VNC
Sistema de Antivirus	ESET
Mesa de Ayuda	SYSAID

SISTEMAS INFORMATICOS	DESCRIPCIÓN
Lenguaje de programación	PL/SQL Developer
	Visual Estudio.net
	Java
	Oracle Developer
Swit Offimatica	Office 365
	Libre office
	Open Office

Fuente: Elaboración propia a partir de [23]

3.1.1.2.2 Áreas de Tecnologías de la Información

a.- Proyectos de Ingeniería de Software

b.- Infraestructura y Soporte Técnico

"a.- Proyectos de Ingeniería de Software

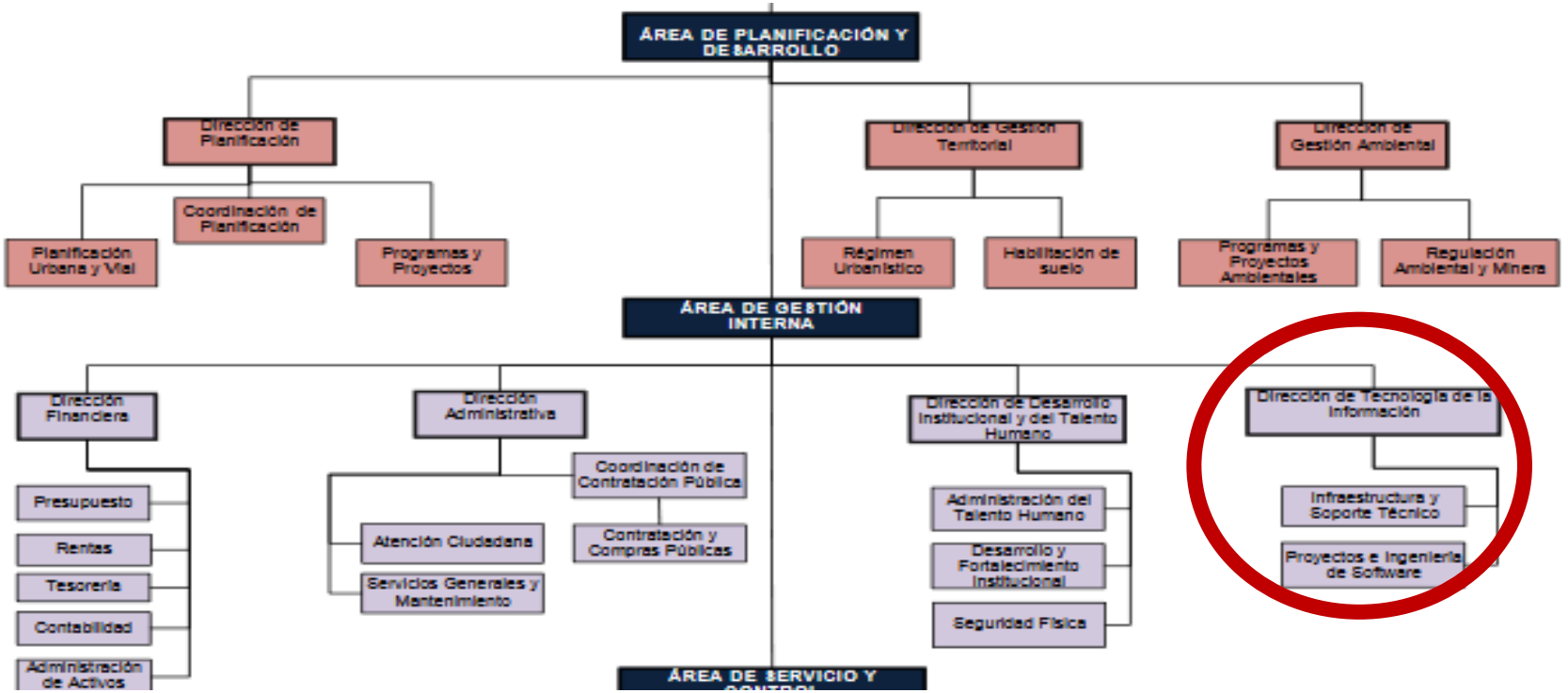
1. Proponer, coordinar, ejecutar y dar seguimiento a proyectos de implementación y mejoramiento de sistemas o procesos informáticos.
2. Definir políticas y estándares para el desarrollo de sistemas en el GAD Municipalidad de Ambato.
3. Analizar, desarrollar y mantener las aplicaciones y bases de datos internas necesarias para el funcionamiento del GAD Municipalidad de Ambato.
4. Asegurar la disponibilidad de la base de datos.
5. Realizar pruebas del sistema o aplicativo informático que garanticen la puesta a punto y eficacia en la implementación.
6. Desarrollar manuales de usuarios y/o socializaciones que permitan al usuario el uso y manejo adecuado del sistema o aplicativo informático.
7. Participar del análisis e implementación de aplicaciones de terceros.
8. Gestionar el mantenimiento de aplicaciones de terceros.
9. Verificar la integridad de la información.

10. Extraer información y generar reportes que no puedan ser accesibles por los sistemas.
11. Administrar el Sistema de Información, el recurso humano, material de la Unidad de Proyectos e Ingeniería de Software.
12. Cumplir con demás funciones y actividades establecidas en la normativa vigente.
13. Gestionar y mejorar continuamente los procesos de la Unidad de Departamento de Proyectos e Ingeniería de Software" **[21]**.

"b.- Infraestructura y Soporte Técnico

1. Mantener y mejorar la conectividad de los sistemas de información.
2. Gestionar el mantenimiento y soporte de los equipos informáticos en la Municipalidad.
3. Realizar el análisis, diseño, desarrollo y pruebas de los sistemas y aplicaciones informáticas.
4. Realizar actividades que permitan la mejora, adaptación o corrección de los sistemas y aplicaciones informáticas.
5. Definición e implementar estándares de gestión para el desarrollo y el mejoramiento de la conectividad para la Municipalidad, así como empresa descentralizadas de la misma.
6. Gestionar, administrar y garantizar la disponibilidad de la base de datos de la Municipalidad para la optimización de recursos.
7. Coordinación y liderazgo de la ejecución de contingencias de la Conectividad.
8. Administrar el Sistema de Información, el recurso humano, material de la Dirección de Tecnología de Información.
9. Cumplir con demás funciones y actividades establecidas en la normativa vigente" **[21]**.

3.1.1.2.3 Organigrama del Departamento de Tecnologías de la Información



Fuente: [21]

3.1.1.2.4 Análisis y discusión de la entrevista

Tabla 14. Entrevista al director del Departamento de Tecnologías de la Información

ENTREVISTA REALIZADA AL DIRECTOR DEL DEPARTAMENTO DE TECNOLOGÍAS DE LA INFORMACIÓN DEL GAD MUNICIPAL DE AMBATO		
OBJETIVO	Recolectar información de la situación actual del Sistema Cabildo y del departamento de Tecnologías de la Información en el GAD de Ambato.	
FECHA:	2 de Julio del 2019	
ENTREVISTADO:	Ing. Eduardo Vinueza	
CARGO:	Jefe de proyectos de desarrollo de software	
N°	**Preguntas**	**Respuestas**
1	¿Conoce Ud si el departamento de TI cuanta con un plan estratégico para la mejora del sistema Cabildo?	Si se cuenta con un plan estratégico para la adquisición de un nuevo sistema, para la migración por motivos que la empresa que desarrollo cabido tiene problemas económicos y técnicos.
2	¿Existen algún plan para la seguridad de la información de la institución?	Se está levantando un proceso de consultoría porque la seguridad de la información a nivel de tecnologías es muy vulnerable, el director con Hacking ético hizo penetraciones y se pudo observar muchas vulnerabilidades.
3	¿Conoce con cuántos sistemas cuenta la institución y cual son sus funciones?	Existen varios módulos que se comunican entre sí.
4	¿Conoce Ud si se ha realizado una Auditoria	No, al momento no se ha realizado.

	Informática en el departamento de TI?	
5	¿Cree necesaria la elaboración de una auditoria informática en el departamento de TI?	Si, para poder ver el estado actual del departamento.
6	¿Ha considerado la importancia que tiene la información que se maneja en la institución?	Siempre la información y en todas las entidades se las ha visto como cuello de botella sin saber que ahora las nuevas tendencias consideran la información se conserva como un Activo y es muy importante.
7	¿El GAD de Ambato ha sufrido ataque mediante la red?	El director realizo hacking ético en el departamento de TI para demostrar las vulnerabilidades que tiene el municipio, pero no se sabría decir si por fuera existe vulnerabilidad. A cuentas del dominio del GAD de Ambato.
8	¿El área de tecnologías de la información cuenta con documentación donde establezca sus funciones?	Si, cada uno tiene su documentación acorde a lo que desarrolla. Con esa información realizan las capacitaciones para los nuevos desarrollos y usuarios finales.
9	¿Considera que el personal del área está capacitado para realizar las tareas que desempeñan?	Está capacitado y especializado para los módulos que ellos llevan, las nuevas tecnologías nos exigen capacitación e investigación es un proceso que se va a conciliar con todos para llegar a una nivelación para todos.
10	¿Se requiere de servicios de terceros	Solo en el caso que se requiera intercambiar información entre instituciones, obviamente con los convenios que existan, más no para

	para cumplir con las funciones del área?	depender de una persona desarrolladoras para utilizar los módulos.
11	¿Conoce Ud si han existido problemas con los usuarios creados en la base del GAD de Ambato?	A nivel de roles y privilegios no han sido correctamente definidos que rol y que privilegio deben tener asignados.
12	¿La empresa posee manuales actualizados de procedimientos y procesos que se deben realizar?	Si cada uno tiene y de cada proceso que se levanta se tiene información, mediante el trabajo que se genera.
ENTREVISTADOR: Andrés Ruíz		

Como se ha demostrado en la Tabla 14 en la entrevista realizada al Ingeniero Eduardo Vinueza Jefe de proyectos de desarrollo de software se logró entender que en el departamento de Tecnologías de Información no se han realizado trabajos de Auditorias Informáticas, las cuales permitan brindar una visión de cómo se encuentra actualmente dicho departamento, también se evidencio que no cuentan con un plan estratégico el cual nos ayude a saber que sucedería en caso de pérdidas o falencias del Sistema Cabildo, uno de los inconvenientes más críticos del departamento de TI es que no cuentan con asignación de perfiles al momento de la creación de usuarios; también se puedo evidenciar la inexistencia de políticas las cuales ayudarían al departamento a un manejo adecuado de procesos y de información.

Los resultados obtenidos no podrán ser comparados con otros trabajos como tesis o papers, ya que no se basan en los cinco principios de Cobit 5.0, los cuales serán aplicados al sistema Cabildo.

3.1.1.3 Sistema Cabildo

El sistema fue desarrollado en el año 2002 e implementado en el año 2004, su lenguaje de programación es Oracle Developers 6i, para la creación de ventanas se trabajó con Forms builders y para la generación de reportes se utilizó Reports builders, este sistema actualmente trabaja con la base de datos Oracle 12c.

El Sistema Cabildo es un sistema de gestión financiera y control municipal, su función principal es la emisión y recaudación de impuestos en la Ciudad de Ambato. Dicho sistema está conformado por varios módulos, los cuales serán utilizados dependiendo el cargo de cada funcionario.

En la actualidad el Gobierno Autónomo Descentralizado de Ambato dispone de un crecimiento continuo de información ocasionando que la información se vuelva vulnerable ante la inseguridad del sistema Cabildo, tiene la siguiente estructura como se puede apreciar en la Figura 3.

Figura 3. Sistema Cabildo

Fuente: Departamentos de Tecnologías de Información

Figura 4. Desglose del proceso de Recaudación

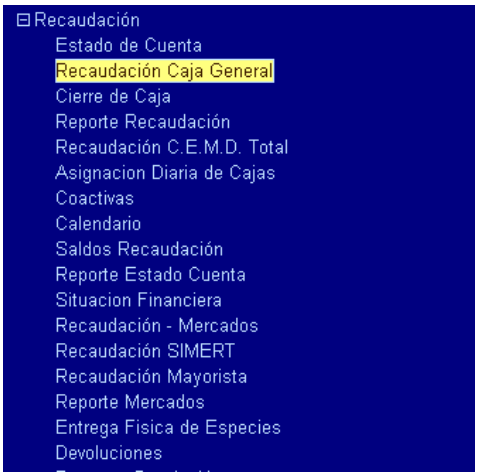
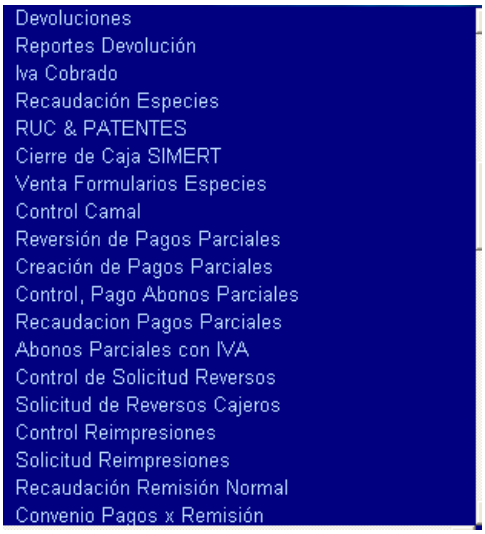


Figura 5. Desglose del proceso de Recaudación (2)



Fuente: Departamentos de Tecnologías de Información

Por el momento el sistema Cabildo se encuentra en funcionamiento y se sigue desarrollando aplicaciones para poder cumplir con los requerimientos que sigan apareciendo, en la parte de tecnologías de la información se encuentran en reuniones para ver si el sistema Cabildo será migrado a otra plataforma, ya que la compañía encargada del desarrollo de dicho sistema se encuentra en problemas económicos.

3.1.1.3.1 Documentación del Sistema Cabildo

Se solicito información del sistema Cabildo la cual ayudará a evidenciar la documentación existente; la cual se podrá evidenciar en la Tabla 15.

Tabla 15. Documentación del Sistema Cabildo

Documentación	Validación	Observación
Plan de Contingencia.	No cumple.	Se pudo evidenciar que no cuentan con un plan de contingencia el cual nos ayude a entender que procedimiento se debería tomar si dicho sistema colapsara.
Plan estratégico.	No cumple.	Se pudo evidenciar que no cuentan con un plan estratégico el cual ayude a una mejora del sistema Cabildo.
Levantamiento de requerimientos.	No cumple.	No se encontró documentación la cual pueda sustentar el levantamiento de requerimientos del proceso de Recaudación.
Diagramas de Flujo.	No cumple.	No se cuenta con diagramas de flujo los cuales ayuden a entender el manejo del sistema Cabildo.

