MODELO DE GOBIERNO DE TI PARA LA JEFATURA DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES DE LA FUERZA AÉREA COLOMBIANA.

ANDREI BAHAMON PAEZ
CARLOS ALBERTO VELÁSQUEZ PINEDA

Universidad EAN
Facultad de Ingeniería
Maestría en Gerencia de Sistemas de Información y Proyectos Tecnológicos
Bogotá D.C., Colombia
2020

MODELO DE GOBIERNO DE TI PARA LA JEFATURA DE LAS TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES DE LA FUERZA AÉREA COLOMBIANA.

ANDREI BAHAMON PAEZ
CARLOS ALBERTO VELÁSQUEZ PINEDA

Trabajo de grado presentado como requisito para optar al título de:
Magister en Gerencia de Sistemas de Información y Proyectos Tecnológicos

Director:
DAGO HERNANDO BEDOYA ORTIZ

Modalidad:
Trabajo Dirigido

Universidad EAN
Facultad de Ingeniería
Maestría en Gerencia de Sistemas de Información y Proyectos Tecnológicos
Bogotá D.C., Colombia
2020

Nota de aceptación

_____
_____
_____
_____
_____

_____
Firma del jurado

_____
Firma del jurado

_____
Firma del director del trabajo de grado

Bogotá D.C. 08 - FEBRERO – 2021

Dedicatoria

A Dios por el regalo de la Vida, a mis padres, por su motivación permanente, a mi esposa Anny e hijo Josué por su paciencia y apoyo a lo largo de este camino. A mi mascota Laika, por su compañía en cada una de las jornadas de estudio. Carlos Velásquez

Tabla de contenido

Lista de gráficos

Lista de tablas

Listado de abreviaturas

CISR: Centro de Investigación de Sistemas de Información.

COBIT: *Control Objectives for Information and related Technology.*

DIACO: Dirección Apoyo al Comando y Control**.**

DICRA: Dirección de Comunicaciones, Radio ayudas y Ayudas Aeroportuarias.

DITIN: Dirección de Tecnologías de la información.

EAN: Escuela de administración y negocios.

FAC: Fuerza Aérea Colombiana.

JETIC: Jefatura de las tecnologías de la información y comunicaciones.

ISO: *International Organization for Standardization.*

ITIL: *Information Technology Infrastructure Library.*

MINTIC: Ministerio de Tecnologías de la Información y las Comunicaciones.

MMGO: Modelo de Modernización para la Gestión de las Organizaciones.

PMBOK: *Project Management Body of Knowledge.*

PMI: *Project Management Institute.*

PYMES: Pequeñas y medianas empresas.

TI: Tecnologías de la Información.

TIC: Tecnologías de la información y Comunicaciones.

SATENA: Servicio Aéreo a Territorios Nacionales.

SGC: Sistema de Gestión de la Calidad.

SGSI: Sistema de Gestión de Seguridad de la Información.

CIAC: Corporación de la Industria Aeronáutica Colombiana.

SNGRD: Sistema Nacional de Gestión del Riesgo de Desastres.

Glosario

COBIT: Acrónimo de *Control Objectives for Information and related Technology* (Objetivos de Control para la Información y Tecnologías Relacionadas). Es un estándar desarrollado por la *Information Systems Audit and Control Foundation* (ISACA), que se preocupa de temas como gobernabilidad, control, aseguramiento y auditorias para TI.

Disponibilidad: Propiedad de que la información y sus recursos relacionados deben estar disponibles y utilizables cuando se los requiera.

Estándar: Conjunto de características y requisitos que se toman como referencia o modelo y son de uso repetitivo y uniforme. Para que sea un estándar debe haber sido construido a través de consenso y refleja la experiencia y las mejores prácticas en un área en particular.

Gestión de TI: Es una práctica que permite operar, innovar, administrar, desarrollar y usar apropiadamente las tecnologías de la información; se ocupa de planificar, construir, ejecutar y monitorear las actividades alineadas con la dirección establecida por el organismo de gobierno para el logro de los objetivos empresariales.

Gobierno: El método o marco de trabajo por el cual una organización es dirigida, administrada y/o controlada.

Gobierno de TI: El gobierno de tecnologías de información establece una dirección que asegura el cumplimiento de la visión estratégica, haciendo visible y cuantificable el valor que devuelven las TI a la organización. Entrega responsabilidades a personas bajo una estructura establecida dentro de la organización, que permita decidir para incentivar el comportamiento deseable de las TI y una adecuada gestión del riesgo.

Incidente: Cualquier evento que no sea parte de la operación estándar de un servicio que ocasione, o pueda ocasionar, una interrupción o reducción de la calidad de dicho servicio.

ISACA: Acrónimo de *Information Systems Audit and Control Association* (Asociación de Auditoría y Control de Sistemas de Información). Organización que surge en 1967 y que establece pautas para los profesionales respecto a la gestión, control, seguridad y auditoría de la información.

ITIL: Librería de Infraestructura de TI de la oficina de Gobierno Gubernamental del Reino Unido (OGC). Un conjunto de lineamientos sobre la administración y procuración de servicios operativos de TI.

Marco de trabajo: Una herramienta para los dueños de los procesos de negocio que facilita la descarga de sus responsabilidades a través de la procuración de un modelo de control de soporte.
Nivel de madurez: Nivel identificado en un modelo de Madurez como el Modelo de Integración de Madurez de la Capacidad.
Planeación estratégica: El plan estratégico es un documento en el que los responsables de una organización reflejan cual será la estrategia para seguir por su compañía en el mediano y largo plazo.
Plan estratégico de TI: Un plan a largo plazo, en el cual la gerencia del negocio y de TI, describen de forma operativa cómo los recursos de TI contribuirán a los objetivos estratégicos empresariales (metas).
Política: Por lo general, un documento que ofrece un principio de alto nivel o una estrategia a seguir. El propósito de una política es influenciar y guiar la toma de decisiones presente y futura, haciendo que estén de acuerdo con la filosofía, objetivos y planes estratégicos establecidos por los equipos de jefatura del área que la implementa.
Portafolio: Una agrupación de programas, proyectos, servicios o activos seleccionados, administrados y vigilados para optimizar el retorno sobre la inversión.
Proceso: Conjunto de procedimientos influenciados por las políticas y estándares de la organización, que toma las entradas provenientes de un número de fuentes, incluyendo otros procesos. Manipula las entradas, y genera salidas, incluyendo a otros procesos, para los clientes de los procesos.
Servicio: Es el conjunto de acciones o actividades de carácter misional diseñadas para incrementar la satisfacción del usuario, dándole valor agregado a las funciones de la entidad.
TI: Acrónimo de “Tecnologías de la Información”. Hace referencia a las aplicaciones, información e infraestructura requerida por una entidad para apoyar el funcionamiento de los procesos y estrategia de negocio.
TIC: Acrónimo de “Tecnologías de la información y las comunicaciones”, conforman el conjunto de recursos necesarios para manipular la información: los computadores, los programas informáticos y las redes necesarias para convertirla, almacenarla, administrarla, transmitirla y encontrarla.

Resumen

Cada vez es mayor el número de organizaciones que incorporan herramientas tecnológicas para soportar sus procesos, motivo por el cual, con la finalidad de ser una institución innovadora en la administración organizacional y en la ejecución de sus procesos, además de ser eficiente financiera y administrativamente, la Fuerza Aérea Colombiana ha incorporado herramientas tecnológicas y sistemas de información que soportan la ejecución de todos los procesos internos.

Teniendo en cuenta que cada vez son más los servicios de TI que soportan los procesos de la FAC, la implementación de un gobierno corporativo de TI es una opción que permitirá alinear la estrategia de TI con la institucional, optimizar la utilización de los recursos de TI, aumentar los beneficios esperados de las inversiones realizadas en este aspecto y disminuir los riesgos asociados. En consecuencia, el objetivo del presente trabajo es diseñar un modelo para el Gobierno de TI y su plan de implementación en la Jefatura de las Tecnologías de la Información y las Comunicaciones de la Fuerza Aérea Colombiana.

En el desarrollo del plan de implementación, inicialmente se realiza la revisión del marco normativo para la gestión de tecnología en entidades públicas, después, con la finalidad de identificar los lineamientos y requerimientos para la elaboración del modelo de gobierno de TI, se realiza el análisis de la estrategia de la Jefatura, y finalmente se construye un modelo de gobierno de TI, el cual contempla los requerimientos definidos como entrada, así como las tareas principales, los principios definidos en el modelo base adoptado, las prácticas claves de gobierno y los indicadores de gestión que permitan valorar el cumplimento de los objetivos de TI y cerrar las brechas identificadas en el diagnóstico.

Palabras claves: Tecnologías de la información y la comunicación, competitividad, Gobierno de TI, Gestión de Conocimiento, Marcos de referencia, Diagnóstico Empresarial.

Abstract

The number of organizations that incorporate technological tools to support their processes is increasing, which is why, in order to be an innovative institution in organizational administration and in the execution of its processes, in addition to being financially and administratively efficient, The Colombian Air Force (FAC) has incorporated technological tools and information systems that support the execution of all internal processes.

Taking into account that increasingly more IT services support FAC processes, the implementation of IT corporate governance is an option that allows aligning the IT strategy with the institutional one, optimizing the use of IT resources, increasing the expected benefits of the investments made in this regard and reducing the associated risks. Consequently, the objective of this work is to design a model for IT governance and its implementation plan in the Head of Information Technologies and Communications of the Colombian Air Force.

In the development of the implementation plan, the regulatory framework for technology management in public entities is reviewed. Then, in order to identify the guidelines and requirements for the development of the IT governance model, the analysis of the strategy of the Headquarters is made, and finally an IT governance model is built, which considers the requirements defined as input, as well as the main tasks, the principles defined in the adopted base model, the key governance practices and the performance indicators, that will be able to assess compliance with IT objectives and close the gaps identified in the diagnosis.

Keywords: Information and communication technologies, competitiveness, IT Governance, Knowledge Management, Frameworks, Business Diagnosis.

1. Introducción

La adopción permanente de herramientas tecnológicas para potencializar diferentes procesos en las organizaciones, cada vez se presenta en mayor proporción en todos los sectores de la industria. Esta dependencia tecnológica hace necesario que existan políticas y lineamientos claros, de manera que los recursos de TI disponibles se utilicen de manera eficiente. En este contexto, el gobierno corporativo de las TIC administra los servicios de TI, con la finalidad de proteger los activos y garantizar que los recursos sean utilizados responsablemente bajo un marco regulatorio, de manera que se haga un uso eficiente de los recursos de TI para el cumplimento de los objetivos corporativos y que, al mismo tiempo, se minimicen los riesgos asociados.

El Gobierno de TI es aplicable en todo contexto organizacional, aunque es un concepto moderno de apoyo a las empresas en la planeación estratégica, en especial a lo que se refiere a la toma de decisiones en tecnología. En efecto, el desarrollo del Gobierno de TI de una manera más integral ha permitido reconocer que no solo es la administración de un recurso, sino un aspecto esencial para generar una estrategia sostenible con el propósito de incrementar su valor, y apoyar en el uso eficaz, eficiente y aceptable de las tecnologías de la información, equilibrando los riesgos y promoviendo las oportunidades que se originan de su uso.

El alcance de la presente investigación es elaborar una propuesta de modelo de Gobierno de TI que esté alienada con la estrategia de la Jefatura de las tecnologías de la información y las comunicaciones de la Fuerza Aérea Colombiana (FAC), cumpliendo con los lineamientos emitidos para entidades públicas a través de la política de Gobierno Digital y el marco normativo asociado.

El objetivo general del proyecto es diseñar un modelo de Gobierno de TI y su plan de implementación en la Jefatura de las Tecnologías de la Información y las Comunicaciones de la FAC, a partir del diagnóstico y del análisis estratégico realizado. Lo anterior, en vista de que actualmente la institución cuenta con una robusta infraestructura de TI para soportar el desarrollo de los procesos, pero no está implementado un gobierno corporativo de TI que emita políticas y lineamientos para la adquisición, implementación, utilización y soporte de los recursos de TI.

Para lograr el objetivo general se han planteado cinco objetivos específicos los cuales son: realizar diagnóstico de la situación actual en relación con el modelo de Gobierno de TI, realizar análisis estratégico de la Jefatura de las Tecnologías de la Información y las Comunicaciones de

la Fuerza Aérea Colombiana con el propósito de definir los lineamientos para alinear el Gobierno de TI con la Estrategia, diseñar un modelo de Gobierno de TI que incluya personas, procesos, tecnología, servicios y datos, elaborar el plan de implementación del modelo desarrollado y por último, efectuar la validación del modelo mediante juicio de expertos, aplicado en la oficina de Gobierno Corporativo de TIC de la Jefatura de las Tecnologías de la Información y Comunicaciones.

El documento presenta la siguiente estructura: El capítulo 1 presenta los objetivos del proyecto, el capítulo 2 presenta la justificación para la realización del trabajo, el capítulo 3 describe el planteamiento del problema y la justificación, en el capítulo 4 se detallan los antecedentes, el capítulo 5 describe el marco institucional, el capítulo 6 desarrolla el marco teórico, el cual incluye la descripción de algunos marcos de referencia, tales como ITIL, IS0 / IEC 38500, ISO / IEC 27001 PMBOK y COBIT y en el capítulo 7 se describe el diseño metodológico utilizado en el desarrollo de la investigación. En este sentido, el presente proyecto se realizó por medio de una investigación no experimental, y una metodología de observación activa de orden cualitativo, profundizando sobre el nivel de madurez de los procesos objeto de estudio, y a través de la información recolectada, se diseñó y documentó un modelo de gobierno de TI que cumple de forma integral los objetivos propuestos.

Finalmente, para desarrollar la propuesta, en el capítulo 8 se relaciona el marco normativo en la gestión de tecnologías de la información y comunicaciones, en el capítulo 9 se describe el diagnóstico realizado en la Jefatura con relación a la gestión de infraestructura tecnológica y el estado actual de los procesos aplicables a un modelo de gobierno de TI, en el capítulo 10 se desarrolla el contexto y es realizado el análisis estratégico para identificar los lineamientos y requerimientos sobre los cuales se desarrolló la propuesta, en el capítulo 11 se describe el modelo de gobierno de TI, partiendo del contexto para entidades públicas en Colombia, en capítulo 12 se desarrolla el plan de implementación del modelo propuesto, y finalmente, en el capítulo 13 se realiza la validación mediante juicio de expertos.

2. Objetivos

2.1. Objetivo general

Diseñar un modelo para el Gobierno de TI y su plan de implementación en la Jefatura de las Tecnologías de la Información y las Comunicaciones de la Fuerza Aérea Colombiana.