Fuente: Elaboración propia

El sistema Cabildo no cuenta con documentación pertinente la cual ayude entender su proceso en la actualidad, tampoco se cuenta con la información del levantamiento de requerimientos, el cual nos ayudaría a entender como está estructurado dicho sistema.

3.1.1.3.2 Base de datos

En la actualidad la base de datos utilizada en el Gobierno Autónomo Descentralizado Municipalidad de Ambato es Oracle 12c esta es manejada por el Área de Desarrollo la cual se encuentra ubicada en el Departamento de Tecnologías de la Información.

Las características que presenta un DBMS son las siguientes:

- Integridad y seguridad de los datos.
- Proporcionar lenguajes para consultas de manera interactiva.
- Solventar una manera interactiva para introducir y editar datos.

Esta base de datos manejada es utilizada a nivel mundial ya que una de sus principales ventajas es la ejecución en todas las plataformas.

En el GAD de Ambato la base de datos cuenta con 3 bases principales que son:

- Muni
- Prd
- GAD de Ambatogis

De esta base se realiza respaldos todos los días a media noche, para poder almacenar toda la información del día.

Uno de los inconvenientes de la base de datos tiene que ver al momento de la creación de usuarios ya que no se tiene establecido a que rol y a que perfil pertenece cada usuario creado en la base de datos.

3.1.1.3.3 Redes y comunicaciones.

Es un conjunto de elementos los cuales están conectados entre sí, en la actualidad el Gobierno Autónomo Descentralizado Municipalidad de Ambato cuenta con el manejo del Checkpoint y el firewall.

El checkpoint ayuda a monitorear el tráfico de red entrante y saliente mediante la generación de reglas, las cuales ayudan a definir ciertos permisos de acceso a la red, dependiendo el perfil del usuario del municipio.

Firewall el cual ayuda a evitar ataques no deseados y el manejo de páginas web.

La conexión de los equipos del Gobierno Autónomo Descentralizado Municipalidad de AMBATO puede ser mediante Ip estáticas y mediante DHCP, los cuales están unidos al dominio de la empresa.

3.1.1.3.4 Seguridad lógica

La seguridad lógica en el municipio es controlada por el departamento de Tecnologías de la Información, la cual maneja varios sistemas de protección, ya que es demasiada información que maneja la empresa y siempre se trata de mantener varios tipos de seguridad como, por ejemplo.

Accesos a la red se trata de mantener solo equipos específicos que pertenecen al municipio para poder evitar posibles ataques.

Antivirus ayuda a controlar que los equipos se encuentren en óptimas condiciones y que elementos externos como flash memory no tengan virus.

3.1.1.3.5 Seguridad física

En la parte de seguridad física en el municipio es alta ya que existe personal capacitado que controla el ingreso de los usuarios y del personal, para el ingreso del personal se cuenta con un sistema biométrico el cual registra la hora de entrada y salida.

Para el ingreso a los datacenter de la institución igual se cuentan con sistemas biométricos y son pocas las personas que tienen acceso a estos lugares.

Para el ingreso de los usuarios se cuenta con guardias de seguridad que se encuentran en todas las puertas de acceso, estos son los encargados de preguntar el motivo de su visita y de receptar la cedula de identidad para poder dirigirse a un departamento en específico.

Con el análisis y documentación descrita se ha desarrollado el primer objetivo el cual nos ayudó a entender la situación actual del sistema Cabildo, al igual que sus falencias de documentación.

3.1.2 Evaluación y Auditoria del Sistema Cabildo

3.1.2.1 Diseño y Ejecución de pruebas de Auditoria Informática

Elaboración y ejecución de pruebas basadas en las cuatro áreas con las que trabaja el sistema Cabildo, las cuales son: Base de Datos, Redes y Comunicación, Seguridad Lógica y Seguridad Física, las cuales ayudaran a encontrar las falencias en estas áreas.

Mediante la ejecución de las pruebas planteadas se espera verificar la documentación pertinente, la cual ayude a una ejecución optima de las pruebas.

3.1.2.2 Listado de pruebas para el Sistema Cabildo

Planteamiento de las pruebas que se realizaran al sistema Cabildo, como se puede apreciar en la Tabla 16.

Tabla 16. Listado de pruebas para el Sistema Cabildo

BASE DE DATOS	
PRUEBA No: P001	Acceso de los usuarios a la base de datos.
PRUEBA No: P002	Creación de usuarios y contraseñas para la base de datos.
PRUEBA No: P003	Selección de personal de tecnologías de la información.
PRUEBA No: P004	Documentación de procesos de base de datos entregada al personal.
PRUEBA No: P005	Estabilidad de la base de datos en transacciones información (rollback).
PRUEBA No: P006	Recuperación de Información(backups).
PRUEBA No: P007	Control de cambios en la estructura de la base de datos.
PRUEBA No: P008	Control de duplicidad de información.
PRUEBA No: P009	Estándares de nomenclatura al momento de creación de tablas.
REDES Y COMUNICACIONES	
PRUEBA No: P010	Comprobar la seguridad configurada en el software para acceso remoto al SI CABILDO.
PRUEBA No: P011	Acceso de las personas que ingresan a las instalaciones y que trabajos se disponen a realizar en los servidores.

PRUEBA No: P0012	Integridad del cableado estructurado.
PRUEBA No: P0013	Configuración del firewall por parte del proveedor.
PRUEBA No: P014	Protocolos con los que trabajan las aplicaciones.
PRUEBA No: P015	Seguridad del checkpoint.
PRUEBA No: P016	Encriptación de información.
SEGURIDAD LÓGICA	
PRUEBA No: P017	Logs de la base de datos.
PRUEBA No: P018	Software instalado en los equipos de cómputo.
PRUEBA No: P019	Licencias del software instalado en los equipos de cómputo cliente.
PRUEBA No: P020	Eliminación de archivos temporales y obsoletos.
PRUEBA No: P021	Creación de usuarios y contraseñas del sistema Cabildo.
PRUEBA No: P022	Tipo de procedimiento de redundancia.
PRUEBA No: P023	Comprobación de los antivirus.
PRUEBA No: P024	Administración de los dispositivos de almacenamiento de los backups
SEGURIDAD FÍSICA	
PRUEBA No: P025	Sistemas de vigilancia (Cámaras).
PRUEBA No: P026	Seguridad del sistema biométrico.
PRUEBA No: P027	Contratos de los empleados de seguridad
PRUEBA No: P028	Contraseñas de acceso a la BIOS.
PRUEBA No: P029	Verificación de los UPS.
PRUEBA No: P030	Verificar el acceso al datacenter

Fuente: Elaboración propia analizando la información del sistema

3.1.2.3 Diseño de pruebas del Sistema Cabildo

Elaboración del diseño de las pruebas planteadas, que se aplicaran al sistema Cabildo, basadas en el listado de la Tabla 16.

Tabla 17. Acceso de los usuarios a la base de datos

ENTORNO: Base de Datos **PRUEBA No:** P001 Acceso de los usuarios a la base de datos.
OBJETIVO DE LA PRUEBA: Verificar si existen políticas actualizadas para el acceso de usuarios y si cumplen su propósito.
RECURSOS NECESARIOS: Acceso a los servidores de la institución Políticas de la base de datos.
PROCEDIMIENTO A EMPLEAR: • Listado de usuarios en la institución. • Ver los logs de registro a la base. • Ver la cantidad de intentos que permite la base.

Fuente: Elaboración propia a partir de la Tabla 16

Tabla 18. Creación de usuarios y contraseñas para la base de datos

ENTORNO: Base de Datos **PRUEBA No:** P002 Creación de usuarios y contraseñas para la base de datos.
OBJETIVO DE LA PRUEBA: Verificar si existe políticas para la creación de usuarios y asignación de perfiles-
RECURSOS NECESARIOS: Acceso a los servidores de la institución. Políticas de la base de datos. Documentación para la asignación de perfiles.
PROCEDIMIENTO A EMPLEAR: • Listado de usuarios asociados con el área de desarrollo. • Estándar para la asignación de usuario (Mayúsculas, minúsculas, caracteres especiales). • Estándar para la asignación de contraseñas (Mayúsculas, minúsculas, caracteres especiales). • Asignación de perfil.

Fuente: Elaboración propia a partir de la Tabla 16

Tabla 19. Selección de personal de tecnologías de la información

ENTORNO: Base de Datos **PRUEBA No:** P003 Selección de personal de tecnologías de la información.
OBJETIVO DE LA PRUEBA: Validar el proceso de selección de personal de TI y ver si cumple con los requisitos establecidos.
RECURSOS NECESARIOS: Acceso a los servidores de la institución Políticas de selección de personal. Contratos de los empleados del área. Pruebas técnicas realizadas a los empleados.
PROCEDIMIENTO A EMPLEAR: • Manual de contratación para las personas del departamento de Tecnologías de la Información. • Ejecución de pruebas técnicas.

Fuente: Elaboración propia a partir de la Tabla 16

Tabla 20. Documentación de procesos de base de datos entregada al personal

ENTORNO: Base de Datos **PRUEBA No:** P004 Documentación de procesos de base de datos entregada al personal.
OBJETIVO DE LA PRUEBA: Validar si la documentación entregada al personal está actualizada y si este cumple con el procedimiento estipulado para el manejo adecuado de la BDD.
RECURSOS NECESARIOS: Políticas para el nuevo personal.
PROCEDIMIENTO A EMPLEAR: • Documentación de la base de datos. • Ejecución de la documentación.

Fuente: Elaboración propia a partir de la Tabla 16

Tabla 21. Estabilidad de la base de datos en transacciones información (rollback)

ENTORNO: Base de Datos **PRUEBA No:** P005 Estabilidad de la base de datos en transacciones información (rollback).
OBJETIVO DE LA PRUEBA: Verificar el proceso de recuperación de información de la base de datos, cuando accidentalmente se elimina un dato.
RECURSOS NECESARIOS: Acceso a los servidores de la institución. Procedimientos para recuperación de información.
PROCEDIMIENTO A EMPLEAR: • Listado de procesos para recuperación de información.

Fuente: Elaboración propia a partir de la Tabla 16

Tabla 22. Recuperación de Información(backups)

ENTORNO: Base de Datos **PRUEBA No:** P006 Recuperación de Información(backups).
OBJETIVO DE LA PRUEBA: Verificar el proceso de recuperación de información de la base de datos, cuando es eliminada accidentalmente.
RECURSOS NECESARIOS: Acceso a los servidores de la institución. Procedimientos para recuperación de información.
PROCEDIMIENTO A EMPLEAR: • Proceso de creación de backups. • Listado de los procesos a los cuales se realiza backups. • Listado de cada cuando tiempo se realizan los backups. • Almacenamientos de los backups en condiciones óptimas. • Pruebas periódicas de los Backups (restore)

Fuente: Elaboración propia a partir de la Tabla 16

Tabla 23. Control de cambios en la estructura de la base de datos

ENTORNO: Base de Datos **PRUEBA No:** P007 Control de cambios en la estructura de la base de datos.
OBJETIVO DE LA PRUEBA: Validar el proceso de control de cambios establecidos para la base de datos.
RECURSOS NECESARIOS: Acceso a los servidores de la institución. Políticas de la base de datos.
PROCEDIMIENTO A EMPLEAR: • Manual para la generación de cambios. • Documentación de los cambios realizados.

Fuente: Elaboración propia a partir de la Tabla 16

Tabla 24. Control de duplicidad de información

ENTORNO: Base de Datos **PRUEBA No:** P008 Control de duplicidad de información.
OBJETIVO DE LA PRUEBA: Verificar el proceso adecuado para evitar la duplicidad de información en la institución.
RECURSOS NECESARIOS: Acceso a los servidores de la institución. Proceso de la estructura de las tablas de la base de datos.
PROCEDIMIENTO A EMPLEAR: • Manual de creación de tablas. • Estructura de la base de datos. • Creación de claves primarias.

Fuente: Elaboración propia a partir de la Tabla 16

Tabla 25. Estándares de nomenclatura al momento de creación de tablas

ENTORNO: Base de Datos **PRUEBA No:** P009 Estándares de nomenclatura al momento de creación de tablas.
OBJETIVO DE LA PRUEBA: Verificar el proceso adecuado para la creación de tablas.
RECURSOS NECESARIOS: Acceso a los servidores de la institución. Políticas de la base de datos.

PROCEDIMIENTO A EMPLEAR • Manual de creación de tablas.

Fuente: Elaboración propia a partir de la Tabla 16

Redes y Comunicaciones

Tabla 26. Comprobar la seguridad configurada en el software VNC para acceso remoto al sistema CABILDO

ENTORNO: Redes y Comunicaciones **PRUEBA No:** P010 Comprobar la seguridad configurada en el software VNC para acceso remoto al sistema CABILDO.
OBJETIVO DE LA PRUEBA: Validar la configuración de seguridad del software utilizado para la conexión remota VNC.
RECURSOS NECESARIOS: Acceso a los servidores. Documentación del programa VNC.
PROCEDIMIENTO A EMPLEAR: • Listado de los usuarios que tienen acceso remoto por VNC. • Configuraciones de seguridad del programa VNC. • Listado de configuraciones del checkpoint para los permisos.

Fuente: Elaboración propia a partir de la Tabla 16

Tabla 27. Acceso físico de las personas que ingresan a las instalaciones de servidores y que trabajos se disponen a realizar

ENTORNO: Redes y Comunicaciones **PRUEBA No:** P011 Acceso físico de las personas que ingresan a las instalaciones de servidores y que trabajos se disponen a realizar.
OBJETIVO DE LA PRUEBA: Comprobar la seguridad al otorgar acceso a las personas a las instalaciones.
RECURSOS NECESARIOS: Documentación de procesos Acceso a los servidores de la institución.
PROCEDIMIENTO A EMPLEAR: • Minuta de acceso de visitantes. • Registro de visitas. • Listado de los lugares a los que tienen acceso.

Fuente: Elaboración propia a partir de la Tabla 16

Tabla 28. Integridad del cableado estructurado

ENTORNO: Redes y Comunicaciones **PRUEBA No:** P012 Integridad del cableado estructurado.
OBJETIVO DE LA PRUEBA: Comprobar la infraestructura del cableado estructurado instalado en las oficinas de la compañía.
RECURSOS NECESARIOS: Documentación del cableado estructurado.
PROCEDIMIENTO A EMPLEAR: • Planos del cableado estructurado instalado en la institución. • Distancia del cableado que se mantiene en los equipos.

Fuente: Elaboración propia a partir de la Tabla 16

Tabla 29. Configuración del firewall por parte del proveedor

ENTORNO: Redes y Comunicaciones **PRUEBA No:** P013 Configuración del firewall por parte del proveedor.
OBJETIVO DE LA PRUEBA: Comprobar la seguridad al otorgar acceso a las personas a las instalaciones.
RECURSOS NECESARIOS: Documentación de las políticas en el firewall
PROCEDIMIENTO A EMPLEAR: • Configuración del firewall. • Listado de acceso a páginas de internet.

Fuente: Elaboración propia a partir de la Tabla 16

Tabla 30. Protocolos habilitados para el manejo de aplicaciones

ENTORNO: Redes y Comunicaciones **PRUEBA No:** P014 Protocolos habilitados para el manejo de aplicaciones.
OBJETIVO DE LA PRUEBA: Comprobar los protocolos con los que trabajan en el GAD de Ambato.
RECURSOS NECESARIOS: Documentación de los protocolos.
PROCEDIMIENTO A EMPLEAR:

• Listado de las aplicaciones. • Listado de protocolos utilizados. • Manual de utilización de protocolos.

Fuente: Elaboración propia a partir de la Tabla 16

Tabla 31. Seguridad del checkpoint

ENTORNO: Redes y Comunicaciones **PRUEBA No:** P015 Seguridad del checkpoint.
OBJETIVO DE LA PRUEBA: Comprobar la seguridad del checkpoint para evitar ataques.
RECURSOS NECESARIOS: Documentación del checkpoint.
PROCEDIMIENTO A EMPLEAR: • Políticas del checkpoint. • Listado de personas encargadas del manejo del checkpoint. • Listado de las reglas empleadas en el checkpoint.

Fuente: Elaboración propia a partir de la Tabla 16

Tabla 32. Encriptación de información

ENTORNO: Redes y Comunicaciones. **PRUEBA No:** P016 Encriptación de información.
OBJETIVO DE LA PRUEBA: Verificar si la información que viaja a través de la red es encriptada.
RECURSOS NECESARIOS: Procesos del manejo de la información.
PROCEDIMIENTO A EMPLEAR: • Proceso del manejo de información. • Tipo de encriptación utilizada en la institución.

Fuente: Elaboración propia a partir de la Tabla 16

Seguridad Lógica

Tabla 33. Logs de la base de datos

ENTORNO: Seguridad Lógica. **PRUEBA No:** P017 Logs de la base de datos.
OBJETIVO DE LA PRUEBA: Revisar los logs para confirmar que los backups se estén realizando en los tiempos estipulados, que cambios se realizó.
RECURSOS NECESARIOS: Acceso a los servidores de la institución. Procesos de los logs.
PROCEDIMIENTO A EMPLEAR: • Proceso de creación de logs. • Listado de los procesos a los cuales se realiza logs. • Listado de cada cuando tiempo se realizan los logs.

Fuente: Elaboración propia a partir de la Tabla 16

Tabla 34. Software instalado en los equipos de cómputo

ENTORNO: Seguridad Lógica. **PRUEBA No:** P018 Software instalado en los equipos de cómputo.
OBJETIVO DE LA PRUEBA: Revisar si el software instalado consta con las licencias respectivas.
RECURSOS NECESARIOS: Acceso a los servidores de la institución. Políticas del software adquirido.
PROCEDIMIENTO A EMPLEAR: • Listado de software adquiridos en la institución. • Manual del software. • Licencia del software.

Fuente: Elaboración propia a partir de la Tabla 16

Tabla 35. Verificar las licencias del software instalado en los equipos de cómputo cliente

ENTORNO: Seguridad Lógica. **PRUEBA No:** P019 Verificar las licencias del software instalado en los equipos de cómputo cliente.
OBJETIVO DE LA PRUEBA: Verificar que el software instalado en la institución se encuentra licenciado.
RECURSOS NECESARIOS: Acceso a los servidores de la institución. Listado del software instalado.
PROCEDIMIENTO A EMPLEAR: • Listado del software autorizado para el manejo de la institución. • Listado de las licencias de cada software instalado en los equipos. • Listado de la cantidad de licencias adquiridas con respecto a la cantidad de equipos o usuarios que hacen uso de este software. • Listado del tiempo de vigencia de las licencias.

Fuente: Elaboración propia a partir de la Tabla 16

Tabla 36. Eliminación de archivos temporales y obsoletos

ENTORNO: Seguridad Lógica. **PRUEBA No:** P020 Eliminación de archivos temporales y obsoletos.
OBJETIVO DE LA PRUEBA: Verificar los pasos necesarios para la liberación de espacio en los servidores de la institución.
RECURSOS NECESARIOS: Procesos para la eliminación de información.
PROCEDIMIENTO A EMPLEAR: • Listado de documentos o procedimientos para la liberación de espacio y eliminación de archivos obsoletos.

Fuente: Elaboración propia a partir de la Tabla 16

Tabla 37. Creación de usuarios y contraseñas del sistema Cabildo

ENTORNO: Seguridad Lógica. **PRUEBA No:** P021 Creación de usuarios y contraseñas del sistema Cabildo.
OBJETIVO DE LA PRUEBA: Comprobar el procedimiento para la creación de usuarios para el sistema Cabildo.
RECURSOS NECESARIOS: Documentación para la creación de usuarios.
PROCEDIMIENTO A EMPLEAR: • Listado de usuarios asociados con el área de desarrollo. • Estándar para la asignación de usuario (Mayúsculas, minúsculas, caracteres especiales). • Estándar para la asignación de contraseñas (Mayúsculas, minúsculas, caracteres especiales). • Asignación de perfil.

Fuente: Elaboración propia a partir de la Tabla 16

Tabla 38. Tipo de procedimiento de redundancia

ENTORNO: Seguridad Lógica. **PRUEBA No:** P022 Tipo de procedimiento de redundancia.
OBJETIVO DE LA PRUEBA: Verificar con qué tipo de raid utiliza la institución y porque motivo se utiliza ese raid.
RECURSOS NECESARIOS: Documentación del Raid. Acceso a los servidores.
PROCEDIMIENTO A EMPLEAR: • Documentación del tipo de raid se utiliza en la institución. • Verificar si la documentación entregada pertenece al raid de la institución.

Fuente: Elaboración propia a partir de la Tabla 16

Tabla 39. Comprobación de los antivirus

ENTORNO: Seguridad Lógica. **PRUEBA No:** P023 Comprobación de los antivirus.
OBJETIVO DE LA PRUEBA: Verificar que los antivirus de la institución se encuentren actualizados.
RECURSOS NECESARIOS: Contratos de los antivirus.
PROCEDIMIENTO A EMPLEAR: • Documentación del antivirus. • Registro de la licencia del antivirus.

Fuente: Elaboración propia a partir de la Tabla 16

Tabla 40. Administración de los dispositivos de almacenamiento de los backups

ENTORNO: Seguridad Lógica. **PRUEBA No:** P024 Administración de los dispositivos de almacenamiento de los backups
OBJETIVO DE LA PRUEBA: Verificar que los antivirus de la institución se encuentren actualizados.
RECURSOS NECESARIOS: Documentación de dispositivo utilizados en la institución.
PROCEDIMIENTO A EMPLEAR: • Listado de medios magnéticos utilizados. • Etiquetas para definir contenido y nivel de seguridad. • Registro de etiquetado.

Fuente: Elaboración propia a partir de la Tabla 16

Seguridad Física

Tabla 41. Sistemas de vigilancia (Cámaras)

ENTORNO: Seguridad Física. **PRUEBA No:** P025 Sistemas de vigilancia (Cámaras)
OBJETIVO DE LA PRUEBA: Verificar el funcionamiento de las cámaras instaladas en la institución.
RECURSOS NECESARIOS: Políticas de las cámaras. Respaldos de la información de las cámaras.
PROCEDIMIENTO A EMPLEAR: • Manual de las cámaras de vigilancia. • Inventario de las cámaras de vigilancia implementados en la institución. • Planos de la ubicación de los sistemas de vigilancia. • Documentación de cada cuanto se elimina la información almacenada.

Fuente: Elaboración propia a partir de la Tabla 16

Tabla 42. Seguridad del sistema biométrico

ENTORNO: Seguridad Física. **PRUEBA No:** P026 Seguridad del sistema biométrico.
OBJETIVO DE LA PRUEBA: Verificar las políticas de los sistemas biométricos.
RECURSOS NECESARIOS: Políticas de los sistemas biométricos. Respaldo de la información de los sistemas biométricos.
PROCEDIMIENTO A EMPLEAR: • Manual de los sistemas biométricos. • Inventario de los sistemas biométricos implementados en la institución. • Planos de la ubicación de los sistemas biométricos.

Fuente: Elaboración propia a partir de la Tabla 16

Tabla 43. Contratos de los empleados de seguridad

ENTORNO: Seguridad Física. **PRUEBA No:** P027 Contratos de los empleados de seguridad
OBJETIVO DE LA PRUEBA: Verificar el listado de empleados en el departamento de seguridad.
RECURSOS NECESARIOS: Contratos de los empleados.
PROCEDIMIENTO A EMPLEAR: • Listado de los empleados de seguridad. • Listado del personal activo. • Contratos del personal.

Fuente: Elaboración propia a partir de la Tabla 16

Tabla 44. Contraseñas de acceso a la BIOS

ENTORNO: Seguridad Física. **PRUEBA No:** P028 Contraseñas de acceso a la BIOS.
OBJETIVO DE LA PRUEBA: Verificar si los equipos del municipio constan con contraseñas al momento de ingresar a la BIOS.
RECURSOS NECESARIOS: Documentación de los equipos.
PROCEDIMIENTO A EMPLEAR: • Inventario de los equipos de la institución. • Características de los equipos. • Listado de las configuraciones de la Bios.

Fuente: Elaboración propia a partir de la Tabla 16

Tabla 45. Verificación de los UPS

ENTORNO: Seguridad Física. **PRUEBA No:** P029 Verificación de los UPS.
OBJETIVO DE LA PRUEBA: Verificar el tiempo de duración de los ups adquiridos en la institución.
RECURSOS NECESARIOS: Documentación de los UPS adquiridos. Requerimientos de los UPS.
PROCEDIMIENTO A EMPLEAR: • Manuales de los UPS de la institución. • Inventario de los UPS. • Planos de la ubicación de los UPS.

Fuente: Elaboración propia a partir de la Tabla 16

Tabla 46. Verificar el acceso al datacenter

ENTORNO: Seguridad Física. **PRUEBA No:** P030 Verificar el acceso al datacenter.
OBJETIVO DE LA PRUEBA: Verificar que los elementos de oficina entregados a los empleados son acordes a sus labores diarias.
RECURSOS NECESARIOS: Documentación del datacenter.
PROCEDIMIENTO A EMPLEAR: • Control Biométrico. • Monitoreo de cámaras. • Acceso remoto mediante VPN. • Teamviwer.

Fuente: Elaboración propia a partir de la Tabla 16

3.1.2.4 Ejecución de pruebas del Sistema Cabildo

Desarrollar las pruebas planteadas para obtener información destacada las cual nos permita conocer la documentación existente en cada área; como se podrá evidenciar en las siguientes tablas.

Base de Datos

Tabla 47. Ejecución de acceso de los usuarios a la base de datos.

Prueba 001	Acceso de los usuarios a la base de datos.		
Actividad	**Descripción de Actividad**	**Validación**	**Observación**
1) Listado de usuarios en la institución.	Verificación de los usuarios que pertenecen y que están activos en la institución.	Cumple	El listado de personas que trabajan en el municipio es manejado por el personal de recursos humanos.
2) Ver los logs de registro a la base.	Evidenciar los usuarios que acceden a la base de datos.	No cumple	Se requiere obtener un registro de logs el cual ayudara a evidenciar los usuarios que desean ingresar a la base de datos.

Fuente: Elaboración propia a partir de la Tabla 17. Acceso de los usuarios a la base de datos

Mediante la Prueba001 realizada se pudo evidenciar que se mantiene un listado de los usuarios la cual es manejada por el área de Talento Humano, también se pudo evidenciar que no cuentan con un log de registro el cual ayudara a mantener un registro de ingreso a la base de datos.

Tabla 48. Ejecución de creación de usuarios y contraseñas a nivel de base de datos

Prueba 002	Creación de usuarios y contraseñas a nivel de base de datos.		
Actividad	**Descripción de Actividad**	**Validación**	**Observación**
1)Listado de usuarios asociados con el área de desarrollo.	Verificación de los usuarios que pertenecen y que están activos en el área de tecnologías de la información.	Cumple	El listado de personas que trabajan en el área de desarrollo es manejado por el personal de recursos humanos.
2) Estándar para la asignación de usuario (Mayúsculas, minúsculas, caracteres especiales).	Controlar si cumplen con ciertas normativas para la creación de usuarios.	No cumple	Se pudo evidenciar que al momento de la asignación de usuarios no cuentan con un estándar el cual ayudaría a manejar una asignación adecuada.
3) Estándar para la asignación de contraseñas (Mayúsculas, minúsculas, caracteres especiales).	Controlar si cumplen con ciertas normativas para la creación de contraseñas.	No cumple	Se pudo observar que las contraseñas asignadas no cumplen con un estándar adecuado ya que pueden ser asignadas al azar.
4) Asignación de perfil.	Evidenciar si al momento de la creación de los usuarios existe la asignación de perfiles de trabajos.	No cumple	Al momento de la asignación de perfiles no se cumple con un proceso adecuado.

Fuente: Elaboración propia a partir de la Tabla 18. Creación de usuarios y contraseñas para la base de datos

Mediante la Prueba002 realizada se pudo evidenciar que al momento de la creación de usuarios no cuentan con un estándar para la asignación de usuarios y contraseñas, el problema más notorio fue que no cumplen con un proceso adecuado para la asignación de perfiles.