2.2. Objetivos específicos

- Realizar diagnóstico de la situación actual en relación con el modelo de Gobierno de TI.
- Realizar análisis estratégico de la Jefatura de las Tecnologías de la Información y las Comunicaciones de la Fuerza Aérea Colombiana, con el propósito de definir los lineamientos para alinear el Gobierno de TI con la Estrategia.
- Diseñar un modelo de Gobierno de TI que incluya personas, procesos, tecnología, servicios y datos.
- Elaborar el plan de implementación del modelo desarrollado.
- Efectuar la validación del modelo, mediante juicio de expertos, aplicado en la oficina de Gobierno Corporativo de TIC de la Jefatura de las Tecnologías de la Información y Comunicaciones.

3. Justificación

Actualmente la Fuerza Aérea Colombiana cuenta con un capital de información conformado por 15 sistemas de información propios, 7 comerciales, 4 sectoriales y 2 motores de bases datos, como se ilustra en el gráfico 1, además de una infraestructura de hardware y redes de datos para soportar el desarrollo de los procesos de la organización; pero no está implementado un gobierno corporativo de TI que emita políticas y lineamientos para la adquisición, implementación, utilización y soporte de los recursos de TI.

Gráfico 1: Sistemas de Información FAC

Fuente: Elaboración propia

Es por esto que, en la Fuerza Aérea Colombiana se presentan diversas problemáticas asociadas a la falta de un gobierno de TI, tales como el bajo aprovechamiento de los recursos de TI, la ineficiencia en los productos y servicios de TI, los altos costos de mantenimiento de la infraestructura, la desactualización del plan de continuidad del negocio, la pérdida de la información, la baja interoperabilidad e integración de la plataforma tecnológica de la FAC, la desactualización del Plan Estratégico de TI, la falta de estandarización y normalización en el proceso de TI y la insuficiente capacitación del personal que administra la infraestructura de TI.

Por lo anterior, es conveniente implementar un gobierno corporativo de TI que armonice la estrategia de la Jefatura de las Tecnologías de la Información y la Comunicación con la institucional, además de emitir políticas en relación con la adquisición, implementación, uso y apropiación de los recursos de TI, de manera que potencialice el rendimiento de servicios de TI disponibles en la organización para que soporten la ejecución de los procesos de manera eficiente. En este mismo sentido, el proyecto está alineado con el objetivo establecido por la Jefatura de las Tecnologías de la Información y la Comunicación, en cuanto se refiere a:

> orientar la gestión de TIC en las dependencias de la Fuerza Aérea Colombiana en concordancia con la reglamentación nacional vigente del sector, a través de la definición de políticas, estrategias, modelo de gestión y modelo de planeación que permitan implementar las tecnologías de información como eje transversal a toda la institución, con el propósito de facilitar el uso de los sistemas de información para la solución de la gestión operacional y administrativa (Fuerza Aérea Colombiana, 2019, p. 15).

Por otro lado, es importante resaltar que el Gobierno Nacional, en cabeza del Ministerio de Tecnologías de la Información y las Comunicaciones ha diseñado el Plan Estratégico Institucional MINTIC 2019-2022, que tiene como objetivo tener un gobierno más eficiente y transparente, mediante el liderazgo para la gestión de TI y con una arquitectura interoperable, apuntando a prestar los mejores servicios y trámites en línea al ciudadano (MinTIC, 2019). Por consiguiente, todas las instituciones públicas deben estar alineadas con las directrices emanadas por el Gobierno Nacional y tomar las acciones necesarias para cumplir con ellas. Vale la pena resaltar que, el Plan Estratégico Institucional MINTIC 2019-2022 no plantea cómo implementar un modelo de gobierno de TI, pero si emite los lineamientos generales que deben ser adoptados por las entidades públicas.

Desde el punto de vista de la relevancia social, es conveniente subrayar que la Fuerza Aérea Colombiana es una organización del Estado, razón por la cual dispone de los recursos públicos para su funcionamiento. Es por esto que, al ser administrada de manera eficiente, generará mayores beneficios a la sociedad colombiana con relación a la satisfacción de los intereses de seguridad, defensa, desarrollo de la población y cumplimiento de los fines del Estado. De esta manera, la implementación de un modelo de gobierno de TI, contribuye al cumplimiento del objetivo estratégico de la Fuerza Aérea Colombiana, puntualmente en lo que se refiere a la responsabilidad administrativa.

De igual manera, considerando el proceso de transformación implementado por la Fuerza Aérea Colombiana mediante la disposición 061 del 22 de diciembre de 2017, en la cual se originó la Jefatura de las Tecnologías de la Información y Comunicaciones, como la fusión de las direcciones de Comunicaciones, Radio ayudas y Ayudas Aeroportuarias - DICRA y la Dirección de Tecnologías de la información – DITIN, se hace necesario la estructuración de un Gobierno Corporativo de TI; toda vez que este proceso de transformación se realizó para garantizar la sostenibilidad de la institución, además de convertirse en una organización militar polivalente, interoperable, con capacidad de actuar bajo estándares internacionales y de despliegue operacional en el marco del posconflicto. En este sentido, la Fuerza Aérea se transforma para asumir nuevos retos, más efectivos y especializados, ejerciendo mayor control de los recursos humanos y económicos, simplificando los procesos y aumentado la velocidad de respuesta para contrarrestar las amenazas (Defensa.com, 2017).

De igual manera, se tomaron como referencia los casos de éxito basado en buenas prácticas a nivel local, tales como los implementados en el Grupo Bancolombia y Ecopetrol. Bancolombia ocupa el primer lugar en el mercado financiero en Colombia, por activos y participación en el mercado, opera en Colombia y El Salvador, tiene filiales en Panamá, las Islas Caimán, Puerto Rico y Perú, además de una agencia en Miami. Es un grupo financiero que opera los servicios de banca múltiple que incluyen inversiones, facturas, fiduciarias, arrendamiento financiero y mercado de valores.

El consejo de administración del Grupo Bancolombia adoptó COBIT como su modelo de referencia de gobierno TI, el cual permite verificar la incorporación y cumplimiento de los sus controles internos. De esta forma, COBIT ofrece un enfoque proactivo para la incorporación de técnicas para mejorar los procesos de tecnología y servicios, brindando al departamento de tecnologías herramientas para mantener un equilibrio entre el cumplimiento y el rendimiento, de esta forma, el modelo de control interno, auditorías internas y externas se fortalecen.

En este sentido, se quiere resaltar que, al implementar un modelo de gobierno de TI en el Grupo Bancolombia, la organización fortalece y da continuidad a sus sistemas y por ende a su operación, donde mantiene la alineación entre la planificación estratégica de negocios y planificación estratégica de TI, un lenguaje común, una asignación adecuada de roles y responsabilidades, un conocimiento de los riesgos alineados con sus fortalezas y debilidades, y

una visión compartida y unificada de sus sistemas de tecnología e información (Ceipa, 2011).

Otro caso identificado en el entorno local es Ecopetrol, que apoyado por el instituto Colombiano del Petróleo (ICP), ayuda a la unidad de infraestructura y servicios, en la necesidad de implementación de buenas prácticas en el control de información y gestión de riesgos. Para lo cual, acogieron modelos como COBIT e ITIL, para gestionar sus sistemas, información y tecnología. Dentro de estas buenas prácticas se utiliza COBIT para implementar su gobierno de TI e implementación de controles e ITIL para mejorar sus prácticas y procedimientos, donde se requería mejorar su retorno de inversión para las inversiones de TI, cumpliendo las normas legales en protección de información y generación de reportes, así como conocer sus índices de desempeño del área de tecnología y su modelo de gobierno de TI (Cordero, 2011).

Finalmente, considerando que la organización en la cual se va a desarrollar el proyecto cuenta con un capital de información robusto para soportar los procesos, es importante hacer referencia a lo expuesto por Bhatt y Grover (2005), quién aduce que las tecnologías de la información y la comunicación por sí solas no se desencadenan en ventajas competitivas, sino que se encuentran apoyadas por un plan estratégico que define el objetivo de las TIC, motivo por el cual se hace necesario que exista un gobierno de TI que emita las políticas para la utilización de las TIC, de manera que se conviertan en un catalizador de los procesos organizacionales; así mismo, de acuerdo con Stern (2002) para que las TIC se constituyan en herramientas de apoyo a la gestión empresarial, apalancando la construcción de estrategias orientadas a la competitividad y la innovación, generando así́ sostenibilidad para la organización y la sociedad.

4. Antecedentes

Cada vez es mayor el número de organizaciones que incorporan herramientas tecnológicas para soportar sus procesos, tanto los estratégicos como los misionales y los de apoyo. Básicamente, este cambio es realizado con el propósito de aumentar la eficiencia y la productividad, además de disminuir el tiempo que tarda la ejecución de un procedimiento y los recursos necesarios para tal fin. En este contexto, las tecnologías de la información y la comunicación rápidamente han pasado a ser un activo fijo intangible de las organizaciones que pueden generar valor diferenciador, por consiguiente, permiten a las empresas ser más competitivas en un mercado global. De la misma manera, también se constituyen en un elemento catalizador que facilita alcanzar los objetivos estratégicos.

Por otro lado, la adopción masiva de las tecnologías de la información y la comunicación se presenta tanto en organizaciones privadas como públicas. En las primeras, la finalidad de invertir en recursos de TI es de posicionarse en el mercado, incrementar la producción y las ventas, para finalmente obtener mayores utilidades. En el segundo caso, el enfoque es un poco diferente, en razón a que la finalidad no es obtener ganancias económicas, sino que es lograr que la administración pública sea eficiente, además de facilitar el desarrollo de las estrategias sectoriales y brindar servicios de gobierno en línea que satisfaga las necesidades de los ciudadanos.

En este sentido, la Fuerza Aérea Colombiana es una institución pública perteneciente al Ministerio de Defensa Nacional, que tiene una misión constitucional emanada del artículo 217 de la carta magna,

> La Nación tendrá para su defensa unas Fuerzas Militares permanentes constituidas por el Ejército, la Armada y la Fuerza Aérea. Las Fuerzas Militares tendrán como finalidad primordial la defensa de la soberanía, la independencia, la integridad del territorio nacional y del orden constitucional. La Ley determinará el sistema de reemplazos en las Fuerzas Militares, así como los ascensos, derechos y obligaciones de sus miembros y el régimen especial de carrera, prestacional y disciplinario, que les es propio (Constitución Política de Colombia,1991).

motivo por el cual, realiza diferentes tipos de operaciones para satisfacer los intereses de seguridad, defensa y desarrollo de su población, además de consolidar la responsabilidad social y legal.

En consecuencia, con la finalidad de ser una institución innovadora en la administración organizacional y en la ejecución de sus procesos, además de ser eficiente financiera y administrativamente, la Fuerza Aérea Colombiana mediante la Jefatura de Tecnologías de la Información y la Comunicación ha incorporado herramientas tecnológicas y sistemas de información que soportan la ejecución de todos los procesos internos, como los gerenciales, misionales, de soporte y de evaluación y mejora.

Teniendo en cuenta que cada vez son más los servicios de Tecnologías de la Información que soportan los procesos de la Fuerza Aérea Colombiana, la implementación de un gobierno corporativo de TI es una opción que permitirá alinear la estrategia de TI con la institucional, optimizar la utilización de los recursos de TI, aumentar los beneficios esperados de las inversiones realizadas en este aspecto y disminuir los riesgos asociados.

Lo anterior, considerando que el capital de información, es decir, infraestructura y aplicaciones, y los demás recursos de TI, deben ser administrados mediante políticas, planes, procesos, y procedimientos que garanticen que éstos se utilicen eficientemente, de tal manera que sean verdaderos catalizadores para el cumplimiento de los objetivos institucionales.

A pesar de que en la actualidad es común asociar gobierno de TI con alineación entre las estrategias de TI y las institucionales, este concepto no es tan moderno, en razón a que Henderson y Venkatraman (1993) propusieron el modelo de alineación estratégica SAM , el cual estaba basado en la alineación que debería existir entre cuatro dominios claves de una organización, como lo son: (a) estrategia del negocio, (b) procesos e infraestructura organizacional, (c) estrategia de TI, y (d) procesos e infraestructura de TI. (citado en *Oxford University Press*, 1993). Posteriormente, en 1998 fue fundado el instituto de gobernanza de TI (*IT Governance Institute*) con el objetivo de crear conciencia internacional en las direcciones empresariales sobre tecnología de la información, además de asesorar a los directivos de las organizaciones en sus obligaciones de gobernanza de TI, siendo esta la primera vez que se hace propiamente referencia al concepto de Gobierno de TI.

Con relación al ámbito local, el concepto de gobierno de TI fue incorporado desde el 2009, año en que se creó el Ministerio de Tecnologías de la Información y las Comunicaciones mediante la ley 1341. Desde entonces, el Gobierno Nacional ha creado un marco normativo para impulsar y regular el sector emitiendo diversas leyes, decretos, resoluciones, y circulares relacionadas con el Gobierno de TI. Finalmente, La Fuerza Aérea Colombiana, estando alineada

con las políticas del Gobierno Nacional, mediante la disposición 061 del 22 de diciembre de 2017, dio origen a su nueva estructura organizacional, en la cual se crea el Comando de Apoyo a la Fuerza, la Jefatura de las Tecnologías de la Información y la Comunicación, y la oficina de Gobierno Corporativo de TIC.

En este sentido, se hace necesario definir e implementar un modelo de gobierno de TI en la Fuerza Aérea Colombiana con la finalidad de armonizar la estrategia de la Jefatura de las Tecnologías de la Información y la Comunicación con la estrategia de la Fuerza Aérea Colombiana, de manera que los recursos de TI disponibles en la organización soporten el desarrollo de los procesos. De igual manera, la adopción de un gobierno de TI permitirá optimizar la utilización de los recursos de TI, monitorear y evaluar el desempeño de los servicios de TI, potencializar los beneficios esperados de la infraestructura de TI y elaborar un plan de tratamiento de riesgos que permita disminuir los impactos de la materialización de alguno de ellos.

Finalmente, es importante resaltar que la gobernanza de TI es transversal a toda la organización, motivo por el cual, es fundamental que el Gobierno de TI y sus planes estratégicos cuenten con la participación de los altos mandos y en general, de las directivas de la Fuerza Aérea Colombiana.

5. Marco institucional

5.1. Misión

Volar, entrenar y combatir para vencer y dominar en el aire, el espacio y el ciberespacio, en defensa de la soberanía, la independencia, la integridad territorial, el orden constitucional y contribuir a los fines del Estado (Fuerza Aérea Colombiana, 2020).

5.2. Visión

Para ejercer el dominio en el aire, el espacio y el ciberespacio, la Fuerza Aérea será innovadora, polivalente, interoperable, líder y preferente regional, con alcance global y con capacidades disuasivas reales, permanentes y sostenibles (Fuerza Aérea Colombiana, 2020).