Tabla 49. Ejecución de selección de personal de tecnologías de la información

Prueba 003	Selección de personal de tecnologías de la información.		
Actividad	**Descripción de Actividad**	**Validación**	**Observación**
1) Manual de contratación para las personas del departamento de Tecnologías.	Evidenciar los pasos que se deben cumplir para la contratación del nuevo personal de tecnologías de la información.	No cumple	No se pudo obtener información la cual ayude a realizar la prueba.
2) Ejecución de pruebas técnicas.	Comprobar si se cumple las pruebas técnicas establecidas en el área.	No cumple	No se realizan pruebas técnicas.

Fuente: Elaboración propia a partir de la Tabla 19. Selección de personal de tecnologías de la información

Mediante la Prueba003 se pudo observar que en el departamento de Tecnologías de la Información no cuentan con un manual de contratación para el nuevo personal, también no cuentan se realizan pruebas técnicas.

Tabla 50. Ejecución de documentación de procesos de base de datos entregada al personal

Prueba 004	Documentación de procesos de base de datos entregada al personal.		
Actividad	**Descripción de Actividad**	**Validación**	**Observación**
1) Documentación de la base de datos.	Evidenciar las características e información de la base de datos.	No cumple	No se tiene documentación la cual ayude a entender las funciones de la base de datos.
2) Ejecución de la documentación.	Comprobar que la información adquirida es verdadera.	No cumple	No se puede ejecutar la documentación de la base de datos por carencia de documentación.

Fuente: Elaboración propia a partir de la Tabla 20. Documentación de procesos de base de datos entregada al personal

Mediante la Prueba004 realizada se pudo evidenciar que al ingresar un nuevo empleado encargado de la base de datos no se cuenta con documentación pertinente acerca de la base de datos, la cual ayudaría a conocer los procesos adecuados del manejo.

Tabla 51. Ejecución de estabilidad de la base de datos en transacciones información (rollback)

Prueba 005	Estabilidad de la base de datos en transacciones información (rollback).		
Actividad	**Descripción de Actividad**	**Validación**	**Observación**
1) Listado de procesos para recuperación de información.	Métodos que ayuden a recuperar información de manera instantánea.	No cumple	No se cuenta con documentación pertinente la cual nos ayude a recuperar información en caso de pérdida o eliminación.

Fuente: Elaboración propia a partir de la Tabla 21. Estabilidad de la base de datos en transacciones información (rollback)

Mediante la Prueba005 realizada se pudo presenciar que no cuentan con un listado de procesos para recuperación de información.

Tabla 52. Ejecución de recuperación de Información(backups)

Prueba 006	Recuperación de Información(backups).		
Actividad	**Descripción de Actividad**	**Validación**	**Observación**
1) Proceso de creación de backups.	Pasos que se deben cumplir para el respaldo de información.	No cumple	No se cuenta con un manual el cual pueda detallar los pasos que se deben cumplir.
2) Listado de los procesos a los cuales se realiza backups.	Registro de los procesos a los que se realizaran backups, dependiendo la	No cumple	Carencia de documentación de los procesos a cuáles se realizan backups.

	importancia de la información.		
3) Listado de cada cuando tiempo se realizan los backups.	Historial de cada cuanto tiempo se realiza los backups.	No cumple	Inexistencia de documentación de cada cuanto tiempo se realizan los backups.

Fuente: Elaboración propia a partir de la Tabla 22. Recuperación de Información(backups)

Mediante la Prueba006 realizada se pudo presenciar que no cuentan con un manual para la recuperación de información, tampoco cuentan con documentación la cual pueda sustentar los procesos a los cuales se realizan los backups y cada cuanto tiempo se realiza las copias de información.

Tabla 53. Ejecución de control de cambios en la estructura de la base de datos

Prueba 007	Control de cambios en la estructura de la base de datos.		
Actividad	**Descripción de Actividad**	**Validación**	**Observación**
1) Manual para la generación de cambios.	Pasos que se deberán seguir para poder generar los cambios necesarios.	No cumple	No cuenta con un manual el cual les ayude a seguir un proceso adecuado.
2) Documentación de los cambios realizados.	Evidenciar la lista de información realizados en la base de datos.	No cumple	Lo cambios solicitados son de manera verbal, no cuentan con documentación la cual ayude a respaldar los cambios realizados.

Fuente: Elaboración propia a partir de la Tabla 23. Control de cambios en la estructura de la base de datos

Mediante la Prueba007 realizada se pudo presenciar que no cuentan con un Manual de cambios el cual ayude a entender el proceso que deben seguir cada vez que se realiza un cambio en la estructura de la base de datos, por otra parte, se pudo evidenciar que todos los cambios que se solicitan son de manera verbal por lo cual no cuentan con documentación la cual ayude a sustentar los cambios realizados, para mantener un control pertinente para la generación de cambios.

Tabla 54. Ejecución de control de duplicidad de información

Prueba 008	Control de duplicidad de información.		
Actividad	**Descripción de Actividad**	**Validación**	**Observación**
1) Manual de creación de tablas.	Pasos que se deberán seguir para la creación de tablas en la base de datos.	No cumple	No cumple con un manual el cual indique el proceso adecuado para la creación de tablas.
2) Estructura de la base de datos.	Esquema de la base de datos la cual nos facilita ver la estructura lógica y física de los datos obtenidos.	No cumple	No se cuenta con documentación de la estructura de la base de datos
3) Creación de clave primaria.	La clave primaria ayuda a evitar redundancia de información, se puede aplicar una clave primaria a una o a varias tablas, dependiendo la necesidad.	No cumple	Como no se cuenta con la estructura de la base de datos no se pudo evidenciar que atributo es la clave primeria en las tablas creadas.

Fuente: Elaboración propia a partir de la Tabla 24. Control de duplicidad de información

Mediante la Prueba008 realizada se pudo presenciar que no cuentan con un manual para la creación de tablas el cual pueda indicar los parámetros y normativas que se deben cumplir al momento de la creación, también se comprobó que no se cuenta con la documentación pertinente de la estructura de la base de datos mediante la cual se pueda evidenciar cuales son los atributos que manejan como claves primarias.

Tabla 55. Ejecución de estándares de nomenclatura al momento de creación de tablas

Prueba 009	Estándares de nomenclatura al momento de creación de tablas.		
Actividad	**Descripción de Actividad**	**Validación**	**Observación**
1) Manual de creación de tablas	Pasos que se deberán seguir para la creación de tablas, en la cual debe estar detallada la nomenclatura que se utiliza.	No cumple.	No cumple con un manual el cual indique el proceso adecuado para la creación de tablas.

Fuente: Elaboración propia a partir de la Tabla 25. Estándares de nomenclatura al momento de creación de tablas

Mediante la Prueba009 realizada se pudo presenciar que no cuentan con un manual para la creación de tablas el cual pueda indicar los parámetros y estándares que se deben cumplir al momento de la creación.

Redes y Comunicación

Tabla 56. Ejecución de comprobar la seguridad configurada en el software VNC para acceso remoto al Sistema CABILDO

Prueba 010	Comprobar la seguridad configurada en el software VNC para acceso remoto al sistema CABILDO.		
Actividad	**Descripción de Actividad**	**Validación**	**Observación**
1) Listado de los equipos que tienen acceso remoto por VNC.	Inventario de los equipos que cuentan con la aplicación VNC, para el acceso remoto.	No cumple.	Todos los equipos del municipio cuentan con el programa VNC.
2) Configuraciones de seguridad del programa VNC.	Pasos que se seguirán en la configuración de	No cumple.	No se tiene documentación de la configuración

	VNC, los cuales se basarán en seguridad.		del programa VNC.
3) Listado de configuraciones del checkpoint para los permisos.	Registro de los permisos utilizados para el manejo de la aplicación VNC, los cuales ayudaran al manejo del sistema Cabildo cuando se necesite.	Cumple.	Por motivos de seguridad no se puede obtener la documentación de las configuraciones del checkpoint.

Fuente: Elaboración propia a partir de la Tabla 26. Comprobar la seguridad configurada en el software VNC para acceso remoto al sistema CABILDO

Mediante la Prueba010 realizada se pudo presenciar que no cuentan con un manual de configuración de seguridad del programa VNC y por motivos de seguridad no se pudo acceder a las configuraciones del checkpoint para revisar los permisos con los que cuenta el sistema Cabildo.

Tabla 57. Ejecución de acceso físico de las personas que ingresan a las instalaciones de servidores y que trabajos se disponen a realizar

Prueba 011	Acceso físico de las personas que ingresan a las instalaciones de servidores y que trabajos se disponen a realizar.		
Actividad	**Descripción de Actividad**	**Validación**	**Observación**
1) Minuta de acceso de visitantes.	Documento elaborado por la institución, la cual ayuda a los guardias y empleados a saber que se está siguiendo el procedimiento adecuado para el ingreso de terceras personas.	Cumple.	Las minutas son entregadas el momento de ingresar a la institución por los guardias de seguridad.

2) Listado de los lugares a los que tienen acceso.	Registro de los lugares a los que los usuarios pueden tener acceso mediante la minuta entregada.	Cumple.	Se cuenta con una hoja de registro en la cual le solicitan que
3) Documentación de permiso a los servidores.	Documentos que validan el permiso para que terceras personas puedan acceder a los servidores.	No cumple.	Se manifiesta que los permisos son de manera verbal que se les otorga a las personas que vayan a realizar trabajos en los servidores.

Fuente: Elaboración propia a partir de la Tabla 27. Acceso físico de las personas que ingresan a las instalaciones de servidores y que trabajos se disponen a realizar

Mediante la Prueba011 realizada se pudo presenciar que para el acceso a los servidores se trabaja conjuntamente con el área de seguridad física la cual es la encargada de dar los permisos a las personas que ingresan a la institución.

Tabla 58. Ejecución de integridad del cableado estructurado

Prueba 012	Integridad del cableado estructurado.		
Actividad	**Descripción de Actividad**	**Validación**	**Observación**
1) Planos del cableado estructurado instalado en la institución.	Documentación del tipo de cableado utilizado en la institución y los lugares en los que fueron instalados.	No cumple.	No se tiene planos en los cuales se pueda evidenciar el cableado actual de la institución.

Fuente: Elaboración propia a partir de la Tabla 28. Integridad del cableado estructurado

Mediante la Prueba012 realizada se pudo presenciar que no cumplen con planos en el cual se pueda evidenciar el cableado de los equipos en la institución.

Tabla 59. Ejecución de configuraciones del firewall por parte del proveedor

Prueba 013	Configuraciones del firewall por parte del proveedor.		
Actividad	**Descripción de Actividad**	**Validación**	**Observación**
1) Configuración del firewall.	Pasos que se seguirán en la configuración del firewall utilizado en la institución.	No cumple.	No se cuentan con documentación pertinente en la cual se establezca la configuración del firewall.
2) Listado de acceso a páginas de internet.	Registro de páginas permitidas en la institución, a las cuales se puede acceder dependiendo su cargo y los permisos que tengan.	No cumple.	No se tiene un listado en el cual se pueda evidenciar las paginas restringidas.

Fuente: Elaboración propia a partir de la Tabla 29. Configuración del firewall por parte del proveedor

Mediante la Prueba013 ejecutada se pudo presenciar que no cuentan con documentación pertinente para la configuración del firewall y tampoco se cuenta con un listado de las paginas restringidas.

Tabla 60. Ejecución de protocolos con los que trabajan las aplicaciones

Prueba 014	Protocolos con los que trabajan las aplicaciones.		
Actividad	**Descripción de Actividad**	**Validación**	**Observación**
1) Listado de las aplicaciones.	Registro de aplicaciones instaladas en la institución.	No cumple.	No cuentan con un listado de todas las aplicaciones instaladas en la institución.
2) Listado de protocolos utilizados.	Registro de los protocolos habilitados y que aplicación la utiliza.	No cumple.	No se tiene documentación de los protocolos que se manejan en la institución.

3) Manual de utilización de protocolos.	Documentación de los protocolos utilizados en las aplicaciones de la institución.	No cumple.	No se cuenta con documentación en la cual se establezca el manejo adecuado de los protocolos.

Fuente: Elaboración propia a partir de la Tabla 30. Protocolos habilitados para el manejo de aplicaciones

Mediante la Prueba014 ejecutada se pudo presenciar que no cuentan con un manual en la cual se establezca un listado de las aplicaciones utilizadas y del uso de los protocolos más seguros para el manejo de las aplicaciones, se solicita generar una política llamada Protocolos con los que trabajan las aplicaciones para el control de las aplicaciones.

Tabla 61. Ejecución de seguridad del checkpoint

Prueba 015	Seguridad del checkpoint.		
Actividad	**Descripción de Actividad**	**Validación**	**Observación**
1) Manual del checkpoint.	Documentación y ventajas del manejo adecuado del checkpoint.	No cumple.	No se puede obtener documentación del checkpoint.
2) Listado de personas encargadas del manejo del checkpoint.	Registro de las personas encargadas, para el manejo del checkpoint.	No cumple.	No existe un listado en el cual se pueda ver las personas que tienen acceso al checkpoint.
3) Listado de las reglas empleadas en el checkpoint.	Registro de las reglas generadas por parte de las personas encargadas del manejo del checkpoint.	No cumple.	No se puede obtener las reglas generadas en la institución por motivos de seguridad.

Fuente: Elaboración propia a partir de la Tabla 31. Seguridad del checkpoint

Mediante la Prueba015 ejecutada se pudo presenciar que no cuentan con un manual del checkpoint y un listado de las personas encargadas del manejo, por motivos de seguridad no se puede obtener las reglas del checkpoint por motivos de seguridad, se recomienda generar una política llamada Seguridad del checkpoint la cual ayude a manejar la documentación correcta del checkpoint.

Tabla 62. Ejecución de encriptación de información

Prueba 016	Encriptación de información.		
Actividad	**Descripción de Actividad**	**Validación**	**Observación**
1) Proceso del manejo de información.	Pasos que ayudaran a salvaguardar la información manejada.	No cumple	No se cuenta con documentación necesaria la cual ayude a entender el manejo de información.
2) Tipo de encriptación utilizada en la institución.	Metodología empleada para el manejo de encriptación de información.	No cumple	No se conoce si utilizan tipo de encriptación en la institución.

Fuente: Elaboración propia a partir de la Tabla 32. Encriptación de información

Mediante la Prueba016 ejecutada se pudo presenciar que no cuentan con un manual acerca de la encriptación de información, se pudo observar que no se cuenta con un proceso y con métodos de encriptación para el manejo de información.

Seguridad Lógica

Tabla 63. Ejecución de logs de la base de datos

Prueba 017	Logs de la base de datos.		
Actividad	**Descripción de Actividad**	**Validación**	**Observación**
1) Proceso de creación de logs.	Pasos que se seguirán para la creación de los logs.	No cumple	No se cuenta con documentación en la cual se pueda determinar el proceso adecuado de los logs.
2) Listado de los procesos a los cuales se realiza logs.	Registro de logs realizados en la institución, dependiendo la importancia.	No cumple	Carencia de registros de los logs que se crean.

3) Listado de cada cuando tiempo se realizan los logs.	Registro de cada cuanto tiempo se realizan los logs, pueden ser diarios, semanales o mensuales.	No cumple	Inexistencia de un registro en el cual se pueda observar cada cuanto tiempo se realizan los logs.

Fuente: Elaboración propia a partir de la Tabla 33. Logs de la base de datos

Mediante la Prueba017 ejecutada se pudo presenciar que no cuentan con un manual acerca del proceso adecuado de la creación de logs ni mucho menos cuentan con un tiempo establecido de la realización de los logs.

Tabla 64. Ejecución de software instalado en los equipos de cómputo

Prueba 018	Software instalado en los equipos de cómputo.		
Actividad	**Descripción de Actividad**	**Validación**	**Observación**
1) Listado de software adquiridos en la institución.	Registro del software utilizado en la institución	No cumple.	No se cuenta con documentación del software adquirido en la institución.
2) Manual del software.	Documentación del software adquirido y empleado.	No cumple.	La mayoría del software utilizado en la institución no cuenta con documentación pertinente.
3) Licencia del software.	Registro de las licencias y el tiempo de vigencia.	Cumple	Ninguna

Fuente: Elaboración propia a partir de la Tabla 34. Software instalado en los equipos de cómputo

Mediante la Prueba018 ejecutada se pudo presenciar que no cuentan con un listado del software adquirido y mucho menos cuentan con sus manuales de usabilidad.

Tabla 65. Ejecución de licencias del software instalado en los equipos de cómputo cliente

Prueba 019	Licencias del software instalado en los equipos de cómputo cliente.		
Actividad	**Descripción de Actividad**	**Validación**	**Observación**
1) Listado del software autorizado para el manejo de la institución.	Registro del software utilizado en la institución	No cumple.	No se cuenta con un listado del software en el cual se pueda visualizar que software es manejado en la institución.
2) Listado de las licencias de cada software instalado en los equipos.	Registro de las licencias y el tiempo de vigencia.	No cumple.	No se cuenta con un registro de la vigencia y la cantidad de licencias adquiridas.
3) Listado de la cantidad de licencias adquiridas con respecto a la cantidad de equipos o usuarios que hacen uso de este software.	Comparación de las licencias con el numero adecuado de máquinas que se utilizan en la institución	No cumple.	No se cuenta con un registro de la cantidad de las licencias adquiridas en la institución.
4) Listado del tiempo de vigencia de las licencias.	Registro del tiempo de utilización del software en los equipos.	No cumple.	No se registró documentación en la cual se pueda evidenciar el tiempo de vigencia de las licencias.

Fuente: Elaboración propia a partir de la Tabla 35. Verificar las licencias del software instalado en los equipos de cómputo cliente

Mediante la Prueba019 ejecutada se pudo presenciar que no cuentan con un registro de las licencias adquiridas en la institución, también se pudo visualizar que no se tiene un listado del software.

Tabla 66. Ejecución de eliminación de archivos temporales y obsoletos

Prueba 020	Eliminación de archivos temporales y obsoletos.		
Actividad	**Descripción de Actividad**	**Validación**	**Observación**
1) Listado de documentos o procedimientos para la liberación de espacio y eliminación de archivos temporales y obsoletos.	Pasos que se deben seguir para la eliminación de archivos basuras u obsoletos, los cuales utilizan memoria en el equipo.	No cumple.	Se necesita crear un registro con las carpetas en las que se almacena información obsoleta.

Fuente: Elaboración propia a partir de la Tabla 36. Eliminación de archivos temporales y obsoletos

Mediante la Prueba020 ejecutada se pudo presenciar que no cuentan con un procedimiento adecuado para la eliminación de archivos temporales y obsoletos, lo cual no ayuda a entender el proceso adecuado para la liberación de memoria.

Tabla 67. Ejecución de creación de usuarios y contraseñas del sistema Cabildo

Prueba 021	Creación de usuarios y contraseñas del sistema Cabildo.		
Actividad	**Descripción de Actividad**	**Validación**	**Observación**
1) Listado de usuarios asociados con el área de desarrollo.	Registro de los usuarios activos asociados en el área de desarrollo.	Cumple.	Ninguna
2) Estándar para la asignación de usuario (Mayúsculas, minúsculas, caracteres especiales).	Controlar si cumplen con ciertas normativas para la creación de usuarios.	No cumple.	Se cuenta con un estándar el cual al momento de la creación de usuarios se toma en cuenta la primera letra de los nombres y apellidos y el año en el que ingresan a la institución, pero no está debidamente documentando.

3) Estándar para la asignación de contraseñas (Mayúsculas, minúsculas, caracteres especiales).	Controlar si cumplen con ciertas normativas para la creación de contraseñas.	No cumple.	No cuentan con un estándar para la creación de contraseñas, ya que por primera vez se les asigna la contraseña del 1 al 5.
4) Asignación de perfil.	Evidenciar si al momento de la creación de los usuarios existe la asignación de perfiles de trabajos.	No cumple.	No se tiene documentación en la cual se detalle el manejo de asignación de perfiles.

Fuente: Elaboración propia a partir de la Tabla 37. Creación de usuarios y contraseñas del sistema Cabildo

Mediante la Prueba021 ejecutada se pudo presenciar que no cuentan con un estándar para la creación de usuarios y contraseñas, pero esta no está documentada de la manera adecuada.

Tabla 68. Ejecución de Tipo de procedimiento de redundancia

Prueba 022	Tipo de procedimiento de redundancia.		
Actividad	**Descripción de Actividad**	**Validación**	**Observación**
1) Documentación del tipo de raid se utiliza en la institución.	Manual del tipo de raid utilizado en la institución, el cual ayudara a respaldar información cuando un servidor sufra algún accidente.	No cumple.	No se cuenta con documentación la cual pueda ayudar a sustentar la documentación de Raid utilizada.
2) Verificar si la documentación entregada pertenece al raid de la institución.	Observar si la documentación entregada concuerda con el raid utilizado.	No cumple.	No se tiene acceso para la verificación del raid.

Fuente: Elaboración propia a partir de la Tabla 38. Tipo de procedimiento de redundancia

Mediante la Prueba022 ejecutada se pudo presenciar que no cuentan con documentación del Raid utilizada en la institución, la cual ayude a mantener la información en caso de pérdida.

Tabla 69. Ejecución de Comprobación de los antivirus

Prueba 023	Comprobación de los antivirus.		
Actividad	**Descripción de Actividad**	**Validación**	**Observación**
1) Documentación del antivirus.	Características del antivirus en donde se pueda constatar las ventajas.	Cumple.	Ninguna.
2) Registro de la licencia del antivirus.	Listado de la vigencia de los antivirus.	No cumple.	No se cuenta con documentación en la cual se pueda verificar el tiempo de vigencia de los antivirus.

Fuente: Elaboración propia a partir de la Tabla 39. Comprobación de los antivirus

Mediante la Prueba023 ejecutada se pudo presenciar que no cuentan con documentación la cual ayude a verificar el registro de las licencias de los antivirus, la cual facilite la visualización del estado actual del antivirus.

Tabla 70. Ejecución de Administración de los dispositivos de almacenamiento de los backups

Prueba 024	Administración de los dispositivos de almacenamiento de los backups.		
Actividad	**Descripción de Actividad**	**Validación**	**Observación**
1) Listado de medios magnéticos utilizados.	Registro de todos los dispositivos utilizados para el almacenamiento de backups.	No cumple.	No se cuenta con un registro de los listados magnéticos que se utilizan en la institución.

2) Etiquetas para definir contenido y nivel de seguridad.	Descripción del contenido y que tipo de seguridad merece ese dispositivo magnético.	No cumple.	No se puede constatar si cuentan con etiquetas por motivos de seguridad.
3) Registro de etiquetado.	Inventario de todos los dispositivos etiquetados.	No cumple.	No tienen un listado de los dispositivos magnéticos creados.

Fuente: Elaboración propia a partir de la Tabla 40. Administración de los dispositivos de almacenamiento de los backups

Mediante la Prueba024 ejecutada se pudo presenciar que no cuentan con procesos para el manejo de dispositivos de almacenamiento ni mucho menos cuentan con un listado del etiquetado que se tiene en la institución.

Seguridad Física

Tabla 71. Ejecución de Sistemas de vigilancia (Cámaras)

Prueba 025	Sistemas de vigilancia (Cámaras).		
Actividad	**Descripción de Actividad**	**Validación**	**Observación**
1) Manual de las cámaras de vigilancia.	Documentación de las cámaras instaladas en la institución.	No cumple.	No se pudo obtener información del manejo de las cámaras por motivo que el área de Tecnología de la Información no está asociada con el área de Seguridad Física.
2) Inventario de las cámaras de vigilancia implementados en la institución.	Registro de la cantidad de cámaras instaladas.	No cumple.	No se pudo obtener información del manejo de las cámaras por motivo que el área de Tecnología de la Información no está asociada con el área de Seguridad Física.
3) Planos de la ubicación de los	Documentación de la ubicación de las cámaras	No cumple.	No se pudo obtener información del manejo de las cámaras por motivo

sistemas de vigilancia.	en cada departamento.		que el área de Tecnología de la Información no está asociada con el área de Seguridad Física.
4) Documentación de cada cuanto se realiza backups de la información.	Listado de cada cuanto tiempo se realiza copias de la información.	No cumple.	No se pudo obtener información del manejo de las cámaras por motivo que el área de Tecnología de la Información no está asociada con el área de Seguridad Física.
5) Documentación de cada cuanto se elimina la información almacenada.	Listado de cada cuanto tiempo se elimina información obsoleta.	No cumple.	No se pudo obtener información del manejo de las cámaras por motivo que el área de Tecnología de la Información no está asociada con el área de Seguridad Física.

Fuente: Elaboración propia a partir de la Tabla 41. Sistemas de vigilancia (Cámaras)

Mediante la Prueba025 ejecutada se pudo presenciar que el departamento de Tecnologías de la Información no cuenta con información sobre el sistema de vigilancia de cámaras, ya que se supo manifestar que el encargado de dicho manejo es el departamento de Seguridad Física.

Tabla 72. Ejecución de seguridad del sistema biométrico

Prueba 026	Seguridad del sistema biométrico.		
Actividad	**Descripción de Actividad**	**Validación**	**Observación**
1) Manual de los sistemas biométricos.	Conocer las características y funcionalidades de los sistemas biométricos.	No cumple.	No se puede obtener documentación de los sistemas biométricos por que la información es manejada por el departamento de seguridad física.
2) Inventario de los sistemas biométricos	Listado de los sistemas	No cumple.	No se puede obtener documentación de los sistemas biométricos por

implementados en la institución.	implantados en la institución.		que la información es manejada por el departamento de seguridad física.
3) Planos de la ubicación de los sistemas biométricos.	Registro de la ubicación de todos los sistemas biométricos ubicados en todos los departamentos.	No cumple.	No se puede obtener documentación de los sistemas biométricos por que la información es manejada por el departamento de seguridad física.

Fuente: Elaboración propia a partir de la Tabla 42. Seguridad del sistema biométrico

Mediante la Prueba026 ejecutada se pudo presenciar que no cuentan con documentación de los sistemas biométricos y tampoco cuentan con planos para saber la ubicación de los sistemas implementados.

Tabla 73. Ejecución de contratos de los empleados de seguridad

Prueba 027	Contratos de los empleados de seguridad		
Actividad	**Descripción de Actividad**	**Validación**	**Observación**
1) Listado de los empleados de seguridad.	Registro de los empleados que trabajan en el área de seguridad.	No se conoce.	No se puede obtener documentación de los empleados de seguridad por motivos de permisos.
2) Listado del personal activo.	Registro del personal activo con el que cuenta la institución.	No se conoce.	No se puede obtener documentación de los empleados activos por motivos de permisos.
3) Contratos del personal.	Documentación de los contratos que se les entrega a los empleados.	No se conoce.	No se puede obtener documentación de los contratos del personal por motivos de permisos.

Fuente: Elaboración propia a partir de la Tabla 43. Contratos de los empleados de seguridad

Mediante la Prueba027 ejecutada se pudo presenciar que en el área de Tecnologías de la Información no se tiene documentación en la cual se pueda conocer como es el manejo del personal de seguridad, ya que esta el área de seguridad física es independiente.

Tabla 74. Ejecución de contraseñas de acceso a la BIOS

Prueba 028	Contraseñas de acceso a la BIOS.		
Actividad	**Descripción de Actividad**	**Validación**	**Observación**
1) Inventario de los equipos de la institución.	Registro de los equipos de la institución.	Cumple.	Ninguna
2) Características de los equipos.	Documentación de las características de la institución como, por ejemplo: Ram, sistema operativo.	Cumple.	Ninguna
3) Listado de las configuraciones de la Bios.	Documentación de la configuración de la Bios para la asignación de contraseñas.	No cumple.	No se cuenta con documentación la cual pueda servir para la asignación de contraseñas de la Bios.

Fuente: Elaboración propia a partir de la Tabla 44. Contraseñas de acceso a la BIOS

Mediante la Prueba028 ejecutada se pudo presenciar que los equipos no cuentan con contraseñas para el acceso a la Bios, lo cual ayudaría a tener un nivel más de seguridad en caso de que se quiera realizar acciones indebidas por terceras personas.

Tabla 75. Ejecución de Verificación de los UPS

Prueba 029	Verificación de los UPS.		
Actividad	**Descripción de Actividad**	**Validación**	**Observación**
1) Manuales de los UPS de la institución.	Documentación de los UPS acerca de su funcionalidad y características.	No cumple.	No se tiene documentación de los UPS.
2) Inventario de los UPS.	Listado de los UPS adquiridos en la institución.	No cumple.	No se tiene un inventario actualizado de los inventarios de los UPS.
3) Planos de la ubicación de los UPS.	Registro de la ubicación de todos los UPS ubicados en la institución.	No cumple.	No se cuenta con documentación la cual ayude a identificar la ubicación de los UPS.