5.3. Objetivos estratégicos FAC

5.3.1. Capacidad operacional

Consiste en fortalecer la capacidad operacional, para ejercer y mantener el dominio del espacio aéreo, disuadir la amenaza, derrotar al enemigo y contribuir al logro de los fines del Estado. Se pretende con este objetivo, ir a la vanguardia, innovar, orientar y tener iniciativa en medidas de prevención, disuasión y reacción, para proteger al personal, aeronaves e infraestructura del poder aeroespacial del país, buscando un posicionamiento regional (FAC, 2011).

5.3.2. Desarrollo humano, científico y cultural

Busca mejorar el clima organizacional, a través del impulso al desarrollo humano, científico, tecnológico y cultural, para ser líder en el ámbito aeroespacial nacional. De igual manera, fomentar la formulación, ejecución, evaluación y difusión de proyectos de investigación, desarrollo tecnológico e innovación que permitan proponer soluciones a las necesidades institucionales (FAC, 2011).

5.3.3. Responsabilidad social y legal

Responsabilidad Social para la Fuerza Aérea, es el compromiso con la misión constitucional y de su efectividad depende el impacto en la sociedad. Sin embargo, además de responder por la seguridad de la Nación mediante las operaciones aéreas y respetando el marco de los Derechos Humanos y el Derecho Internacional Humanitario, también desarrolla diferentes actividades que impactan la sociedad como es el cuidado del ambiente y la interacción y colaboración con la comunidad, a través de campañas de acción integral y jornadas de tipo humanitario que fortalecen las relaciones con las partes interesadas de la Fuerza (FAC, 2011).

5.3.4. Responsabilidad administrativa

Este objetivo consiste en consolidar una gestión ética y una cultura organizacional de integridad, transparencia y eficiencia para obtener el mejor provecho durante el empleo de los recursos humanos, materiales y tecnológicos, y el logro de excelentes resultados operacionales y al mismo tiempo mantener la confiabilidad en la rendición de cuentas (FAC, 2011).

5.4. Estructura organizacional

La Fuerza Aérea Colombiana para desarrollar las funciones propias de la entidad y para una buena administración de los recursos en el desarrollo de la operación, ha agrupado las funciones en 5 procesos, los cuales mediante la filosofía de “enfoque basado en procesos”, determina y gestiona de manera eficaz las diferentes actividades relacionadas entre sí, manteniéndose el control continuo entre los vínculos y los procesos, así como en su combinación e interacción. Lo anterior, con el fin de mejorar la satisfacción ciudadana y el desempeño de la Fuerza Aérea Colombiana. Los 5 procesos a su vez se reagruparon en cuatro tipos de procesos: Gerenciales, Misionales, Soporte y Evaluación y Mejora, para conformar el Mapa de Procesos de la Fuerza Aérea (FAC, 2011).

5.4.1. Procesos gerenciales

El direccionamiento estratégico de la Fuerza Aérea Colombiana actualiza permanentemente la estrategia de la Fuerza y proporciona la alineación de los diferentes componentes organizacionales con el propósito de acercar a la Fuerza al cumplimiento de su misión. La actualización permanente de la estrategia comprende la revisión y ajuste de los objetivos, los procesos y las iniciativas estratégicas dentro del entorno estratégico en que se desenvuelve la institución. La alineación organizacional enfoca las actividades y recursos de la Fuerza para desarrollar sinergias que la potencialicen (FAC, 2011).

5.4.2. Procesos misionales

El proceso misional de la Fuerza Aérea es Operaciones Aéreas, el cual está asociado con el ámbito de las operaciones militares. Para ello debe planear, conducir, ejecutar y evaluar las operaciones aéreas con acciones de mejora continua, para la seguridad y defensa de la nación, por medio del cumplimiento de sus funciones típicas del control del espacio aéreo, tendiente a dominar el teatro de operaciones, la aplicación de la fuerza como sinónimo de emplear el poder de combate, multiplicación de la fuerza para aumentar la efectividad del combate y apoyo a la fuerza para sostener su operación. En términos de las finalidades de desarrollo social y el servicio a la comunidad, el proceso de operaciones aéreas desarrolla operaciones no relacionadas con la guerra para apoyar a la población en caso de desastres naturales, participar en las actividades de protección del medio ambiente, en las operaciones de búsqueda y rescate en caso de accidentes y naufragios (FAC, 2011).

5.4.3. Procesos de soporte

El proceso de gestión de apoyo se compone de una serie de actividades, que van desde la recepción de las necesidades logísticas, hasta la entrega de aeronaves, equipo asociado y su equipo de apoyo confiables y seguros para desarrollar las operaciones aéreas. El proceso de gestión humana, en el acrecentamiento y conservación del esfuerzo, las experiencias, los conocimientos y las habilidades de los miembros de la organización, en beneficio del individuo,

de la propia organización y del país en general. El proceso de ayudar a los empleados a alcanzar un nivel de desempeño y una calidad de conducta personal y social que cubra sus necesidades (FAC, 2011).

5.4.4. Procesos de evaluación y mejora

Conjunto de actividades sistemáticas y secuenciales que tienen como objetivo verificar el cumplimiento de los patrones establecidos por la institución, la aplicación de la normatividad legal que orienta y regula la actuación pública en el ejercicio de las funciones y en general de todos los lineamientos, programas, planes y políticas establecidos por la alta dirección como marco de referencia para el cumplimento de la misión, de las funciones y logros de los objetivos estratégicos (FAC, 2011).

5.5. Posición en el mercado

La Fuerza Aérea Colombiana pertenece al sector económico terciario o de servicios, en razón a que es una organización gubernamental que apoya el desarrollo económico y social del país y que tiene la responsabilidad de satisfacer los intereses de seguridad, defensa y desarrollo de su población, siendo sus principales clientes la sociedad colombiana, las entidades del estado y las demás Fuerzas Militares. Así mismo, dispone de capacidades propias del poder aéreo, las cuales la hacen diferente a las demás Fuerzas Militares y de Policía de Colombia. Algunas de las actividades distintivas más significativas de la organización son la conducción de operaciones aéreas estratégicas, el desarrollo de operaciones de defensa aérea y control del espacio aéreo, el apoyo aéreo cercano, el transporte aéreo militar, puentes aéreos y transporte de personalidades del gobierno, ejercer de autoridad aeronáutica de la aviación de Estado y reacción eficaz ante emergencias nacionales o desastres naturales. De igual manera, para promover el desarrollo social y económico del país, la Fuerza Aérea tiene bajo su responsabilidad la dirección de SATENA[1] y de la CIAC[2].

[1] Servicio Aéreo a Territorios Nacionales
[2] Corporación de la Industria Aeronáutica Colombiana

SATENA es una sociedad de economía mixta que cubre las regiones más apartadas y de difícil acceso del territorio nacional, siendo la única alternativa de transporte aéreo en esos lugares, acortando distancias entre las poblaciones y los centros de desarrollo. Por su parte, la CIAC es una empresa líder en la industria aeroespacial nacional con base en su condición de fabricante de productos aeronáuticos y de estación reparadora que ha desarrollado proyectos como la modernización de las aeronaves de entrenamiento T-27, que consiste en actualizar la aviónica de análogo a digital.

Con relación a las demás organizaciones que pertenecen al sector de seguridad y defensa nacional, la imagen de favorabilidad de la Fuerza Aérea Colombiana ocupa el primer lugar, con un porcentaje de aceptación del 83%, según los datos publicados en abril de 2018 por la encuesta Pulso País realizada por DATEXCO (Pulso País, 2018).

5.6. Sector de seguridad y defensa Nacional

El sector de Seguridad y Defensa Nacional, en cabeza del Ministerio de Defensa, tiene la responsabilidad de contribuir a la gobernabilidad democrática, la prosperidad colectiva y la erradicación de la violencia, mediante el ejercicio de la seguridad y la defensa, la aplicación adecuada y focalizada de la fuerza y el desarrollo de capacidades mínimas disuasivas. Su nivel de cumplimento, se mide en base a indicadores de eficiencia como secuestros, extorsión, hectáreas de coca destruidas, homicidios, entre otros.

Para cumplir con la misión, el Ministerio cuenta con una Secretaria General, además del viceministro para las Políticas y Asuntos Internacionales, el viceministro para la Estrategia y Planeación y el viceministro del Grupo Social Empresarial del Sector Defensa ‘GSED’ y Bienestar.

Así mismo, tiene adscritas diversas organizaciones centralizadas como el Comando General de las Fuerzas Militares, el Ejército Nacional, la Armada Nacional, la Fuerza Aérea Colombiana, la Dirección de Policía Nacional y la Dirección de Policía Judicial e Investigación (DIJIN[3]), además de algunas entidades descentralizadas, las cuales conforman un grupo social y empresarial de la defensa encaminadas a prestar apoyo logístico, entre los cuales están la

[3] Dirección de Policía Nacional y la Dirección de Policía Judicial e Investigación

Agencia Logística de la Fuerzas Miliares, la Industria Militar de Colombia (INDUMIL[4]), La Corporación de la Industria Aeronáutica Colombiana (CIAC), El Fondo Rotatorio de la Policía Nacional, y la Corporación de Ciencia y Tecnología para el Desarrollo de la Industria Naval, Marítima y Fluvial (COTECMAR[5]). Del mismo modo, otras organizaciones igualmente descentralizadas, están constituidas para apoyar la seguridad, entre las cuales están la Superintendencia de Vigilancia y Seguridad Privada, la Defensa Civil Colombiana, el Servicio Aéreo a Territorios Nacionales (SATENA) y la Corporación de Alta Tecnología.

Los lineamientos del Sector de Seguridad y Defensa Nacional, están definidos en la POLÍTICA DE DEFENSA Y SEGURIDAD TODOS POR UN NUEVO PAÍS, la cual tiene como objetivo general: "Coadyuvar a la terminación del conflicto armado, la consolidación de la paz, el desarrollo socioeconómico, la defensa de los intereses nacionales y el mejoramiento de la seguridad pública y ciudadana, mediante el mantenimiento de una Fuerza Pública moderna, fortalecida, motivada y operativa" (Ministerio de Defensa, 2015, p. 15).

En la política de Seguridad y Defensa Nacional, se han definido ocho áreas misionales, las cuales abarcan las responsabilidades del sector Defensa y definen las funciones estratégicas del sector. Las áreas misionales se describen brevemente a continuación:

- Convivencia y Seguridad Ciudadana: acciones encaminadas a garantizar los derechos, libertades, desarrollo social y proyección humana, con esfuerzos coordinados con las autoridades político-administrativas, que satisfagan las necesidades de los habitantes.
- Seguridad Pública: acciones encaminadas a asegurar el accionar de la Fuerza Pública en todo el territorio nacional para neutralizar y desarticular los actores ilegales y sus manifestaciones conexas organizadas nacionales y trasnacionales que atenten contra los intereses nacionales.
- Defensa Nacional: acciones encaminadas a proteger la soberanía y la integridad territorial en los dominios terrestre, marítimo, fluvial, aéreo, espacial y ciberespacial

[4] Industria Militar de Colombia

[5] Corporación de Ciencia y Tecnología para el Desarrollo de la Industria Naval, Marítima y Fluvial

frente a cualquier tipo de agresión sea interna o externa, convencional o no convencional.

- Gestión del Riesgo de Desastres: acciones para contribuir a la prevención, atención y mitigación del riesgo de desastres a nivel nacional en el marco del Sistema Nacional de Gestión del Riesgo de Desastres (SNGRD).
- Cooperación Internacional: acciones para fortalecer alianzas estratégicas que permitan dar una respuesta integral a las amenazas comunes de los Estados, a través del intercambio de bienes, conocimientos, tecnologías y mejores prácticas en materia de seguridad y defensa de forma sostenida y sustentable.
- Protección de los recursos naturales y del Medio Ambiente: acciones para prestar apoyo a las autoridades ambientales, a los entes territoriales y a la comunidad, en la defensa y protección del medio ambiente y los recursos naturales renovables y no renovables, en las funciones y acciones de control y vigilancia previstas por la ley.
- Contribución al Desarrollo del país: acciones en campos como el transporte, la construcción, las telecomunicaciones y la tecnología e innovación, que permitan promover el papel de la Fuerza Pública en el desarrollo económico y social de la Nación.
- Gestión, apoyo y desarrollo proyectivo: proveer funciones comunes de dirección, administración y gestión en el Sector de Defensa y Seguridad para el desarrollo de la infraestructura logística, desarrollo tecnológico, gestión del talento humano y potenciación del conocimiento, así como garantizar la legitimidad de las acciones de la Fuerza Pública (Ministerio de Defensa, 2020).

5.7. Presupuesto de la seguridad y defensa Nacional

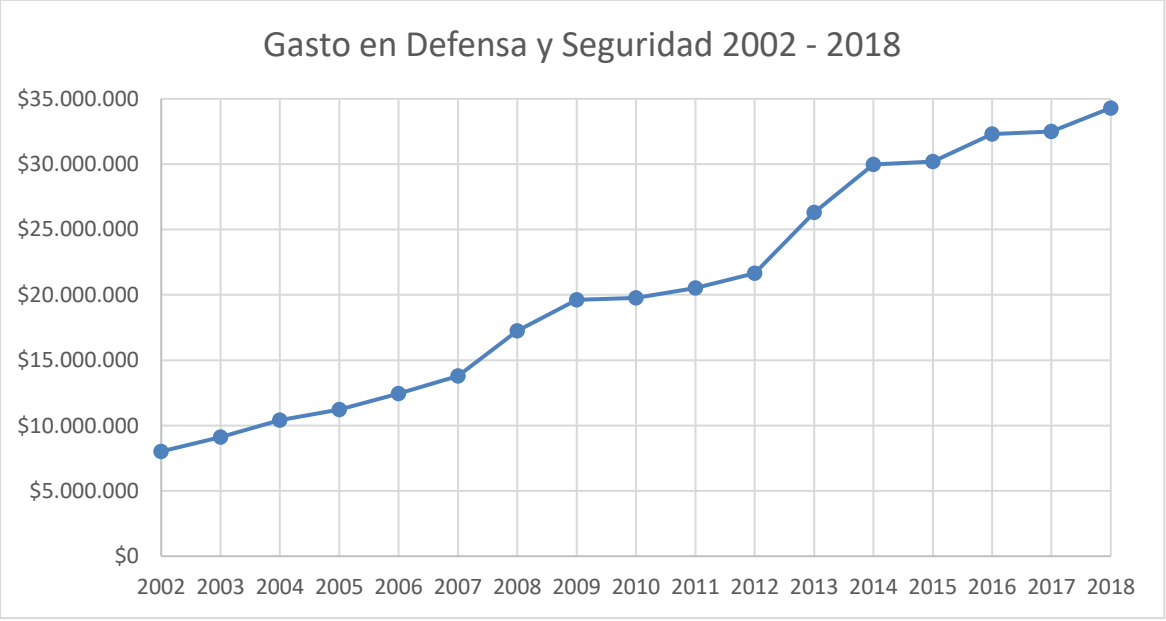
El Estado Colombiano, en pro de proteger sus intereses nacionales, defender la soberanía, el orden constitucional, la integridad territorial y velar por la seguridad de sus habitantes, además de impulsar el desarrollo económico mediante la inversión de multinacionales extranjeras, lo que impactaría en el crecimiento mercantil del país, ha desarrollado una política de seguridad y defensa, haciendo esfuerzos económicos importantes al destinar gran parte del presupuesto de la nación para tal fin. En los últimos años, se han asignado más recursos a la cartera de defensa,

debido al aumento del personal de la Fuerzas Armadas y la adquisición de nuevos sistemas de armas.