Fuente: Elaboración propia a partir de la Tabla 45. Verificación de los UPS

Mediante la Prueba029 ejecutada se pudo presenciar que no cuentan con manuales de los UPS los cuales nos faciliten entender las características y usabilidad de estos, tampoco se puede saber específicamente el lugar en el que se encuentran ubicados.

Tabla 76. Ejecución de acceso al datacenter

Prueba 030	Acceso al datacenter.		
Actividad	**Descripción de Actividad**	**Validación**	**Observación**
1) Control Biométrico.	Acceso de seguridad el cual ayuda a controlar el ingreso del personal selecto para esa tarea.	No cumple.	Se cuenta con sistemas biométricos, pero no existe documentación la cual ayude a sustentar las características de los sistemas biométricos.
2) Monitoreo de cámaras.	Control de vigilancia el cual monitorea las actividades que se realizan en el datacenter.	No cumple.	Se cuenta con sistemas de cámaras, pero no existe documentación la cual ayude a sustentar las características de las cámaras.

3) Acceso remoto mediante VPN o Teamviwer.	Método de ingreso el cual ayuda a reiniciar o a emplear cierta actividad desde otro equipo de cómputo.	No cumple.	No se cuenta con documentación acerca del manejo del programa Teamviwer O VPN.

Fuente: Elaboración propia a partir de la Tabla 46. Acceso al datacenter

Mediante la Prueba030 ejecutada se pudo presenciar que existen sistemas biométricos y monitoreo de cámaras para el acceso al datacenter por otra parte no cuentan con documentación acerca del VPN o Teamviwer, lo cual genera una falencia de información.

Con la ejecución de las pruebas realizadas al sistema Cabildo se pudo evidenciar la carencia de información que presentan las áreas de Base de Datos, Redes y Comunicación, Seguridad Física y Seguridad Lógica, a continuación, las pruebas que hemos evaluado servirán para ser separadas en los diferentes principios de Cobit 5 dependiendo las características que cumplan y así poder culminar con el objetivo 2.

3.1.2.5 Aplicación de los principios COBIT 5.0

La metodología Cobit 5.0 cuenta con cinco principios los cuales fueron utilizados para clasificar las diferentes pruebas realizadas y poder separarlas dependiendo las características que cumplan; como se evidenciara en la Tabla 77.

Tabla 77. Pruebas realizadas dividas por Principios COBIT 5.0

Principios / **Pruebas**	**Principio 1. Satisfacer las Necesidades de las Partes Interesadas**	**Principio 2: Cubrir la Empresa Extremo-a-Extremo**	**Principio 3: Aplicar un Marco de Referencia único integrado**	**Principio 4: Hacer Posible un Enfoque Holístico**	**Principio 5: Separar el Gobierno de la Gestión**
PRUEBA No: P001 Acceso de los usuarios a la base de datos.	X	X		X	
PRUEBA No: P002 Creación de usuarios y contraseñas para la base de datos.	X	X		X	
PRUEBA No: P003 Selección de personal de tecnologías de la información.	X	X		X	
PRUEBA No: P004 Documentación de procesos de base de	X	X		X	

datos entregada al personal.					
PRUEBA No: P005 Estabilidad de la base de datos en transacciones información (rollback).	X	X		X	
PRUEBA No: P006 Recuperación de Información(backups).	X	X		X	
PRUEBA No: P007 Control de cambios en la estructura de la base de datos.	X	X		X	
PRUEBA No: P008 Control de duplicidad de información.	X	X		X	
PRUEBA No: P009 Estándares de nomenclatura al momento de creación de tablas.	X	X		X	
Redes y Comunicación					
PRUEBA No: P010	X	X		X	

Comprobar la seguridad configurada en el software para acceso remoto al sistema CABILDO.					
PRUEBA No: P011 Acceso de las personas que ingresan a las instalaciones y que trabajos se disponen a realizar en los servidores.	X	X		X	
PRUEBA No: P012 Integridad del cableado estructurado.	X	X		X	
PRUEBA No: P013 Configuración del firewall por parte del proveedor.	X	X		X	
PRUEBA No: P014 Protocolos con los que trabajan las aplicaciones.	X	X		X	
PRUEBA No: P015 Seguridad del checkpoint.	X	X		X	
PRUEBA No: P016	X	X		X	

Encriptación de información.					
Seguridad Lógica					
PRUEBA No: P017 Logs de la base de datos.	X	X		X	
PRUEBA No: P018 Software instalado en los equipos de cómputo.	X	X		X	
PRUEBA No: P019 Licencias del software instalado en los equipos de cómputo cliente.	X	X		X	
PRUEBA No: P020 Eliminación de archivos temporales y obsoletos.	X	X		X	
PRUEBA No: P021 Creación de usuarios y contraseñas del sistema Cabildo.	X	X		X	
PRUEBA No: P022 Tipo de procedimiento de redundancia.	X	X		X	

PRUEBA No: P023 Comprobación de los antivirus.	X	X		X	
PRUEBA No: P024 Administración de los dispositivos de almacenamiento de los backups.	X	X		X	
Seguridad Física					
PRUEBA No: P025 Sistemas de vigilancia (Cámaras).	X	X		X	
PRUEBA No: P026 Seguridad del sistema biométrico.	X	X		X	
PRUEBA No: P027 Contratos de los empleados de seguridad	X	X		X	
PRUEBA No: P028 Contraseñas de acceso a la BIOS.	X	X		X	
PRUEBA No: P029 Verificación de los UPS.	X	X		X	

PRUEBA No: P030 Acceso al datacenter.	X	X		X	

Fuente: Elaboración propia a partir de la Tabla 16. Listado de pruebas para el Sistema Cabildo

Los siguientes resultados se sintetizarán de manera global para poder tener un enfoque claro del por qué una prueba puede cumplir uno o varios principios de Cobit 5, como se mostró en la Tabla 77.

Principio 1. Satisfacer las Necesidades de las Partes Interesadas

Todas las pruebas generadas encajan al principio 1 debido a que cumplen con las necesidades de las partes externas e internas, la parte externa tiene que ver con sociedad en general, clientes, auditores externos, con la parte interna se refiere a la organización administrativa, las personas responsables de los procesos de negocios, auditores internos.

Principio 2: Cubrir la Empresa Extremo-a-Extremo

Todas las pruebas generadas encajan al principio 2 debido a que en este principio será controlado y manipulado por los roles de negocio, también serán utilizados y manejados por las distintos Actividades, roles y relaciones de las Tecnologías de la Información.

Principio 3: Aplicar un Marco de Referencia único integrado

Todas las pruebas generadas no cumplen con el principio 3 debido a que en el Departamento de Tecnologías de Información nunca se han generado pruebas las cuales ayuden a seguir un proceso adecuado, este principio podría cumplirse siempre y cuando existan pruebas anteriores las cuales se rijan a un estándar o a una norma.

Principio 4: Hacer Posible un Enfoque Holístico

1. Principios, políticas y marcos de referencia necesarios para poder cumplir y registrar las operaciones necesarias para el manejo del sistema Cabildo.
2. Procesos pasos adecuados para gestionar las Actividades de la TI relacionadas con el sistema Cabildo.
3. Estructuras organizativas definición de las responsabilidades de los roles asociadas en las Tecnologías de la Información las cuales estarán relacionadas con el sistema Cabildo.
4. Cultura, ética y comportamiento de los colaboradores y de la empresa, los cuales aportaran las pautas necesarias para el cumplimiento de las leyes, políticas y procedimientos internos los cuales ayudaran a la protección de información y de activos pertenecientes a los activos de Tecnologías de Información.
5. Información sustentable para el manejo de las partes interesadas las cuales ayudaran a demostrar la normativa ante personas externas, incluyendo situaciones judiciales.
6. Servicios, infraestructura y aplicaciones pertenecientes a la empresa las cuales proporcionan tecnologías para el proceso de información y servicios relacionados con el sistema Cabildo.
7. Personas, habilidades y competencias las cuales llevan a cabo la toma de acciones y de decisiones correctivas pertenecientes a Tecnologías de la Información.

Todas las pruebas empleadas cumplen con el principio 4, debido a que cada prueba cumple con las 7 categorías de catalizadores los cuales vienen planteadas en la metodología Cobit.

Principio 5: Separar el Gobierno de la Gestión

Las pruebas generadas van a cumplir con los principios de Gobierno ya que se Evaluará, Orientara y Supervisara las pruebas realizadas, por el contrario, no cumplirán con los principios de Gestión ya que no existe una parte encargada de Planificar ni de Construir estas políticas.

En conclusión, las pruebas realizadas no cumplirán el principio 5.

Con la ejecución y análisis de las pruebas planteadas al Sistema Cabildo se pudo aplicar con eficiencia los principios Cobit 5 y dividirlos dependiendo su categoría, lo cual ayudo a culminar de manera satisfactoria el segundo objetivo planteado en el presente trabajo.

3.1.2.6 Informe de la Auditoria

El presente informe realizado muestra la evaluación ejecutada al sistema Cabildo el cual es el encargado de la recaudación de bienes en la ciudad de Ambato, las áreas evaluadas fueron Base de Datos, Redes y Comunicación, Seguridad Lógica y Seguridad Física las cuales están vinculadas a dicho sistema de la institución del Gobierno Autónomo Descentralizado Municipal de Ambato.

De acuerdo con la auditoría realizada se pudo concluir que el Departamento de Tecnologías de la Información (TI) es la encarga del manejo de la información, la cual ayuda a tomar las decisiones en la institución. De esta manera se puede considerar que el Sistema Cabildo es el activo más importante de la institución.

Es por ello que mediante la auditoría realizada se trata de garantizar las normativas y procesos informáticos basándonos en la metodología Cobit para reducir los riesgos de la información. A continuación, se pondrá en consideración los hallazgos en el presente trabajo.

Base de Datos

Basándonos en el literal **3.1.2.1 Diseño y Ejecución de pruebas de Auditoria Informática** se encontró las siguientes falencias en el área de Base de Datos.

- No existen estándares para la asignación de usuarios y contraseñas.
- Carecen de asignación de perfiles.
- No manejan manuales de contratación.
- No tienen ejecución de pruebas técnicas.
- No manejan documentación de la base de datos.
- Carecen de listado de procesos para recuperación de información.
- Falta de procesos de creación de backups.
- No cuentan con manuales de generación de cambios.
- Carencia de manual de creación de tablas.
- No manejan estructura de la base de datos.

Redes y Comunicaciones

Basándonos en el literal **3.1.2.1 Diseño y Ejecución de pruebas de Auditoria Informática** se encontró las siguientes falencias en el área de Redes y Comunicaciones.

- Carencia de listado de los equipos que tienen acceso remoto por VNC.
- No manejan configuraciones de seguridad del programa VNC.
- Falta de listados de configuraciones del checkpoint para los permisos.
- No manejan planos del cableado estructurado instalado en la institución.
- No manipulan configuración del firewall.
- Carencia de listado de acceso a páginas de internet.
- No tienen listado de las aplicaciones.
- No cuentan con un listado de protocolos utilizados.
- No maneja un manual de utilización de protocolos.
- No existe manual del checkpoint.
- Carencia de listado de personas encargadas del manejo del checkpoint.
- Falta de listado de las reglas empleadas en el checkpoint.
- Inexistencia de proceso del manejo de información.
- Carencia de tipos de encriptación utilizada en la institución.

Seguridad Lógica

Basándonos en el literal **3.1.2.1 Diseño y Ejecución de pruebas de Auditoria Informática** se encontró las siguientes falencias en el área de Seguridad Lógica.

- Inexistencia de proceso de creación de logs.
- Falta de listado de los procesos a los cuales se realiza logs.
- Carencia de listado de cada cuando tiempo se realizan los logs.
- No tienen un listado de software adquiridos en la institución.
- No manejan un manual del software.
- Inexistencia de licencia del software.
- No manejan un listado del software autorizado para el manejo de la institución.
- No cuentan con un listado de las licencias de cada software instalado en los equipos.
- Carencia de listado de la cantidad de licencias adquiridas con respecto a la cantidad de equipos o usuarios que hacen uso de este software.

- Inexistencia de listado del tiempo de vigencia de las licencias.
- Falta de listado de documentos o procedimientos para la liberación de espacio y eliminación de archivos temporales y obsoletos.
- Carencia de estándar para la asignación de usuario (Mayúsculas, minúsculas, caracteres especiales).
- Carencia de estándar para la asignación de contraseñas (Mayúsculas, minúsculas, caracteres especiales).
- No tienen documentación del tipo de raid se utiliza en la institución.
- No cuentan con registro de la licencia del antivirus.
- Falta de un listado de medios magnéticos utilizados.
- Inexistencia de etiquetas para definir contenido y nivel de seguridad.
- Carencia de registro de etiquetado.

Seguridad Física

Basándonos en el literal **3.1.2.1 Diseño y Ejecución de pruebas de Auditoria Informática** se encontró las siguientes falencias en el área de Seguridad Física.

- Carencia de manual de las cámaras de vigilancia.
- Inexistencia de inventario de las cámaras de vigilancia implementados en la institución.
- Carencia de planos de la ubicación de los sistemas de vigilancia.
- Falta de documentación de cada cuanto se realiza backups de la información.
- Incumplimiento de documentación de cada cuanto se elimina la información almacenada.
- Carencia de manual de los sistemas biométricos.
- No cuentas con un inventario de los sistemas biométricos implementados en la institución.
- Falta de planos de la ubicación de los sistemas biométricos.
- Carencia de listados de las configuraciones de la Bios.
- Falta de manuales de los UPS de la institución.
- Inexistencia de inventario de los UPS.
- Carencia de planos de la ubicación de los UPS.

Recomendaciones

Base de Datos

Se recomienda generar documentación de la Base de Datos en la cual se detalle los procesos, políticas y estándares los cuales faciliten el manejo óptimo de los recursos.

Redes y Comunicación

Se sugiere implementar documentación referente al firewall, protocolos de seguridad y checkpoint, la cual ayude a entender los procesos, políticas y estándares que se deben cumplir, para el manejo óptimo de los recursos adquiridos.

Seguridad Lógica

Se recomienda generar documentación acerca de los equipos informáticos, así como de los procesos de eliminación de información, adquisición de licencias, medios magnéticos los cuales son de importancia en la institución.

Seguridad Física

Se sugiere generar documentación acerca de los UPS, Cámaras de Vigilancias, sistemas biométricos en la cual se detalle los procesos de manejo de cada elemento, así como su ubicación y características.