El Ministerio de Defensa Nacional y el Departamento Nacional de Planeación trabajan conjuntamente en la asignación de presupuesto para el gasto en Defensa y Seguridad, basados en un documento llamado “Metodología para el Cálculo del Gasto en Defensa y Seguridad”, el cual define que:

> El concepto de los gastos destinados a asuntos de Defensa y Seguridad involucra todas las erogaciones que hace el país con el fin de mantener la paz y la seguridad pública. Esto implica tener en cuenta todos los recursos utilizados para tal fin, tanto los asignados al sector a través del Presupuesto General de la Nación, como aquellos recibidos a través de programas de cooperación internacional como el Plan Colombia, los diferentes proyectos que se realizan particularmente con los sectores minero y energético a través de convenios, o el gasto en seguridad y vigilancia que realiza el sector privado, entre otros. Sin embargo, dado que el interés es medir el esfuerzo que hace el Gobierno Nacional en el Sector Defensa y Seguridad, el análisis del GDS se enfocará en el presupuesto asignado por la nación a través de la ley anual respectiva, para las entidades que lo conforman. (Ministerio de Defensa Nacional. Departamento Nacional de Planeacion, 2008). En el gráfico 2 se ilustra el gasto de defensa en millones de pesos colombianos desde 2002 hasta 2018.

Gráfico 2: Gasto de Defensa y Seguridad 2002 – 2018



Fuente: Elaboración propia, Datos Tomados MDN

El presupuesto general de la nación para el año 2015 fue de $203.6 billones de pesos, de los cuales, $30.2 billones fueron destinados al sector Defensa, lo que equivale al 14.8%. A su vez, a la Fuerza Aérea Colombiana le asignaron $1.4 billones, lo que representa el 4.8%, siendo el porcentaje más bajo del presupuesto asignado a las Fuerzas Militares, en razón a que al Ejercito le fue entregado el 22.1% del presupuesto, que equivale a 6.7 billones de pesos y a la Armada Nacional el 5.4%, que representan $1.6 billones de pesos.

Para la vigencia 2016, el presupuesto general de la nación fue de $215.9 billones de pesos, de los cuales se le asignó el 14.9% al sector defensa, lo que equivale a $32.3 billones de pesos. A la Fuerza Aérea Colombiana, se le asigno $1.38 billones de pesos, que corresponden al 4.27%. En comparación al presupuesto asignado al año anterior, hubo una reducción de 1.42%. En el 2017, el presupuesto general de la nación fue de $224.4 billones de pesos, de los cuales se asignaron 32.5 billones para el sector defensa, lo que equivale al 14.4%. A la Fuerza Aérea, se le asigno $1.38 billones de pesos, lo que equivale al 4.2% del presupuesto total del sector. El presupuesto general de la Nación aprobado para el 2018 fue de 235 billones de pesos, de los cuales le asignaron $34.29 billones al sector de Defensa Nacional, lo que equivale al 14.5%. A su vez, a la Fuerza Aérea, le asignaron $1.36 billones de pesos, que representa el 3.9%.

De las cifras anteriores, se puede inferir que la Fuerza Aérea Colombiana, en los últimos cuatro años, ha recibido el menor presupuesto de las Fuerzas Militares. No obstante, de los recursos asignados en el 2018, el 88.9% están reservados para los gastos de funcionamiento, mientras el 11.1% podrá ser utilizado en proyectos de inversión. Para la misma vigencia, al Ejercito Nacional se le asignó el 22,3% del presupuesto de defensa, pero 96.86% está destinado para los gastos de operación, y solo podrán invertir el 3.14%. De igual manera, a la Armada Nacional, se le adjudicaron el 4.6% de los recursos, de los cuales, el 90.6% son gastos de funcionamiento y el 9.4% está destinado para proyectos de inversión. En conclusión, aunque la Fuerza Aérea ha recibido la menor parte del prepuesto de defensa, ha destinado el mayor porcentaje en proyectos de inversión (Ministerio de defensa, 2020).

6. Marco teórico

En los párrafos siguientes, se revisará la literatura en la cual se fundamenta la investigación, haciendo referencia a diferentes artículos, estándares y mejores prácticas relacionados al tema objeto de estudio; los cuáles serán utilizados como referencia para alcanzar los objetivos propuestos. La idea principal de la investigación es elaborar una propuesta para la implementación de un gobierno corporativo de TI en la Jefatura de las Tecnologías de la Información y Comunicaciones de la Fuerza Aérea Colombiana, de manera que se potencialice la infraestructura de TI como una herramienta para soportar los procesos de manera eficiente y de esta forma, alcanzar los objetivos institucionales.

6.1. Tecnologías de la información y las comunicaciones

En primer lugar, es importante mencionar que la globalización y las tecnologías de la información y las comunicaciones han impactado en el desarrollo y crecimiento de las sociedades y sus economías. La sociedad actual, se caracteriza por los avances tecnológicos, los cuales cada vez suceden con mayor velocidad, motivo por el cual, se incrementa la necesidad de adoptar estrategias para incorporar en la cotidianidad de las organizaciones dichas tecnologías, con el objetivo de asegurar la sostenibilidad, eficiencia, rentabilidad y productividad, además de aumentar la capacidad competitiva y de innovación.

En relación con la competitividad de las organizaciones, es importante construir una ventaja competitiva sostenible en un mercado identificable, junto a una estrategia a nivel corporativo, que debe pertenecer a la visión general de una empresa diversificada (Furrer, 2010). Por su parte, Porter aduce que la competitividad de una nación depende de la capacidad de su industria para innovar y que una empresa logra ventaja competitiva cuando realiza de forma sostenible innovaciones para el mercado (Porter, 1990). De igual manera, la competitividad es una variable multifactorial que está relacionada con la formación empresarial, las habilidades administrativas, laborales y productivas, la gestión, la innovación y el desarrollo tecnológico (Corona, 2002).

Por otro lado, las tecnologías de la información y las comunicaciones se han convertido en un activo fijo intangible que generan valor diferenciador a las organizaciones, siendo un catalizador de los procesos organizacionales, los cuales se constituyen en herramientas de apoyo a la gestión

empresarial, apalancando el diseño de estrategias orientadas a la competitividad y la innovación, generando así sostenibilidad para la organización y la sociedad (Stern, 2002). De la misma manera, las TIC se constituyen en un recurso estratégico para las organizaciones, las cuales benefician a las instituciones a encontrar nuevas oportunidades en el mercado, con bajos costos y alta probabilidad de éxito (Shin, 2007).

Así mismo, las TIC son un conjunto de tecnologías capaces de producir, almacenar y transmitir información digital (Schiavo, 2007). De igual manera, el Ministerio de las tecnologías de la información y las comunicaciones señala que, las TIC se pueden precisar como el conjunto de recursos, herramientas, equipos, programas informáticos, aplicaciones, redes y medios, que permiten la compilación, procesamiento, almacenamiento y transmisión de información como: voz, datos, texto, video e imágenes (Ley 1341, 2009). Del mismo modo, la *Information Technology Association of America* – ITAA-, citado en Barragán, (2009), señala que las TIC se pueden precisar como el estudio, diseño, desarrollo, fomento, mantenimiento y administración de la información por medio de sistemas informáticos, motivo por el cual, la información adquiere un valor relevante en los procesos organizacionales, que debe ser gestionada de manera eficiente mediante la implementación de herramientas tecnológicas que garanticen la disponibilidad, confiabilidad e integridad de la misma, con la finalidad de generar, compartir y utilizar el conocimiento existente, para contribuir a dar solución a las necesidades organizacionales.

En relación con lo anterior, Drucker (2000) citado en Bernal, et al, (2012), señala que la administración de conocimiento requiere necesariamente de la tecnología de la información y la comunicación para optimizar su apropiación, generación y uso como ventaja competitiva empresarial. De igual manera, Quinn, Anderson & Finkelstein (1996) citados en Bernal, et al, (2012), señalan que para que el conocimiento genere verdadero valor a la organización, debe estar soportado en una infraestructura tecnológica que permita crear, consolidar y compartir el conocimiento.

6.2. Gobierno de TI

Sin embargo, el acceso, uso y adopción de las TIC constituye una condición necesaria pero no suficiente para mejorar la productividad y competitividad de las organizaciones (Wolf & Pilat, 2004). De igual manera, aunque la infraestructura tecnológica es fundamental para la

organización, ésta por sí sola no representa una ventaja competitiva, sino que debe estar apoyada por un plan estratégico que defina el objetivo de las TIC y de esta manera, potencializar el efecto de las TIC en la organización (Bhatt & Grover, 2005). En consecuencia, se hace necesario constituir un gobierno corporativo de las TIC, que administre la infraestructura y los servicios de TI de la organización, con la finalidad de proteger los activos y garantizar que los recursos de TI sean usados responsablemente bajo un marco regulatorio, de manera que se haga un uso eficiente de ellos para el cumplimento de los objetivos corporativos y que, al mismo tiempo, se minimicen los riesgos asociados.

En relación a lo anterior, el Gobierno de Tecnologías de Información es un conjunto de políticas, procesos y procedimientos definidos para gestionar y monitorear la infraestructura de TI de una organización, con el fin de alcanzar sus objetivos mediante la generación de valor agregado, la administración del riesgo y el análisis del retorno de la inversión sobre TI (Verhoef, 2007). De la misma manera, *IT Governance Institute* define que el gobierno de TI es parte integral de la junta directiva y de la dirección ejecutiva, que a su vez conforma el gobierno corporativo y consiste en el liderazgo, los procesos y las estructuras que aseguran que las tecnologías de la organización apoyen los objetivos y estrategias de la empresa (ITGI, 2007).

De manera similar, la gobernanza de TI es un conjunto de objetivos, principios, organigramas, políticas y reglas que definen o limitan lo que pueden hacer los gerentes del área (Rahimi et al., 2016). Igualmente, Muñoz y Ulloa (2011) citados por Marulanda, et al, (2017), señalan que el gobierno de TI es la estructura de relaciones y procesos para dirigir la organización para alcanzar los objetivos, mediante la agregación de valor y el balance entre el riesgo y el retorno sobre las TI y sus procesos (Muñoz & Ulloa, 2011). Lo anterior se obtiene al integrar e institucionalizar las buenas prácticas para garantizar que las TI soporten los objetivos del negocio y facilitar que la empresa aproveche al máximo su información mediante la maximización de los beneficios, la capacitación de las oportunidades y el aprovechamiento de las ventajas competitivas.

De igual forma, se puede definir el Gobierno de TI como “el alineamiento estratégico de las TI con la organización de forma tal que se consigue el máximo valor de negocio por medio del desarrollo y mantenimiento de un control y responsabilidades efectivas, gestión del desempeño y gestión de riesgos de las TI” (Webb et al., 2006, p. 7), generando algunos elementos relevantes

para las organizaciones, tales como, el alineamiento estratégico, la entrega de valor de negocio a través de las TI, la gestión del desempeño, la gestión de riesgos y el control y responsabilidades.

Consecuentemente, el concepto de gobierno de TI se puede precisar como una parte del gobierno corporativo que lidera y controla los recursos de TI, mediante un conjunto de procesos, procedimientos, planes y políticas, las cuales permiten alinear los objetivos de TI con los corporativos, reducir la incertidumbre o riesgo, generar valor agregado y lograr un mejor desempeño de los recursos de TI, de manera que éstos soporten los objetivos del negocio y faciliten a la organización obtener el máximo beneficio de las inversiones realizadas en TI.

Considerando que el gobierno de TI emite los procesos, procedimientos, planes y políticas para la administración de los recursos de TI, la comunicación adquiere una relevancia significativa, en razón a que ésta es la base para que un gobierno de TI sea efectivo (Marulanda Echeverry et al., 2017). Ésta debe ser clara, se debe realizar mediante un lenguaje común entre las partes interesadas, y debe fluir de manera precisa en todas las direcciones de la organización.

Continuando con este análisis, de acuerdo con el Centro de Investigación de Sistemas de Información (CISR) citado en Harkins, (2013), el gobierno de TI puede definirse como un marco para los derechos de decisión y la rendición de cuentas para fomentar un comportamiento deseable en el uso de TI. En este sentido, la gobernanza puede describirse como la gestión estratégica de la organización, toda vez que los actores que están a cargo del gobierno de TI están tomando las grandes decisiones relacionadas con las políticas que impulsarán la organización al cumplimiento de sus objetivos, dado que los ejecutivos de TI establecen prioridades, políticas y programas que ayudan a los empleados de todos los niveles a alcanzar estos objetivos (Earth & Sky, 2016).

Por su parte, la gestión del gobierno de TI debe alinear los procesos, los recursos y la información de TI, con las estrategias y los objetivos de la organización mediante la implementación de mejores prácticas o marcos de referencias, que permitan hacer un uso responsable de los recursos de TI, además de monitorear y evaluar el rendimiento de los servicios proporcionados por TI para asegurar que la información de la organización y las tecnologías relacionadas soporten los objetivos de negocio. En este sentido, Carrillo (2009) citado en Muñoz y Villegas, (2011), señala que los principales objetivos de un gobierno de TI son (a) proveer dirección estratégica a la organización, (b) asegurar el logro de los objetivos, (c) establecer que

los riesgos se administran adecuadamente y, (d) verificar que los recursos de la empresa se utilizan responsablemente.

De la misma manera, Bowen, Decca y Rohde (2007) citados en Marulanda, et al, (2017) señalan que el gobierno de TI incluye tres dimensiones: estructura de gobierno de las tecnologías, el proceso de gobernabilidad y las métricas de resultados. La estructura de gobierno de TI es la parte del gobierno de TI que realiza la alineación de la estrategia y los objetivos de TI con los organizacionales. El proceso de gobierno de TI se focaliza en establecer las políticas y procedimientos para la ejecución de proyectos de inversión. Finalmente, las métricas de resultados de TI son los responsables de evaluar el gobierno de TI, además de la estructura y los procesos para asegurar que los resultados deseados sean alcanzados. De manera similar, el gobierno corporativo provee la estructura a través de la cual se establecen los objetivos de la empresa, los medios para alcanzar estos objetivos, así como la forma de hacer un seguimiento a su desempeño (OCDE, 2004).

Por esta misma línea, *IT Governance Institute* señala que las actividades del gobierno de TI se pueden agrupar en cinco áreas fundamentales: (a) Alineación estratégica, (b) entrega de valor, (c) administración de recursos, (d) administración del riesgo y, (e) medición de desempeño (IT Governance Institute, 2007). La Alineación estratégica se encarga de alinear los planes de la organización con los de TI, además de definir, mantener y validar la generación de valor que TI genera a la organización. En la entrega de valor se ejecuta la propuesta de valor a través de todo el ciclo de entrega, de manera que se asegure que TI entrega los beneficios definidos en la estrategia, centrándose en optimizar los costos. En la entrega de valor de TI se materializa la entrega a tiempo de los servicios de TI definidos en el acuerdo de servicios. La administración de recursos está relacionada con la inversión óptima y con la adecuada administración de los recursos críticos de TI tales como aplicaciones, información, infraestructura y datos. La administración de riesgos se refiere a la necesidad que tiene la administración de tener un panorama claro de los posibles riesgos que se pueden presentar en la organización, además de la implementación de un plan de tratamiento de riesgos que minimicen los efectos de la materialización de este sobre el cumplimiento de los objetivos. En último lugar, en la medición del desempeño se efectúa la valoración de la estrategia implementada, evaluando la utilización de los recursos, el desempeño de procesos y la entrega de servicio. En este sentido, es importante

definir los indicadores que permitan medir la eficiencia y la entrega de valor que generan los recursos de TI a la organización.

Por otro lado, Hardy (2006) citado en Marulanda, et al, (2017), señala que es responsabilidad del gobierno corporativo de TI emitir un marco general de las políticas de la organización, que estén soportadas en los principios de gobierno corporativo y que incluyan revisar y guiar la estrategia corporativa, establecer y seguir los objetivos de gestión del rendimiento y garantizar la integridad de los sistemas de la organización. En consecuencia, se deben armonizar las dos estrategias, estrategia corporativa y estrategia de TI, se debe garantizar la infraestructura para soportar las estrategias y metas, y se deben implementar métricas para monitorear y evaluar el desempeño de los servicios de TI.

Finalmente, considerando que los desarrollos tecnológicos avanzan a pasos agigantados, por consiguiente, los contextos de la industria también lo hacen rápidamente, motivo por el cual, las organizaciones que quieren ser sostenibles en el tiempo deben tener suficiente flexibilidad para aprender y adaptarse al entorno a la misma velocidad que éste lo hace. No obstante, este cambio se debe hacer de manera controlada, siguiendo una dirección estratégica basada en estándares o buenas prácticas. Por la razón anterior, en los párrafos siguientes, se abordarán algunos conceptos relacionados con los marcos de referencia o buenas prácticas de gobierno de TI.

6.3. Marcos de referencia

Los elementos del gobierno de TI están definidos en los estándares, marcos de referencia y buenas prácticas, los cuales contienen la metodología para hacer uso eficiente, efectivo y aceptable de las tecnologías de información. A pesar de que en la literatura se encuentra un número importante de marcos de referencia para dar soporte a la implementación de distintos aspectos del gobierno de TI, en el desarrollo de la investigación se seleccionaron los marcos de control COBIT e ISO 38500 y las normas o estándares de gobierno TI como PMBOK, ISO 27000, ITIL, toda vez que son estándares internacionalmente aceptados e implementados por diferentes industrias para la gestión eficiente de los recursos de TI.

6.3.1. COBIT 5

Inicialmente, COBIT es un marco de referencia para el gobierno de TI que define los requerimientos de control, los aspectos técnicos y los riesgos de negocio. Para COBIT, la implementación del gobierno de TI permite a las organizaciones alinear las estrategias de TI con la estrategia de la organización, disminuir el impacto del riesgo, proporcionar estructuras organizacionales que faciliten la implementación de estrategias y metas, además de medir el desempeño de TI. COBIT se basa en cinco principios para el gobierno y la gestión de TI en las organizaciones: (a) satisfacer las necesidades de las partes interesadas, (b) cubrir la empresa de extremo a extremo, (c) aplicar un marco de referencia único integrado, (d) hacer posible un enfoque holístico y (e) separar el gobierno de la gestión.

En este mismo sentido, en la búsqueda del equilibrio de la generación de beneficios que impactan el gobierno de TI, la correcta definición y mitigación de niveles de riesgo y la definición de políticas que regulen el uso eficiente de recursos, el modelo COBIT dentro de su estructura incluye el concepto de modelos de madurez, donde se tiene en cuenta el nivel de desarrollo de la capacidad en la organización, factores críticos de éxito considerando sus capacidades y generalidades e indicadores que permitan una medición y evaluación de los procesos en cada uno de sus dominios (Rodenes y Bauset, 2009).

Así mismo, COBIT en su versión 5, a nivel operacional para el dominio de gobierno de TI contiene 37 procesos dentro de los cuales cinco procesos son de gobierno corporativo (a) EDM01: Asegurar el establecimiento y mantenimiento del marco de referencia de gobierno, donde los requerimientos para el gobierno de TI ejecutan y mantiene las estructuras, procesos y prácticas facilitadoras, junto a sus responsabilidades y la autoridad que se debe asignar para cumplir la misión, metas y objetivos de la organización. (b) EDM02: Asegurar la entrega de beneficios, busca contribuir al foco del negocio dando valor desde los procesos de negocios, servicios de TI y activos de TI desde una perspectiva financiera aceptable, donde lo invertido y los costos se encuentran alineados con la estrategia de TI. (c) EDM03: Asegurar la optimización del riesgo, en los que las necesidades y la tolerancia al riesgo son comprendidos, aceptados y divulgados al interior de la organización y de igual manera el riesgo es identificado y gestionado. (d) EDM04: Asegurar la optimización de recursos, en el que las personas, procesos y tecnologías,

cuentan con las capacidades necesarias para soportar y ejecutar los objetivos de la empresa a un coste óptimo. (e) EDM05: Asegurar la transparencia hacia las partes interesadas, donde los mecanismos de medición de las TI cuentan con sus respectivos informes, aprobaciones en cuanto a conformidad y desempeño en el que se evidencia su transparencia, y en el que las partes interesadas entienden las metas, las métricas y las acciones correctivas necesarias (ISACA, 2012).

6.3.2. ISO/IEC 27001: 2013.

De manera semejante, ISO/IEC 27001: 2013 establece los requerimientos de un sistema de gestión de la seguridad de la información; además de ayudar a identificar, gestionar y minimizar el rango de amenazas a las cuales está expuesta regularmente la información. Así mismo, está diseñado para asegurar que la selección de controles se realice de manera adecuada, con la finalidad de proteger los activos de información, además de brindar confianza a las partes interesadas, incluyendo los clientes de la organización. Éste estándar define una metodología de gestión de la seguridad clara y estructurada, que permite reducir el riesgo de pérdida, robo o corrupción de la información, generando confianza entre las partes interesadas al garantizar la calidad, disponibilidad, integridad y confidencialidad de la información. De igual modo, establece medidas para gestionar los riesgos, los cuales son revisados permanentemente para asegurar la continuidad del negocio tras la ocurrencia de algún tipo de incidente.

El uso de la norma internacional ISO / IEC 27001, permite la planificación e implementación exitosa de sistemas para asegurar la gestión de la seguridad de la información, donde los activos de información son valorados y si llega tener una perturbación, se da un tratamiento contra los ataques y amenazas de seguridad a estos activos, estos se representan como eventos que resultan de una distorsión en los requisitos básicos de seguridad, tales como confidencialidad, integridad y disponibilidad de la información, de aquí la necesidad de implementar medidas que aseguren de forma física, técnica y administrativa esta información, esto involucra una evaluación de riesgos, determinando el nivel óptimo de seguridad en términos de rentabilidad y costos, acelerando la implementación de las medidas de seguridad necesarias (Luka, 2019).

6.3.3. ITIL V3

ITIL es un conjunto de guías que fueron desarrolladas en 1980 por la oficina de comercio del Reino Unido. Su objetivo principal es alinear los servicios de TI a las necesidades y los procesos de la organización. Es una herramienta administrativa y de gestión, la cual permite incursionar exitosamente en los múltiples ámbitos de competitividad. De igual manera, proporciona un conjunto de buenas prácticas, las cuales orientan a las organizaciones en el proceso de adaptación o implementación de un marco de referencia para la administración de los servicios de TI, permitiendo identificar los servicios necesarios para el cumplimiento de los objetivos, así como optimizar la calidad de los servicios de TI. Igualmente, tiene un conjunto de guías claras y comprensibles para la definición, el diseño, la implementación, y mantener una gestión de procesos para los servicios de TI. En consecuencia, los objetivos de este marco de referencia son: (a) identificar los procesos de la organización que son soportados por los servicios de TI, (b) mejorar la calidad de los servicios de TI, (c) mejorar la entrega de servicios, como una parte integral de un todo de los requerimientos de negocio para una calidad en la gestión de TI y (d) asegurar que los clientes tengan acceso a los servicios apropiados para soportar las funciones del negocio.

De igual manera, contemplando el conjunto de buenas prácticas, se deben considerar los indicadores representativos que contrastan la eficiencia en la provisión del servicio contra la disponibilidad de los servicios críticos, así mismo, los indicadores relacionados con la capacidad, disponibilidad y continuidad de los servicios, todos ellos recogidos en la fase de diseño de ITIL del ciclo de vida del servicio, otro indicador contrastado ha sido la satisfacción del usuario, el cual analiza el proceso de relaciones con el negocio enmarcado en la fase de estrategia de ITIL, por último el indicador contrastado que influye sobre el aporte de valor, es el control de los servicios, donde el inventario de activos y gestión eficiente de los cambios, así como el control de los servicios de TI está enmarcado en la fase de transición, incluyendo los procesos de gestión del cambio y gestión de la configuración (Rodenes & Bauset, 2009).

6.3.4. PMBOK. 5ª EDICIÓN

Por otro lado, PMBOK es un estándar desarrollado por PMI (*Project Management Institute*) que define pautas para la dirección de proyectos, además de los conceptos relacionados con los mismos. Esta guía, identifica las buenas prácticas en relación con la aplicación de los recursos disponibles, tales como conocimientos, procesos, habilidades, herramientas y técnicas, las cuales, al ser utilizadas de manera adecuada, generan un impacto positivo en la ejecución de los proyectos. Otra característica importante de PMBOK es que integra y promueve un lenguaje común para el uso y aplicación de los conceptos de la dirección de proyectos entre todas las partes interesadas. PMBOK contiene dos grandes secciones, la primera se enfoca en los procesos y contextos de un proyecto, la segunda lo hace sobre las áreas de conocimiento específico para la gestión de un proyecto. Así mismo, describe el ciclo de los proyectos en términos de la integración entre los procesos, de sus interacciones y de los propósitos a los que responden.

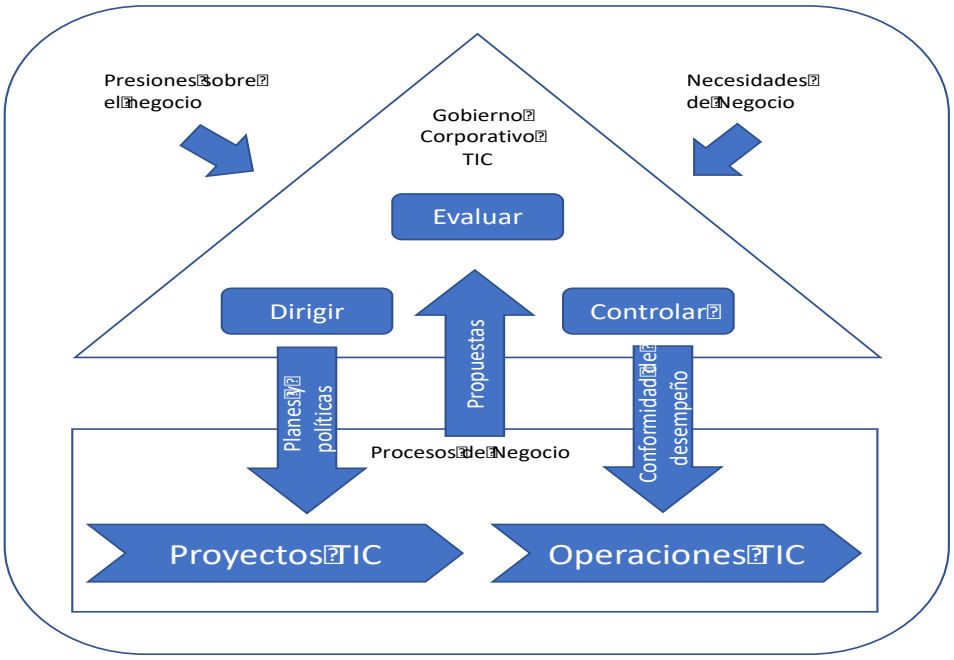
6.3.5. ISO/IEC 38500:2008

Finalmente, en el proceso de investigación, se identificó un estándar de gobierno de TI que se enfoca en proporcionar un marco de principios para que los directores los utilicen al evaluar, dirigir y monitorear el uso de la tecnología de la información en sus organizaciones, como se ilustra en el gráfico 3, como lo es la ISO/IEC 38500, la cual toma los servicios de información y comunicaciones como eje para la generación de directrices básicas de orientación a la alta dirección, en relación con un buen gobierno de TI que subsane la insuficiencia de los sistemas de tecnología de información en la definición de un alcance del sistema de gestión, el cual puede obstaculizar el desempeño y la competitividad de las organizaciones al exponerlas en el cumplimiento de la legislación, entre otros muchos riesgos, en relación con el gobierno corporativo de TI (ICONTEC, 2009).

De acuerdo con el marco para el buen gobierno corporativo de la tecnología de la información, el estándar ISO/IEC 38500 incorpora seis principios, los cuales expresan el comportamiento de preferencia para guiar la toma de decisiones en una organización, siendo estos: responsabilidad, estrategia, adquisición, desempeño, conformidad, y comportamiento humano. Este modelo define que los directores deberían controlar la Tecnología de la

Información a través de tres tareas principales, tales como evaluar el uso actual y futuro de la Tecnología de la Información, dirigir la preparación e implementación de los planes y las políticas para garantizar que el uso de las TI satisface los objetivos del negocio y monitorear la conformidad con las políticas y el desempeño frente a los planes (ICONTEC, 2009).