3.1.3 Plan de mejores prácticas

Mediante la ejecución de las pruebas realizadas en el punto 3.1.2.4 denominada **Ejecución de pruebas del Sistema Cabildo**, se recomendará sugerencias para la creación de planes de mejores prácticas para las áreas de Base de Datos, Redes y Comunicación, Seguridad Lógica y Seguridad Física, con las cuales se podrá obtener una mayor integridad, confidencialidad y confiabilidad de la información, las que se podrán evidenciar en las Tablas 78,79,80 y Tabla 81.

Tabla 78. Plan de mejores prácticas para Base de Datos

Pruebas				Estrategias de mejoramiento			
N°	**Denominación**	**Objetivo**	**Resultados**	**Acciones**	**Recursos necesarios**	**Tiempo estimado**	**Personal responsable**
P001	Acceso de los usuarios a la base de datos.	Verificar si existen políticas actualizadas para el acceso de usuarios y si cumplen su propósito.	• Se requiere obtener un registro de logs el cual ayudara a evidenciar los usuarios que desean ingresar a la base de datos.	Controlar el ingreso a la base de datos, y llevar un registro adecuado de las personas que acceden.	•Listado de usuarios en la institución •Ver los logs de registro a la base. •Ver la cantidad de intentos que permite la base.	2 semanas	Ing. Jhony Li
P002	Creación de usuarios y contraseñas a nivel de base de datos.	Verificar si existe políticas para la creación de usuarios y asignación de perfiles.	• Se pudo evidenciar que al momento de la asignación de usuarios no cuentan con un estándar el cual ayudaría a manejar una asignación adecuada. • Se pudo observar que las contraseñas asignadas no cumplen con un estándar adecuado ya que pueden ser asignadas al azar. • Al momento de la asignación de perfiles no se cumple con un proceso adecuado.	Ayudar a la creación de usuarios y se podrá asignar los perfiles necesarios dependiendo el cargo de cada usuario.	•Listado de usuarios asociados con el área de desarrollo. •Estándar para la asignación de usuario (Mayúsculas, minúsculas, caracteres especiales). •Estándar para la asignación de contraseñas (Mayúsculas,	1 mes	Ing. Jhony Li

					minúsculas, caracteres especiales). •Asignación de perfil.		
P003	Selección de personal de tecnologías de la información.	Validar el proceso de selección del personal de TI y ver si cumple con los requisitos establecidos.	• No se pudo obtener información la cual ayude a realizar la prueba. • No se realizan pruebas técnicas.	Evidenciar cuales son los procesos que se deben tomar en cuenta para la selección del personal.	•Manual de contratación para las personas del departamento de Tecnologías de la Información. •Ejecución de pruebas técnicas.	3 semanas	Ing. Jhony Li
P004	Documentación de procesos de base de datos entregada al personal.	Validar si la documentación entregada al personal está actualizada y si este cumple con el procedimiento estipulado para el manejo adecuado de la BDD.	• No se tiene documentación la cual ayude a entender las funciones de la base de datos. • No se puede ejecutar la documentación de la base de datos por carencia de documentación.	Entender el manejo adecuado de la base de datos.	•Documentación de la base de datos. •Ejecución de la documentación.	3 semanas	Ing. David Hidalgo
P005	Estabilidad de la base de datos en	Verificar el proceso de recuperación de	• No se cuenta con documentación pertinente la cual nos ayude a	Ayudar a mantener un proceso	•Listado de procesos para recuperación de información.	1 mes	Ing. Paúl Espinoza

	transacciones información (rollback).	información de la base de datos, cuando accidentalmente se elimina un dato.	recuperar información en caso de pérdida o eliminación.	adecuado para la recuperación de información.			
P006	Recuperación de Información(backups).	Verificar el proceso de recuperación de información de la base de datos, cuando es eliminada accidentalmente.	• No se cuenta con un manual el cual pueda detallar los pasos que se deben cumplir. • Carencia de documentación de los procesos a cuáles se realizan backups. • Inexistencia de documentación de cada cuanto tiempo se realizan los backups.	Mostrar el proceso a seguir para recuperación de información en la base de datos.	•Proceso de creación de backups. •Listado de los procesos a los cuales se realiza backups. •Listado de cada cuando tiempo se realizan los backups. •Almacenamientos de los backups en condiciones óptimas. •Pruebas periódicas de los Backups (restore)	1 mes	Ing. David Hidalgo
P007	Control de cambios en la estructura de la base de datos.	Validar el proceso de control de cambios	• No cuenta con un manual el cual les ayude a seguir un proceso adecuado. • Lo cambios solicitados son de manera verbal, no cuentan con	Guía de pasos necesarios para la realización de	•Manual para la generación de cambios.	3 semanas	Ing. Paúl Espinoza

		establecidos para la base de datos.	documentación la cual ayude a respaldar los cambios realizados.	cambios en la base de datos.	•Documentación de los cambios realizados.		
P008	Control de duplicidad de información.	Verificar el proceso adecuado para evitar la duplicidad de información en la institución.	• No cumple con un manual el cual indique el proceso adecuado para la creación de tablas. • No se cuenta con documentación de la estructura de la base de datos • Como no se cuenta con la estructura de la base de datos no se pudo evidenciar que atributo es la clave primeria en las tablas creadas.	Ayudar a evitar la redundancia de información en la base de datos.	•Manual de creación de tablas. •Estructura de la base de datos. •Creación de claves primarias.	2 semanas	Ing. Paúl Espinoza
P009	Estándares de nomenclatura.	Verificar el proceso adecuado para la creación de tablas.	• No cumple con un manual el cual indique el proceso adecuado para la creación de tablas.	Especificar procesos y normas que se deben utilizar para la creación de tablas, usuarios o contraseñas.	•Manual de creación de tablas.	2 semanas	Ing. Paúl Espinoza

Fuente: Elaboración propia

Tabla 79. Plan de mejores prácticas para Redes y Comunicación

Pruebas				Estrategias de mejoramiento			
N°	**Denominación**	**Objetivo**	**Resultados**	**Acciones**	**Recursos necesarios**	**Tiempo estimado**	**Personal responsable**
P010	Comprobar la seguridad configurada en el software VNC para acceso remoto al sistema CABILDO.	Validar la configuración de seguridad del software utilizado para la conexión remota VNC.	• Todos los equipos del municipio cuentan con el programa VNC. • No se tiene documentación de la configuración del programa VNC.	Ayudar a controlar la seguridad del software VNC el cual se utiliza para conexión al sistema Cabildo.	•Listado de los usuarios que tienen acceso remoto por VNC. •Configuraciones de seguridad del programa VNC. •Listado de configuraciones del checkpoint para los permisos.	1 mes	Ing. Henry Flores
P011	Acceso físico de las personas que ingresan a las instalaciones de servidores y que trabajos se disponen a realizar.	Comprobar la seguridad al otorgar acceso a las personas a las instalaciones.	• Se manifiesta que los permisos son de manera verbal que se les otorga a las personas que vayan a realizar trabajos en los servidores.	Mantener un proceso adecuado para el ingreso de terceras personas a las instalaciones.	•Minuta de acceso de visitantes. •Registro de visitas. •Listado de los lugares a los que tienen acceso.	3 semanas	Ing. Henry Flores
P012	Integridad del cableado estructurado.	Comprobar la infraestructura del cableado estructurado	• No se tiene planos en los cuales se pueda evidenciar el cableado actual de la institución.	Verificar el cumplimiento adecuado del	•Planos del cableado estructurado instalado en la institución.	2 meses	Ing. Henry Flores

		instalado en las oficinas de la compañía.		cableado estructurado.	•Distancia del cableado que se mantiene en los equipos.		
P013	Configuraciones del firewall por parte del proveedor.	Comprobar la seguridad al otorgar acceso a las personas a las instalaciones.	• No se cuentan con documentación pertinente en la cual se establezca la configuración del firewall. • No se tiene un listado en el cual se pueda evidenciar las paginas restringidas.	Análisis de las configuraciones utilizadas en el firewall y sus ventajas.	•Configuración del firewall. •Listado de acceso a páginas de internet.	1 mes	Ing. Henry Flores
P014	Protocolos con los que trabajan las aplicaciones.	Comprobar los protocolos con los que trabajan en el GAD de Ambato.	• No cuentan con un listado de todas las aplicaciones instaladas en la institución. • No se tiene documentación de los protocolos que se manejan en la institución. • No se cuenta con documentación en la cual se establezca el manejo	Manejar protocolos seguros para las aplicaciones de la institución.	•Listado de las aplicaciones. •Listado de protocolos utilizados. •Manual de utilización de protocolos.	3 semanas	Ing. Roberto Oñate

			adecuado de los protocolos.				
P015	Seguridad del checkpoint.	Comprobar la seguridad del checkpoint para evitar ataques.	• No se puede obtener documentación del checkpoint. • No existe un listado en el cual se pueda ver las personas que tienen acceso al checkpoint. • No se puede obtener las reglas generadas en la institución por motivos de seguridad.	Ayudar a entender el manejo del checkpoint mediante la generación de reglas.	•Políticas del checkpoint. •Listado de personas encargadas del manejo del checkpoint. •Listado de las reglas empleadas en el checkpoint.	2 semanas	Ing. Roberto Oñate
P016	Encriptación de información.	Verificar si la información que viaja a través de la red es encriptada.	• No se cuenta con documentación necesaria la cual ayude a entender el manejo de información. • No se conoce si utilizan tipo de encriptación en la institución.	Mantener la información segura, mediante procesos de encriptación.	•Proceso del manejo de información. •Tipo de encriptación utilizada en la institución.	2 meses	Ing. Roberto Oñate

Fuente: Elaboración propia

Tabla 80. Plan de mejores prácticas para Seguridad Lógica

Pruebas				Estrategias de mejoramiento			
N°	**Denominación**	**Objetivo**	**Resultados**	**Acciones**	**Recursos necesarios**	**Tiempo estimado**	**Personal responsable**
P017	Logs de la base de datos.	Revisar los logs para confirmar que los backups se estén realizando en los tiempos estipulados, que cambios se realizó.	• No se cuenta con documentación en la cual se pueda determinar el proceso adecuado de los logs. • Carencia de registros de los logs que se crean. • Inexistencia de un registro en el cual se pueda observar cada cuanto tiempo se realizan los logs.	Mantener un registro de las acciones que se realizan en la base de datos.	•Proceso de creación de logs. •Listado de los procesos a los cuales se realiza logs. •Listado de cada cuando tiempo se realizan los logs.	2 semanas	Ing. Santiago Cortés
P018	Software instalado en los equipos de cómputo	Revisar si el software instalado consta con las licencias respectivas.	• No se cuenta con documentación del software adquirido en la institución. • La mayoría del software utilizado en la institución no cuenta con documentación pertinente.	Llevar un proceso adecuado del software instalado en los equipos de la institución.	•Listado de software adquiridos en la institución. •Manual del software. •Licencia del software.	2 meses	Ing. Santiago Cortés

P019	Licencias del software instalado en los equipos de cómputo cliente.	Verificar que el software instalado en la institución se encuentra licenciado.	• No se cuenta con un listado del software en el cual se pueda visualizar que software es manejado en la institución. • No se cuenta con un registro de la vigencia y la cantidad de licencias adquiridas. • No se cuenta con un registro de la cantidad de las licencias adquiridas en la institución. • No se registró documentación en la cual se pueda evidenciar el tiempo de vigencia de las licencias.	Controlar la vigencia de las licencias adquiridas en la institución.	•Listado del software autorizado para el manejo de la institución. •Listado de las licencias de cada software instalado en los equipos. •Listado de la cantidad de licencias adquiridas con respecto a la cantidad de equipos o usuarios que hacen uso de este software. •Listado del tiempo de vigencia de las licencias.	2 meses	Ing. Santiago Cortés
P020	Eliminación de archivos temporales y obsoletos.	Verificar los pasos necesarios para la liberación de espacio en los servidores de la institución.	• Se necesita crear un registro con las carpetas en las que se almacena información obsoleta.	Mantener un proceso adecuado para la eliminación de información obsoleta.	•Listado de documentos o procedimientos para la liberación de espacio y eliminación de archivos obsoletos.	2 meses	Ing. Santiago Cortés

P021	Creación de usuarios y contraseñas del sistema Cabildo.	Comprobar el procedimiento para la creación de usuarios para el sistema Cabildo.	• Se cuenta con un estándar el cual al momento de la creación de usuarios se toma en cuenta la primera letra de los nombres y apellidos y el año en el que ingresan a la institución, pero no está debidamente documentando. • No cuentan con un estándar para la creación de contraseñas, ya que por primera vez se les asigna la contraseña del 1 al 5. • No se tiene documentación en la cual se detalle el manejo de asignación de perfiles.	Ayudar a mantener un proceso adecuado al igual que una asignación específica para la asignación de perfiles.	•Listado de usuarios asociados con el área de desarrollo. •Estándar para la asignación de usuario (Mayúsculas, minúsculas, caracteres especiales). •Estándar para la asignación de contraseñas (Mayúsculas, minúsculas, caracteres especiales). •Asignación de perfil.	1 semana	Ing. Patricio Mayorga
P022	Tipo de procedimiento de redundancia.	Verificar con qué tipo de raid utiliza la institución y porque motivo se utiliza ese raid.	• No se cuenta con documentación la cual pueda ayudar a sustentar la documentación de Raid utilizada.	Entender el tipo de Raid manejado en la institución y las ventajas de dicho Raid.	•Documentación del tipo de raid se utiliza en la institución. •Verificar si la documentación	1 mes	Ing. Patricio Mayorga

			• No se tiene acceso para la verificación del Raid.		entregada pertenece al raid de la institución.		
P023	Comprobación de los antivirus.	Verificar que los antivirus de la institución se encuentren actualizados.	• No se cuenta con documentación en la cual se pueda verificar el tiempo de vigencia de los antivirus.	Tener un proceso adecuado para el mantenimiento óptimo de los antivirus.	•Documentación del antivirus. •Registro de la licencia del antivirus.	2 meses	Ing. Patricio Mayorga
P024	Administración de los dispositivos de almacenamiento de los backups.	Verificar que los antivirus de la institución se encuentren actualizados.	• No se cuenta con un registro de los listados magnéticos que se utilizan en la institución. • No se puede constatar si cuentan con etiquetas por motivos de seguridad. • No tienen un listado de los dispositivos magnéticos creados.	Controlar un proceso adecuado del almacenamiento de información, que se maneja en la institución.	•Listado de medios magnéticos utilizados. •Etiquetas para definir contenido y nivel de seguridad. •Registro de etiquetado.	1 mes	Ing. Patricio Mayorga