Gráfico 3: Modelo para el Gobierno Corporativo de las TI.



Fuente: Elaboración propia a partir de ICONTEC, 2009.

6.4. Diagnóstico empresarial

Por otro lado, partiendo del hecho de que la intervención en todas las organizaciones debe partir del resultado de una valoración inicial, la cual permita identificar la situación actual o grado de madurez, tanto de la cadena de valor como de los aspectos que, de alguna manera, afectan el cumplimento de los objetivos de la organización, se definirán algunos términos relacionados con el diagnóstico empresarial.

El diagnóstico empresarial es “un proceso que permite establecer los puntos fuertes y débiles, las fuerzas restrictivas, la dinámica del cambio, el sistema operacional y la salud de una organización” (Prieto, 2012, p. 24). Así mismo, se puede definir como un proceso de

comparación entre dos situaciones: la actual, que se puede determinar mediante un proceso de revisión detallada y documentación de los hallazgos, y el estado deseado, que está definido por lo que se quiere llegar a ser. La brecha entre estas dos situaciones, se puede llamar diagnóstico.(Vidal, 2004). De igual forma, Valdés Rivera (1998), citado en Braidot, Formento, & Nicolini, (2003), señala que realizar el diagnóstico empresarial permite a la organización pasar de un estado de incertidumbre a otro de conocimiento, además de medir los signos vitales a través de indicadores previamente establecidos.

Usualmente, al realizar el diagnóstico empresarial, se identifican algunos problemas o puntos débiles en la organización, y con base a esos aspectos observados, se diseña un plan de acción, el cual estará orientado en dar solución a las situaciones deficientes identificadas o potencializar los recursos de la organización. En ese sentido, para desarrollar un diagnóstico empresarial, en primera instancia se debe realizar una revisión previa, la cual consiste en la preparación de la documentación necesaria para la elaboración del diagnóstico. Posteriormente, para identificar las fortalezas y debilidades, se debe realizar un análisis detallado de cada una de las dependencias de la organización, que permitirá definir la estrategia para gestionar el riesgo y potencializar las oportunidades (Prieto, 2012).

Una vez finalizado el análisis, se podrán identificar las necesidades existentes en la organización, al igual que las causas y las posibles consecuencias en el cumplimiento de los objetivos estratégicos de la organización. Con base en el análisis y una vez definidas y priorizadas las necesidades, se realiza el plan de acción, el cual debe tener el alcance claramente definido, considerando aspectos como los recursos necesarios para su implementación.

A diferencia de lo anterior, Vidal señala que el proceso diagnóstico empresarial consta de seis pasos: (a) identificación de la organización, (b) auditoría externa, (c) auditoría interna o análisis del direccionamiento estratégico, (d) auditoría interna análisis de factores internos por funciones cruzadas, e) selección, descripción y análisis del macro problema y (f) diseño de estrategias y nuevo plan estratégico (Vidal, 2004).

En este sentido, para obtener la información que se utilizará para realizar un diagnóstico empresarial, se puede recurrir a las siguientes fuentes: las teorías o modelos, el plan estratégico organizacional, los estudios de Benchmarking y los comportamientos históricos de la organización (Vidal, 2004). Las Teorías o modelos consisten en revisar detalladamente la documentación de los procesos y procedimientos que son desarrollados en la organización con la

finalidad de establecer que desviaciones existen entre lo que se está realizando y lo que se debería realizar. Los marcos y modelos establecen métodos, parámetros y pautas. El objetivo es verificar si la organización está cumpliendo con los modelos adoptados para el desarrollo de los procesos. Los planes estratégicos organizacionales definen todo aquello que la organización quiere lograr, además de la manera de lograrlo, motivo por el cual, en él se traza la hoja de ruta para alcanzar los objetivos de la organización. Al utilizar esta fuente para realizar el diagnóstico empresarial, se deberá comparar lo planeado contra lo ejecutado. Los Estudios de Benchmarking están enfocados en identificar las mejores prácticas adoptadas por organizaciones similares y realizar la comparación entre la tendencia del mercado y los estándares adoptados en la organización objeto del diagnóstico y los comportamientos históricos de la organización consistentes en identificar el comportamiento histórico de la organización en ciertos periodos de tiempo, los cuales proporcionan datos para realizar el diagnóstico (Vidal, 2004).

Para realizar el diagnóstico organizacional existe una gran variedad de modelos. En los siguientes párrafos se analizará brevemente las características más relevantes de algunos de ellos, lo cual es de gran utilidad al momento de realizar el diagnóstico organizacional, en razón a que explica coherente y sistemáticamente el funcionamiento de ellas. El Modelo para la Modernización de la Gestión de Organizaciones (MMGO), que es una metodología diseñada por la Universidad EAN y su objetivo fundamental es facilitar la modernización gerencial de las empresas hacia organizaciones modernas, competitivas, centradas en la innovación y capaces de competir en un mundo global.

Esta metodología, contempla dos factores fundamentales para la modernización de las organizaciones. El primero está enfocado en la gestión organizacional, que contempla aspectos como la carencia de un direccionamiento estratégico, la obsolescencia tecnológica de las plantas, la modalidad gerencial y la cultura empresarial, las deficiencias en comunicación, las deficiencias en la logística y las dificultades para financiar proyectos ambiciosos. El otro factor está relacionado con el entorno macroeconómico de las organizaciones, tales como la carencia de una agenda de desarrollo interno que promueva el aumento de la competitividad y la productividad, la inexistencia de programas y proyectos para la conformación de cadenas productivas y la disminución de la demanda interna por la pérdida de poder adquisitivo de la

población, la repentina apertura comercial con fuerte elevación de las importaciones competitivas de la producción nacional y el lento crecimiento de las exportaciones.

El modelo MMGO promueve el aumento de la competitividad y la productividad de las PYMES, actuando sobre los principales componentes organizacionales de la empresa, siendo su principal característica el nivel de detalle que maneja en el análisis situacional y en la identificación de las actividades que conformarán la ruta de cambio, mejoramiento y reconversión hacia las mejores prácticas en la organización.

Finalmente, el modelo MMGO describe 4 estadios de desarrollo, los cuales reflejan los distintos niveles de crecimiento en términos de su capacidad de gestión, gerencia y administración, disponibilidad de recursos y de infraestructura, que tienen las organizaciones. Cada uno de los estadios refleja el estado de madurez de la organización, lo que le permite identificar la brecha para alcanzar el estado deseado.

7. Diseño metodológico

7.1. Marco metodológico

Inicialmente, es importante subrayar que el objeto de estudio del proyecto de investigación es diagnosticar la gestión de los recursos de TI en la Jefatura de las Tecnologías de Información y Comunicaciones de la Fuerza Aérea Colombiana, y basado en los marcos de referencia, diseñar un modelo de gobierno de TI y su plan de implementación, motivo por el cual, para desarrollarlo se propone ejecutar las siguientes fases:

- **Estudio marcos de referencia:** Inicialmente se analizarán de manera detallada los marcos de referencia y buenas prácticas en relación con el gobierno corporativo de TI, tales como COBIT, ISO 27000, ITIL, PMBOK e ISO 38500. Una vez definidos los marcos que serán objeto de estudio, se efectuará una comparación entre ellos, de manera que se puedan identificar y seleccionar los componentes que sean aplicables para la definición del modelo a proponer.

- **Diagnóstico organizacional:** Con la finalidad de establecer la brecha entre el estado actual y el deseado, se realizará el diagnóstico de la situación presente en relación con el modelo de gobierno de TI. A pesar de que previamente se habían mencionado el modelo MMGO para realizar diagnóstico empresarial, por la especificidad del tema que se desea valorar, ninguno de los componentes del MMGO va a ser utilizado para la ejecución de esta actividad. En este sentido, considerando que la finalidad del diagnóstico en la organización es determinar el grado de madurez en el cual se encuentra la gestión de TI en Jefatura de las Tecnologías de Información y Comunicaciones de la Fuerza Aérea Colombiana, se utilizará como herramienta principal de comparación el Manual para la Implementación de la Política de Gobierno Digital suministrado por MINTIC y los niveles de capacidad definidos en COBIT 5, el cual permitirá establecer el nivel de madurez en cada uno de los dominios. De igual manera, se realizará el análisis estratégico de la Jefatura de las Tecnologías de la Información y las Comunicaciones de la Fuerza Aérea Colombiana, con el propósito de definir los lineamientos para alinear el Gobierno

de TI con la Estrategia.

Además, con la finalidad de identificar la situación actual de los procesos y la infraestructura que se tiene en el área TI y la arquitectura de sus sistemas de información, se realizará la revisión del entorno de la organización en la cual se desarrollará la propuesta. En consecuencia, para realizar el diagnóstico y determinar el grado de madurez o modelo de capacidad de los procesos del gobierno corporativo de las TIC en la organización, se analizará cada uno de los procesos definidos por COBIT. Por cada proceso, se definirá el nivel de capacidad, enmarcándolo en los niveles de madurez establecidos por el marco de referencia, es decir, incompleto, ejecutado, gestionado, establecido, predecible u optimizado. Las actividades anteriores permitirán determinar las necesidades y oportunidades existentes en la Jefatura de las Tecnologías de Información y Comunicaciones de la Fuerza Aérea en relación la gestión de TIC, es decir, identificar las brechas entre la situación actual y el estado deseado, y con base a ella, trazar la hoja ruta para alcanzarlo.

- **Diseño de modelo de gobierno de TI para la Jefatura de Tecnología de la Información y Comunicaciones:** Una vez terminado el diagnóstico y establecida la brecha que separa la JETIC del estado final deseado, se procederá a diseñar un modelo de gobierno de TI basado en el marco de referencia seleccionado, el cual estará alineado con la estrategia de la Jefatura de las tecnologías de la información y la comunicación e incluirá aspectos importantes para la organización, tales como personas, procesos, tecnología, datos y servicios.

- **Elaboración del plan de implementación:** Una vez finalizado el diseño de modelo de gobierno de TI apropiado para la Jefatura de las Tecnologías de Información y Comunicaciones, se elaborará su plan de implementación, considerando los pasos del modelo propuesto y los recursos disponibles para tal fin.

- **Validación del modelo**: Finalmente, se realizará la validación del modelo mediante juicio de expertos aplicado en la oficina de Gobierno Corporativo de TIC de la Jefatura de las Tecnologías de la Información y Comunicaciones.

7.2. Tipo de investigación

El proyecto propuesto es una investigación de campo a través del estudio descriptivo, realizando la recolección de información y análisis de diferentes modelos de gobierno de tecnologías de la información. En este sentido, el presente proyecto se puede considerar como una investigación no experimental, en razón a que se realiza sin la manipulación deliberada de variables y en que sólo se observan los fenómenos en su ambiente natural para analizarlos (Hernandez, 2014).

De igual manera, se utilizará una metodología de observación activa de orden cualitativo, llevando a cabo una revisión bibliográfica profunda y un análisis digital, haciendo uso de la revolución tecnológica, la cual permite profundizar sobre la situación actual de la organización objeto de estudio, y a través de la información recolectada poder diseñar y documentar un modelo de gobierno de TI que cumpla de forma integral los objetivos propuestos (Ruiz Olabuénaga, 2012).

En consecuencia, se debe explorar el contexto seleccionado para considerar la relación con el ambiente, teniendo en cuenta todas las posibles situaciones que pudieran entorpecer el estudio, así como las personas y permisos que se requiere para un análisis más detallado y fiel de la información. Lo anterior significa negociar con estas personas, explicando de forma clara y detallada el fin del estudio y por qué fueron elegidos, cuanto tiempo aproximadamente se requiere de ellos y que se va a realizar con los resultados obtenidos.

Para lograr que se cumpla a cabalidad esta metodología se deben contemplar importantes tareas en el trabajo de campo como los son: a) acceso al contexto, ambiente o sitio b) registrar observaciones de todas las iteraciones c) realizar entrevistas iniciales d) elaborar repositorios de documentos e) realizar bitácoras de las actividades a desarrollar y por último f) realizar una correcta elaboración y clasificación de materiales y medios utilizados (Hernandez, 2014).

7.3. Técnicas de recolección y análisis de información

Es importante hacer referencia a que existen diferentes técnicas de recolección de datos, las cuales permiten recopilar la información necesaria para llevar a cabo la investigación. Por lo anterior, la información será recopilada a partir de la revisión de la caracterización de los

procesos, entrevistas con los funcionarios de las áreas de interés y aplicación de cuestionarios de preguntas abiertas y cerradas, métodos de observación, escalamiento de Likert y visitas en campo.

A su vez, el análisis de la información recolectada se realizará mediante la tabulación y procesamiento de los datos, de manera que se pueda comparar las actividades que se realizan en la organización en relación con la gestión de los recursos de TI, con las definidas en cada uno de los niveles del modelo de madurez especificados por el marco de referencia.

En tal virtud, se diseñará un plan de recolección de información, analizando referencialmente las diferentes situaciones, ajustando el resultado del estudio para la construcción de un juicio de expertos aplicado en la oficina de Gobierno Corporativo de TIC de la Jefatura de las Tecnologías de la Información y Comunicaciones (Galeano M, 2003).

Así mismo, considerando que es importante conservar un orden al momento de recolectar la información, este proceso será realizado en diferentes etapas, que permitan una búsqueda eficaz de información. En este sentido, primero se identificará qué tipo de información es requerida, dónde se puede realizar la búsqueda, y como analizar y evaluar las fuentes, ya sean medios físicos o digitales. Finalmente, se utilizará de manera adecuada esta información para posterior realizar su integración de forma adecuada. Todo este proceso será apoyado en herramientas que permitan recopilar y citar los diferentes documentos que sean utilizados en el desarrollo de esta investigación (Argudo, 2013).

7.4. Población y Muestra

De acuerdo con Lepkowski (2008) citado por Hernández (2014), la población o universo es un conjunto de todos los casos que concuerdan con determinadas características definidas por el investigador. Con relación a lo anterior, la población de la investigación es el personal de la Fuerza Aérea Colombiana que pertenece a la Jefatura de las Tecnologías de la Información y Comunicaciones, quienes, desde su rol intervienen en los procesos estratégicos, operativos y tácticos de la Jefatura objeto de estudio. En síntesis, la población está compuesta 108 funcionarios que pertenecen a la JETIC.

Por otra parte, la muestra de una investigación es un subgrupo de la población o universo que se utiliza por economía de tiempo y recursos, que implica definir la unidad de muestreo y de

análisis y que requiere delimitar la población para generalizar resultados y establecer parámetros. Las clases de muestras pueden ser probabilística o no probabilística. En la probabilística todos los elementos de la población tienen la misma posibilidad de ser escogidos para la muestra y se obtienen definiendo las características de la población y el tamaño de la muestra, y por medio de una selección aleatoria o mecánica de las unidades de muestreo (Hernandez, 2014). Por otra parte, de acuerdo con Johnson, (2014), Hernández-Sampieri et al., (2013) y Battaglia, (2008) citados por Hernández (2014), en las muestras no probabilísticas, la elección de los elementos no depende de la probabilidad, sino de causas relacionadas con las características de la investigación o los propósitos del investigador. De acuerdo con lo anterior, la muestra del presente trabajo de investigación es de tipo no probabilística, toda vez que, de acuerdo con los objetivos de la investigación, la muestra será un subconjunto de la población que ocupa cargos de directores y subdirectores de cada una de las direcciones que hacen parte de JETIC, quienes interesan a los investigadores porque ofrecen una gran riqueza para la recolección y el análisis de los datos, siendo estos cargos ocupados por 14 oficiales, quienes serán la muestra de la investigación.

8. Marco normativo

En la tabla 1 se relacionan las principales normas a considerar para la elaboración de modelo de gobierno de TI para la Jefatura de Tecnología de Información y Comunicaciones de la Fuerza Aérea Colombiana y otras regulaciones relevantes para el sector Defensa en el tema tecnológico.

Tabla 1: Marco Normativo

NORMA	DESCRIPCIÓN
Art. 217 de la Constitución Política	Finalidad primordial de las Fuerzas Militares.
Ley 527 de 1999	Por medio de la cual se define y reglamenta el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales, y se establecen las entidades de certificación.
Decreto 1747 de 2000	Por el cual se reglamenta parcialmente la Ley 527 de 1999, en lo relacionado con: "Las entidades de certificación, los certificados y las firmas digitales".
Resolución 0891 del 16 de marzo de 2009	Por la cual se crea el Comité de Integración de Tecnologías de Información y Comunicaciones – CITI – del Sector Defensa, para fijar las políticas de estandarización en materia de tecnología, comunicaciones y servicios en el Ministerio de Defensa Nacional.
Ley 1273 de 2009	Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado – denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.
Ley 1341 de 2009	Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las tecnologías de la información y las comunicaciones.
Plan Estratégico Institucional 2011-2030	Mediante el cual se define la dirección estratégica de la Fuerza Aérea Colombiana que contribuye al diseño e implantación de planes para lograr los objetivos estratégicos en el 2030.
Circular 17 de 2011	Por la cual se reglamenta y ordena la verificación del uso legal de software en las entidades u organismos públicos de orden nacional y territorial.
Decreto 2693 de 2012	El cual define los elementos transversales a la Estrategia Gobierno en Línea, para fortalecer la identificación de usuarios, la caracterización de infraestructuras tecnológicas e incorporar la política de seguridad de la información.
Decreto 2609 de 2012 Nivel Nacional	Por el cual se reglamenta el Título V de la Ley 594 de 2000, parcialmente los artículos 58 y 59 de la Ley 1437 de 2011 y se dictan otras disposiciones en materia de Gestión Documental para todas las Entidades del Estado.

Fuente: Elaboración Propia

Tabla 1: Marco Normativo (Continuación).

NORMA	DESCRIPCIÓN
Ley 1672 de 2013	Por la cual se establecen los lineamientos para la adopción de una política pública de gestión integral de residuos de aparatos eléctricos y electrónicos (RAEE), y se dictan otras disposiciones.
Decreto 1377 de 2013	Reglamentar parcialmente la Ley, 1581 de 2012, por la cual se dictan disposiciones generales para la protección de datos personales.
Decreto 32 de 2013.	Creación de la comisión intersectorial que se denominará "Comisión Nacional Digital y de Información Estatal", cuyo objeto será la coordinación y orientación superior de la ejecución de funciones y servicios públicos relacionados con el manejo de la información pública, el uso de infraestructura tecnológica de la información para emitir los lineamientos rectores del Grupo de Respuesta a Emergencias Cibernéticas de Colombia del MDN.
Directiva Permanente 2014-18-MDN.	Implementación de un sistema de seguridad de la información y estandarización de las Políticas de Seguridad de la información para el sector Defensa.
Decreto 886 de 2014.	El presente decreto tiene como objeto reglamentar la información mínima que debe contener el Registro Nacional de Bases de Datos.
Decreto 2573 de 2014	Son los lineamientos, instrumentos y plazos de la estrategia de Gobierno en línea para garantizar el máximo aprovechamiento de las TIC, con el fin de contribuir con la participación de un Estado más eficiente y participativo.
Decreto 1078 de 2015	Por la cual se definen principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones -TIC- y se crea la Agencia Nacional de Espectro.
Decreto 415 del 2016	El cual tiene por objeto señalar los lineamientos para el fortalecimiento institucional y ejecución de los planes, programas y proyectos de tecnologías y sistemas de información en la respectiva entidad.
Documento del modelo de gestión IT4+	Modelo integral de gestión estratégica con tecnología cuya base fundamental es la alineación entre la gestión de tecnología y la estrategia sectorial o institucional.
Disposición 061 del 22 de diciembre de 2017	Por la cual se reestructura la organización de las dependencias de la Fuerza Aérea Colombiana.
Decreto 2194 2017	Decreto Único Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, Decreto número 1078 de 2015.
Resolución No. 0000548 del 2017	Código de buen Gobierno del Ministerio, Fondo de tecnología de la información y Comunicaciones.
Plan Nacional de Tecnologías de la Información	Plan de implementación de TI en Colombia
Modelo de Gestión de la Fuerza Aérea Colombiana	Por medio de la cual se “busca liderar la organización desde un enfoque holístico y sistémico, basado en el rediseño de procesos; parte del estudio pormenorizado de las actividades y tareas que se desarrollan en cada una de las Áreas Funcionales y Departamentos del Nivel Central, con el propósito de conformar los Procesos Gerenciales, Misionales y de Apoyo”.

Fuente: Elaboración Propia

Tabla 1: Marco Normativo (Continuación).

NORMA	DESCRIPCIÓN
Decreto 090 de 2018	Serán objeto de inscripción en el Registro Nacional de Bases de Datos, las bases de datos que contengan datos personales cuyo Tratamiento automatizado o manual sea de sociedades y/o entidades sin ánimo de lucro y personas jurídicas de naturaleza pública.
Manual para la Implementación de la Política de Gobierno Digital V5 del 2018.	En el cual se emiten los lineamientos para la implementación de la Política de Gobierno Digital de acuerdo con el Decreto 1078 de 2015.
Decreto N° 1008 de 2018	Por el cual se establecen los lineamientos generales de la política de Gobierno Digital y se subroga el capítulo 1 del título 9 de la parte 2 del libro 2 del Decreto 1078 de 2015, Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones"
Resolución MDN-5563 2018.	Por la cual se formula el PETI del Sector Defensa y Seguridad 2018-2022' y se emiten otros lineamientos relacionados con las TICs y las Comunicaciones en el Sector Defensa.
Circular 2018-272- MDN	La utilización de servicios en la nube se debe realizar bajo los siguientes parámetros: servicios de CLOUD debe ser clara las obligaciones del contratista en cuanto a la responsabilidad respecto a la conservación de los contenidos (información), borrado de datos, propiedad intelectual y niveles de servicio (ANS).
Política Sectorial de Tecnologías en la NUBE - Circular MINDEFENSA.	Uso de soluciones en la NUBE a nivel Institucional; para permitir que los sistemas de TI sean escalables y elásticos bajo demanda.
Directiva Permanente No. 03 de 2019 - MDN.	Política de privacidad y protección de datos; define los lineamientos la política de tratamiento de datos personales en el Ministerio de Defensa.
Plan Estratégico Tecnologías de Información y Comunicaciones 2019- 2022 FAC	Mediante el cual se alinea los sistemas de información con las políticas del sector a nivel nacional, permitiendo articular las herramientas que se utilizan en las dependencias de la Fuerza Aérea Colombiana para el período 2019-2022.

Fuente: Elaboración Propia

9. Diagnóstico organizacional

Actualmente, los sistemas de información de la Jefatura de las Tecnologías de la Información y Comunicaciones de la Fuerza Aérea Colombiana, se rigen por los lineamientos del Plan Estratégico de Tecnologías de la Información – PETI, por ello, para el diagnóstico se utilizará como herramienta principal de comparación los procesos definidos por COBIT, en relación a los lineamientos estipulados en el manual para la implementación de la Política de Gobierno Digital suministrado por MINTIC, el cual, está basado en el decreto 1078 de 2015, que a su vez, está fundamentado en el decreto 1151 de 2008. Este último estableció como objetivo de la estrategia Gobierno en línea "Contribuir con la construcción de un Estado más eficiente, más transparente y participativo, y que preste mejores servicios a los ciudadanos y a las empresas, a través del aprovechamiento de las Tecnologías de la Información y la Comunicación" (Decreto 1151, 2008).

En consecuencia, los requerimientos emanados del manual para la implementación de la Política de Gobierno Digital, el Plan Estratégico de Tecnologías de la Información y demás decretos y documentos relacionados en el marco normativo, ver tabla 1, se homologaron a los procesos definidos por COBIT, como se describe en la tabla 2, con la finalidad de determinar el estado actual, identificar el nivel de capacidad deseado, y de esta manera, establecer la brecha.

Una vez homologados los procesos a COBIT, la técnica utilizada para recopilar la información para identificar el nivel de capacidad del Gobierno de TI en la Jefatura de las Tecnologías de la Información y Comunicaciones de la Fuerza Aérea Colombiana, fue aplicar una encuesta al personal directivo de la Jefatura, en la cual cada encuestado, basado con su experiencia y conocimiento de la organización, valoró en una escala de 1 a 5, el nivel de cumplimiento de las actividades de las prácticas claves de gobierno de acuerdo con el marco utilizado, para posteriormente ser tabulada y ponderada para definir el nivel de capacidad actual. En consecuencia, los resultados obtenidos se describen en los numerales 9.1 y 9.2.

Tabla 2: Homologación a procesos COBIT

Manual de implementación de Gobierno Digital	Proceso COBIT 5.0	Práctica Clave de Gobierno
Proceso de Gestión de TI	APO01 Gestionar el Marco de Gestión de TI	APO01.01: Definir la estructura organizativa.
		APO01.02: Establecer roles y responsabilidades.
		APO01.03: Mantener los elementos catalizadores del sistema de gestión.
		APO01.04 Comunicar los objetivos y la dirección de gestión.
Definición de una política de TI alineada con la misión		APO01.05: Optimizar la ubicación de la función de TI.
		APO01.06: Definir la propiedad de la información (datos) y del sistema.
Estructura organizacional del área de TI		AP001.07: Gestionar la mejora continua de los procesos
		APO01.08: Mantener el cumplimiento con las políticas y procedimientos.
Gestión del Portafolio	APO05 Gestionar el Portafolio	APO05.01: Establecer la mezcla del objetivo de inversión.
		APO05.02: Determinar la disponibilidad y las fuentes de fondos.
		APO05.03: Evaluar y seleccionar los programas a financiar.
		APO05.04: Supervisar, optimizar e informar sobre el rendimiento del portafolio de inversiones.
		APO05.05: Mantener los portafolios.
		APO05.06: Gestionar la consecución de beneficios.
Instancias de decisión de TI	APO06 Gestionar el Presupuesto y los Costes	APO06.01: Gestionar las finanzas y la contabilidad.
		APO06.02: Priorizar la asignación de recursos.
		APO06.03: Crear y mantener presupuestos.
		APO06.04: Modelar y asignar costes.
		APO06.05: Gestionar Costes
Cumplimiento con los requerimientos de usuario	APO09 Gestionar los Acuerdos de Servicio	APO09.01: Identificar servicios TI
		APO09.02: Catalogar servicios basados en TI
		APO09.03: Definir y preparar acuerdos de servicio.
		APO09.04: Supervisar e informar de los niveles de servicio.
		APO09.05: Revisar acuerdos de servicio y contratos.
Relaciones con proveedores.	APO10 Gestionar los Proveedores	APO10.01: Identificar y evaluar las relaciones y contratos con proveedores.
		APO10.02: Seleccionar proveedores.
		APO10.03: Gestionar contratos y relaciones con proveedores.
		APO10.04: Gestionar el riesgo en el suministro.
		APO10.05: Supervisar el cumplimiento y el rendimiento del proveedor.
Administración de la calidad.	APO11 Gestionar la Calidad	APO011.01: Establecer un sistema de gestión de la calidad.
		APO11.02: Definir y gestionar los estándares, procesos y prácticas de calidad.
		APO11.03: Enfocar la gestión de la calidad en los clientes.
		APO11.04 Supervisar y hacer controles y revisiones de calidad.
		APO11.05: Integrar la gestión de la calidad en la implementación de soluciones y la entrega de servicios.
		APO11.06: Mantener una mejora continua.

Fuente: Elaboración Propia

Tabla 2: Homologación a procesos COBIT (Continuación).

Manual de implementación de Gobierno Digital	Proceso COBIT 5.0	Práctica Clave de Gobierno
Gestión de Riesgos	APO12 Gestionar el Riesgo	APO12.01: Recopilar datos.
		APO12.02: Analizar el riesgo.
		APO12.03: Mantener un perfil del riesgo.
		APO12.04: Expresar el riesgo.
		APO12.05: Definir un portafolio de acciones para la gestión de riesgos.
		APO12.06: Responder al riesgo.
Seguridad de los sistemas	APO13 Gestionar la Seguridad	APO13.01: Establecer y mantener un SGSI.
		APO13.02: Definir y gestionar un plan de tratamiento del riesgo de la seguridad de la información.
		APO13.03: Supervisar y revisar el SGSI.
Gestionar los Programas y Proyectos	BAI01 Gestión de Programas y Proyectos	BAI01.01: Mantener un enfoque estándar para la gestión de programas y proyectos.
		BAI01.02: Iniciar un programa.
		BAI01.03: Gestionar el compromiso de las partes interesadas.
		BAI01.04: Desarrollar y mantener el plan de programa.
		BAI01.05: Lanzar y ejecutar el programa.
		BAI01.06: Supervisar, controlar e informar de los resultados del programa.
		BAI01.07: Lanzar e iniciar proyector dentro de un programa.
		BAI01.08: Planificar proyectos.
		BAI01.09: Gestionar la calidad de los programas y proyectos.
		BAI01.010: Gestionar el riesgo de los programas y proyectos.
		BAI01.011: Supervisar y controlar proyectos.
		BAI01.012: Gestionar los recursos y los paquetes de trabajo del proyecto.
		BAI01.013: Cerrar un proyecto o iteración.
		BAI01.014: Cerrar un programa.
Gestión de cambios	BAI06 Gestionar los Cambios	BAI06.01: Evaluar, priorizar y autorizar peticiones de cambio.
		BAI06.02: Gestionar cambios de emergencia.
		BAI06.03: Hacer seguimiento de cambios de estado.
		BAI06.04: Cerrar y documentar los cambios.
Gestionar el Conocimiento	BAI08 Gestionar el Conocimiento	BAI08.01: Cultivar y facilitar una cultura de intercambio de conocimientos.
		BAI08.02: Identificar y clasificar las fuentes de información.
		BAI08.03: Organizar y contextualizar la información, transformadora en conocimiento.
		BAI08.04: Utilizar y compartir el conocimiento.
		BAI08.05: Evaluar y retirar la información.
Gestionar los Activos	BAI09 Gestionar los Activos	BAI09.01: Identificar y registrar activos actuales.
		BAI09.02: Gestionar activos críticos
		BAI09.03: Gestionar el ciclo de vida de los activos
		BAI09.04: Optimizar el coste de los activos.
		BAI09.05: Administrar licencias.

Fuente: Elaboración Propia

Tabla 2: Homologación a procesos COBIT (Continuación).

Manual de implementación de Gobierno Digital	Proceso COBIT 5.0	Práctica Clave de Gobierno
Continuidad del negocio.	DSS04 Gestionar la Continuidad	DSS04.01: Definir la política de continuidad del negocio, objetivos y alcance.
		DSS04.02: Mantener una estrategia de continuidad.
		DSS04.03: Desarrollar e implementar una respuesta a la continuidad del negocio.
		DSS04.04: Ejercitar, probar y revisar el plan de continuidad.
		DSS04.05: Revisar, mantener y mejorar el plan de continuidad.
		DSS04.06: Proporcionar formación en el plan de continuidad.
		DSS04.07: Gestionar acuerdos de respaldo.
		DSS04.08: Ejecutar revisiones posteriores a la reanudación.

Fuente: Elaboración Propia

9.1. Procesamiento estadístico de datos

Tabla 3: Ficha técnica de la encuesta de diagnostico

FICHA TECNICA DE LA ENCUESTA	
Dirección	La encuesta de esta investigación fue realizada por Carlos Alberto Velásquez Pineda y Andrei Bahamon Páez, estudiantes de Maestría en Gerencia de Sistemas de Información y Proyectos Tecnológicos de la Universidad EAN.
Técnica	El tipo de encuesta utilizada fue de preguntas cerradas con una escala de medición con valoración de 1 a 5 (Escala de Likert), donde 1 es no se cumple y 5 se cumple totalmente.
Fecha de realización	La encuesta fue realizada el 15 de junio de 2020.
Cantidad de entrevistados	14 oficiales que ocupan cargo de directores o subdirectores de la Jefatura de las Tecnologías de la Información y Comunicaciones

Fuente: Elaboración Propia

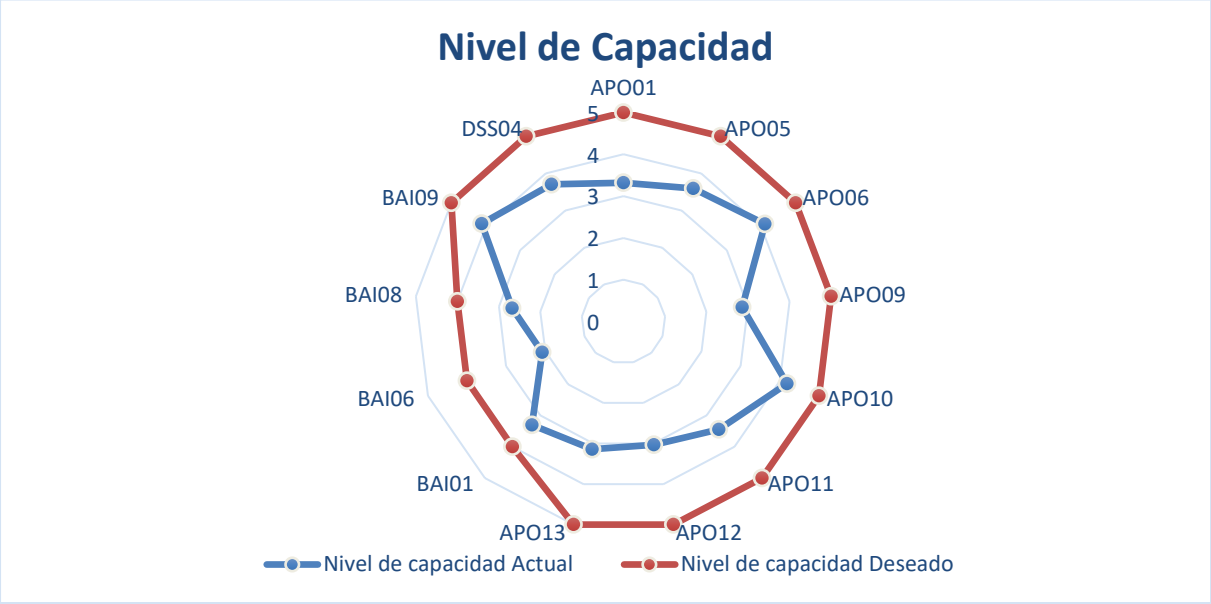
Una vez aplicada la encuesta al personal de directores y subdirectores de la Jefatura de las Tecnologías de la Información y Comunicaciones, se obtuvo el resultado ilustrado en el gráfico 4, el cual detalla el nivel de capacidad actual para los procesos de COBIT descritos en la tabla 2, los cuales debe cumplir el modelo de Gobierno de TI a proponer, de acuerdo con los lineamientos emanados en el manual de Gobierno Digital y demás documentos analizados.

Tabla 4: Procesos COBIT en JETIC

Ítem	Identificador	Proceso COBIT 5.0
1	APO01	Gestionar el Marco de Gestión de TI
2	APO05	Gestionar el Portafolio
3	APO06	Gestionar el Presupuesto y los Costes
4	APO09	Gestionar los Acuerdos de Servicio
5	APO10	Gestionar los Proveedores
6	APO11	Gestionar la Calidad
7	APO12	Gestionar el Riesgo
8	APO13	Gestionar la Seguridad
9	BAI01	Gestión de Programas y Proyectos
10	BAI06	Gestionar los Cambios
11	BAI08	Gestionar el Conocimiento
12	BAI09	Gestionar los Activos
13	DSS04	Gestionar la Continuidad

Fuente: Elaboración Propia

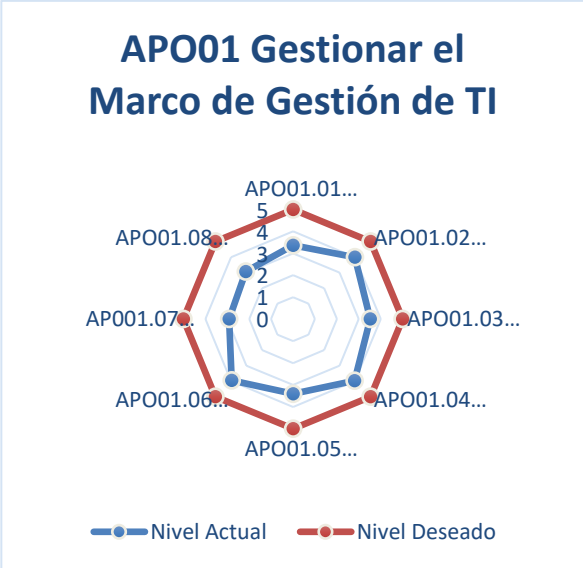
Gráfico 4: Nivel de Capacidad en JETIC



Fuente: Elaboración Propia

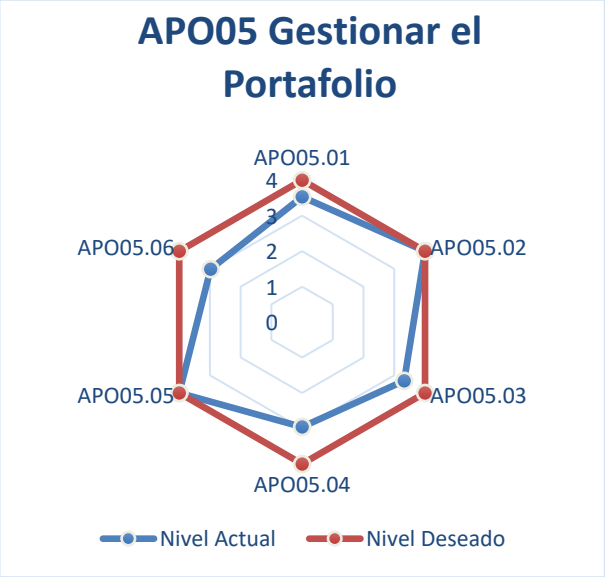
De igual manera, con la finalidad de profundizar en el análisis y obtener más elementos para la identificación de las brechas, se realizó la tabulación de los valores obtenidos de la encuesta, con relación a la valoración de las prácticas claves de gobierno definidas para cada uno de los procesos seleccionados de COBIT, las cuales fueron descritas en la tabla 2.

Gráfico 5: Brecha Gestionar el Marco de Gestión de TI



Fuente: Elaboración Propia

Gráfico 6: Brecha Gestionar el Portafolio



Fuente: Elaboración Propia

Gráfico 7: Brecha Gestionar el Presupuesto y los Costes

Fuente: Elaboración Propia

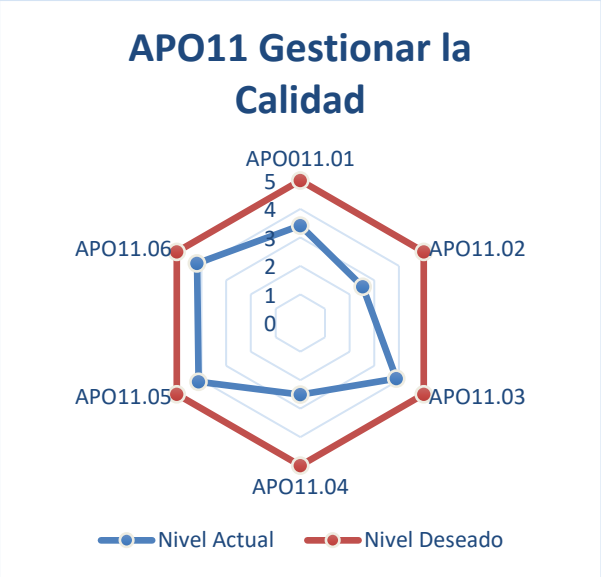
Gráfico 8: Brecha Gestionar los Acuerdos de Servicio

Fuente: Elaboración Propia

Gráfico 9: Brecha Gestionar los Proveedores

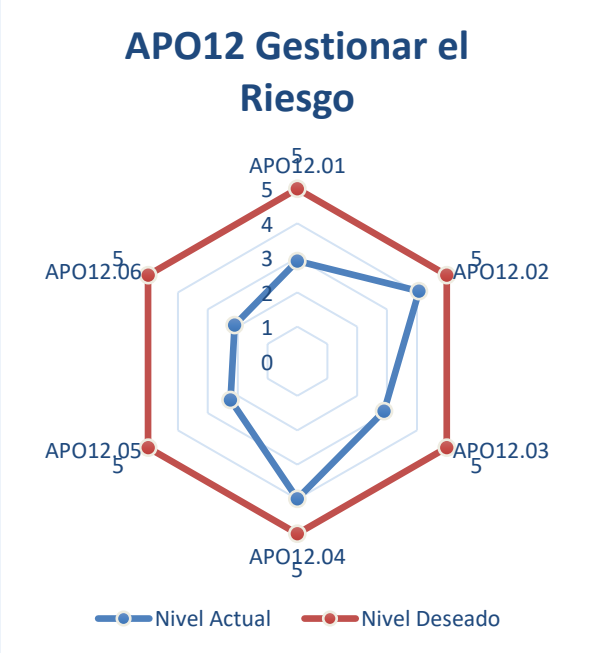
Fuente: Elaboración Propia

Gráfico 10: Brecha Gestionar la Calidad



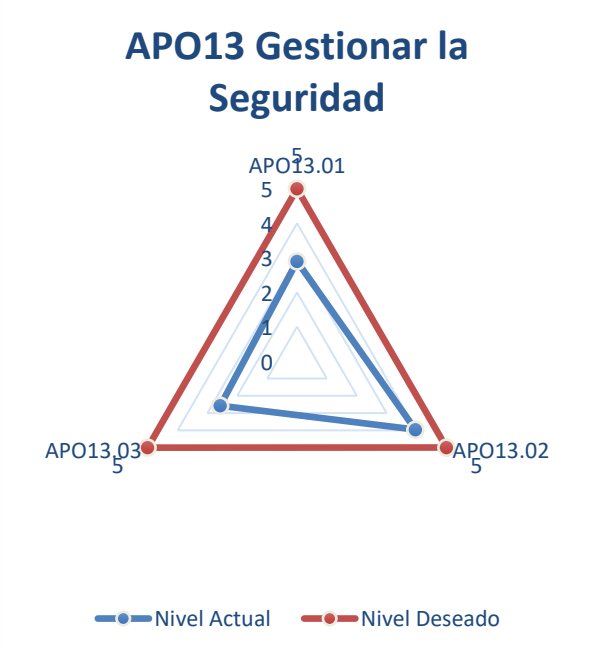
Fuente: Elaboración Propia

Gráfico 11: Brecha Gestionar el Riesgo



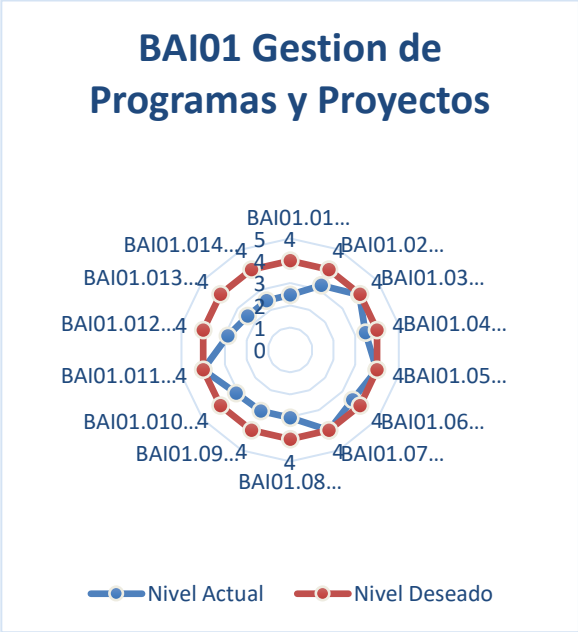
Fuente: Elaboración Propia

Gráfico 12: Brecha Gestionar la Seguridad