Fuente: Elaboración propia

Tabla 81. Plan de mejores prácticas para Seguridad Física

Pruebas				Estrategias de mejoramiento			
N°	**Denominación**	**Objetivo**	**Resultados**	**Acciones**	**Recursos necesarios**	**Tiempo estimado**	**Personal responsable**
P025	Sistemas de vigilancia (Cámaras).	Verificar el funcionamiento de las cámaras instaladas en la institución.	• No se pudo obtener información del manejo de las cámaras por motivo que el área de Tecnología de la Información no está asociada con el área de Seguridad Física.	Emplear un proceso óptimo de los sistemas de vigilancia, pero principalmente basándose en el cuidado del datacenter.	•Manual de las cámaras de vigilancia. •Inventario de las cámaras de vigilancia implementados en la institución. •Planos de la ubicación de los sistemas de vigilancia. •Documentación de cada cuanto se elimina la información almacenada.	3 semanas	Departamento de Tecnologías de la Información y departamento de Seguridad Física.
P026	Seguridad del sistema biométrico.	Verificar las políticas de los sistemas biométricos.	• No se puede obtener documentación de los sistemas biométricos por que la información es manejada por el	Emplear un proceso óptimo de los sistemas biométricos de la institución, el	•Manual de los sistemas biométricos. •Inventario de los sistemas	3 semanas	Departamento de Tecnologías de la Información y departamento de Seguridad Física.

			departamento de seguridad física	cual ayude a evitar el ingreso de terceras personas.	biométricos implementados en la institución. •Planos de la ubicación de los sistemas biométricos.		
P027	Contratos de los empleados de seguridad.	Verificar el listado de empleados en el departamento de seguridad.	• No se puede obtener documentación de los empleados de seguridad por motivos de permisos.	Controlar el proceso para la selección del personal.	•Listado de los empleados de seguridad. •Listado del personal activo. •Contratos del personal.	3 semanas	Departamento de Tecnologías de la Información y departamento de Seguridad Física.
P028	Contraseñas de acceso a la BIOS.	Verificar si los equipos del municipio constan con contraseñas al momento de ingresar a la BIOS.	• No se cuenta con documentación la cual pueda servir para la asignación de contraseñas de la Bios.	Obtener un método adicional de seguridad, el cual nos ayudara a evitar el cambio de sistema operativo en los equipos de la institución.	•Inventario de los equipos de la institución. •Características de los equipos. •Listado de las configuraciones de la Bios.	2 semanas	Departamento de Tecnologías de la Información y departamento de Seguridad Física.

P029	Verificación de los UPS.	Verificar el tiempo de duración de los ups adquiridos en la institución.	• No se tiene documentación de los UPS. • No se tiene un inventario actualizado de los inventarios de los UPS. • No se cuenta con documentación la cual ayude a identificar la ubicación de los UPS.	Controlar el funcionamiento de los UPS, así como sus características.	•Manuales de los UPS de la institución. •Inventario de los UPS. •Planos de la ubicación de los UPS.	3 semanas	Departamento de Tecnologías de la Información y departamento de Seguridad Física.
P030	Acceso al datacenter.	Verificar que los elementos de oficina entregados a los empleados son acordes a sus labores diarias.	• Se cuenta con sistemas biométricos, pero no existe documentación la cual ayude a sustentar las características de los sistemas biométricos. • Se cuenta con sistemas de cámaras, pero no existe documentación la cual ayude a sustentar las características de las cámaras. • No se cuenta con documentación acerca del manejo del programa Teamviwer O VPN.	Mantener un proceso adecuado para el ingreso al datacenter, el cual será monitoreado por cámaras y sistemas biométricos.	•Control Biométrico. •Monitoreo de cámaras. •Acceso remoto mediante VPN. •Teamviwer.	1 semana	Departamento de Tecnologías de la Información y departamento de Seguridad Física.

Fuente: Elaboración propia

Con la elaboración de los planes de mejores prácticas elaborados para las áreas de Base de Datos, Redes y Comunicación, Seguridad Lógica y Seguridad Física, de esta manera se contribuirá con la confidencialidad y confiabilidad en los procesos del sistema Cabildo y del departamento de Tecnologías de la Información, como se puede observar se ha cumplido todos los objetivos planteados, los cuales servirán para el beneficio del sistema Cabildo y del departamento de Tecnologías de la Información del Gobierno Autónomo Descentralizado Municipalidad de Ambato.

CAPITULO IV.- CONCLUSIONES Y RECOMENDACIONES

4.1 Conclusiones

Una vez desarrollado todos los objetivos planteados se obtuvieron las siguientes conclusiones.

En el Gobierno Autónomo Descentralizado Municipal de Ambato se evaluó la situación actual del sistema Cabildo, utilizando la metodología Cobit, principalmente basándonos en los principios de Cobit.

Mediante la ejecución de pruebas a las diferentes áreas como son Base de Datos, Redes y Comunicaciones, Seguridad Física y Seguridad Lógica y con ayuda de los principios Cobit se evaluó el sistema Cabildo, las cuales nos ayudó a evidenciar las falencias existentes.

Las pruebas ejecutadas fueron separadas dependiendo el principio Cobit que cumplieron lo cual permitió ver el desempeño del sistema Cabildo y por consiguiente el del departamento de Tecnologías de la Información.

4.2 Recomendaciones

Se sugiere implementar nuevas metodologías las cuales ayuden a gestionar de mejor manera la información manejada en el sistema Cabildo

Es importante generar políticas las cuales ayuden a mejorar el desempeño del departamento de Tecnologías de la información y por ende al sistema Cabildo.

Se propone realizar auditorías periódicamente las cuales ayuden a seguir identificando los fallos con los que cuentan tanto el departamento de Tecnologías de la Información (TI) y el sistema Cabildo.

Se propone realizar auditorías periódicamente las cuales ayuden a seguir identificando los fallos con los que cuentan tanto el departamento de Tecnologías de la Información (TI) y el sistema Cabildo.

Referencias Bibliográficas

[1] A. H. Sánchez, "Auditorías de seguridad informática y la OSSTMM." [en línea]. Disponible en: http://es.scribd.com/doc/17740680/Auditorias-de-Seguridad-Informatica-y-la-OSSTMM, 2009.

[2] Espinoza, Maritza (2007) *"*Auditoria Informática para los departamentos Financiero, Tesorería, Proveeduría, Agencia Norte y agencia Sur de la Empresa municipal de agua potable y Alcantarillado de Ambato*",* Proyecto de Pasantía de Grado, previo a la obtención del Título de Ingeniera en Sistemas Computacionales e Informáticos, Universidad Técnica de Ambato, Facultad de ingeniería en sistemas Electrónica e Industrial, Ciudad Ambato, Ecuador.

[3] M. G. Hernández Pinto, "Diseno de un plan estratégico de seguridad de información en una empresa del sector comercial." [en línea]. Disponible en: http://www.dspace.espol.edu.ec/handle/123456789/10730, 2006.

[4] J. Ana Lucía, "Auditoria Informática del Sistema de Información de la empresa Cocinas Internacionales utilizando Cobit v.5", *Repositorio.espe.edu.ec*, 2016. [Online]. Available: http://repositorio.espe.edu.ec/xmlui/bitstream/handle/21000/12111/T-ESPE-053368.pdf?sequence=1&isAllowed=y. [Accessed: 26- Oct- 2019].

[5] Badillo Pinto, P. (2016). *Guía de implementación de Tecnologías de la Información aplicando Cobit en Auditorias de entidades financieras, para disminuir errores procedimentales*. [online] Dspace.unach.edu.ec. Available at: http://dspace.unach.edu.ec/bitstream/51000/1603/1/UNACH-EC-ISC-2016-0001.pdf [Accessed 26 Oct. 2019].

[6] L. Campo, "Sistema de Información", *Incap.int*. [Online]. Available: http://www.incap.int/sisvan/index.php/es/acerca-de-san/conceptos/797-sin-categoria/501-sistema-de-informacion. [Accessed: 30- Oct- 2019].

[7] "Definición de seguridad informática — Definicion.de", *Definición.de*, 2018. [Online]. Available: https://definicion.de/seguridad-informatica/. [Accessed: 02- Nov- 2018].

[8]Seguridad Informática", *EcuRed*, 2018. [Online]. Available: https://www.ecured.cu/Seguridad_Inform%C3%A1tica. [Accessed: 02- Nov- 2018].

[9]"Significado de Auditoría", *Significados*, 2013. [Online]. Available: https://www.significados.com/auditoria/. [Accessed: 28- Oct- 2019].

[10]C. Muñoz Razo, "Auditoría en sistemas computacionales", *Google Books*, 2002. [Online]. Available: https://books.google.com.ec/books?id=3hVDQuxTvxwC&pg=PR12&dq=tipos%20de%20auditoria%20libros&hl=es&sa=X&ved=0ahUKEwikjPyOwb_lAhUQqlkKHesIB_sQ6AEIQzAE&fbclid=IwAR2VzTJINXGQiyN-QbP7AWxoaCgmkjzM8jOFemqrgoO5zPbMPsXAdaukx6I#v=onepage&q=tipos%20de%20auditoria%20libros&f=false. [Accessed: 28- Oct- 2019].

[11] M. Piattini, *Auditoria Informática, Un enfoque práctico*, 2nd ed.

[12]"TIPOS Y CLASES DE AUDITORIAS INFORMATICAS", *prezi.com*, 2016. [Online]. Available: https://prezi.com/1p1ouq256zjt/tipos-y-clases-de-auditorias-informaticas/. [Accessed: 29- Oct- 2019].

[13]"Auditoria Informatica de Desarrollo De Proyectos o Aplicacio", *prezi.com*, 2019. [Online]. Available: https://prezi.com/yg2wqjqcamas/auditoria-informatica-de-desarrollo-de-proyectos-o-aplicacio/. [Accessed: 29- Oct- 2019].

[14]P. Nuño, "Auditoría de sistemas | ¿Qué es una auditoría de sistemas?", *Emprende Pyme*, 2017. [Online]. Available: https://www.emprendepyme.net/auditoria-de-sistemas.html. [Accessed: 29- Oct- 2019].

[15]E. Redacción, "8 ventajas de hacer una auditoría informática", *Blog.apser.es*, 2016. [Online]. Available: https://blog.apser.es/2016/03/03/8-ventajas-de-hacer-una-auditoria-informatica. [Accessed: 29- Oct- 2019].

[16]"DOMINIOS Y PROCESOS DE COBIT", *Cobitmmatiasc.blogspot.com*, 2019. [Online]. Available: http://cobitmmatiasc.blogspot.com/2017/03/dominios-y-procesos-de-cobit.html. [Accessed: 27- Oct- 2019].

[17] T. Velásquez Pérez, A. Puentes Velásquez and Y. Pérez Pérez, "Model for implementation of IT corporate governance", *Scielo.org.co*, 2019. [Online]. Available:

http://www.scielo.org.co/scielo.php?script=sci_arttext&pid=S0123-921X2015000500015&lang=es. [Accessed: 27- Aug- 2019].

[18]R. Meadows, Cobit 5, Un Marco de Negocio para el Gobierno y la Gestión de las TI de la Empresa. 2012, p. www.isaca.org.

[19]"Plan estrategico", *Gadmatic.ambato.gob.ec*, 2015. [Online]. Available: https://gadmatic.ambato.gob.ec/lotaip/2018/enero/anexo%20literal%20k/Plan%20Estrategico%202015-2019.pdf. [Accessed: 01- Nov- 2019].

[20]"Modelo de gestión y estructura del Gobierno Autonomo Descentralizado Municipalidad de Ambato", *Ambato.gob.ec*, 2012. [Online]. Available: http://www.ambato.gob.ec/indexn/images/2015/abril/lotaip/ANEXOS%20LITERAL%20a3)/ANEXO%202.pdf. [Accessed: 01- Nov- 2019].

[21]"Reglamento Orgánico Funcional", *Gadmatic.ambato.gob.ec*, 2016. [Online]. Available:https://gadmatic.ambato.gob.ec/lotaip/2016/enero/anexo%20literal%20a3/REGLAMENTO%20ORGANICO%20FUNCIONAL.pdf. [Accessed: 27- Aug- 2019].

[22]"Metas y objetivos unidades administrativas", *Ambato.gob.ec*, 2018. [Online]. Available: https://ambato.gob.ec/wp-content/uploads/downloads/2019/01/a4-metas-y-objetivos-unidades-administrativas-lleno-DICIEMBRE-2018..pdf. [Accessed: 01- Nov- 2019].

[23] Plan de contingecia informático del GAD Municipalidad de Ambato. Ambato: Direccion de Tecnologias de la Informacion, 2017.

Anexos

ENTREVISTA REALIZADA AL DIRECTOR DEL DEPARTAMENTO DE TECNOLOGÍAS DE LA INFORMACIÓN DEL GAD MUNICIPAL DE AMBATO		
OBJETIVO		
FECHA:		
ENTREVISTADO:		
CARGO:		
N°	**Preguntas**	**Respuestas**
1	¿Conoce Ud si el departamento de TI cuanta con un plan estratégico para la mejora del sistema Cabildo?	
2	¿Existen algún plan para la seguridad de la información de la institución?	
3	¿Conoce con cuántos sistemas cuenta la institución y cual son sus funciones?	
4	¿Conoce Ud si se ha realizado una Auditoria	

	Informática en el departamento de TI?	
5	¿Cree necesaria la elaboración de una auditoria informática en el departamento de TI?	
6	¿Ha considerado la importancia que tiene la información que se maneja en la institución?	
7	¿El GAD de Ambato ha sufrido ataque mediante la red?	
8	¿El área de tecnologías de la información cuenta con documentación donde establezca sus funciones?	
9	¿Considera que el personal del área está capacitado para realizar las tareas que desempeñan?	
10	¿Se requiere de servicios de terceros para cumplir con las funciones del área?	

11	¿Conoce Ud si han existido problemas con los usuarios creados en la base del GAD de Ambato?	
12	¿La empresa posee manuales actualizados de procedimientos y procesos que se deben realizar?	
		ENTREVISTADOR: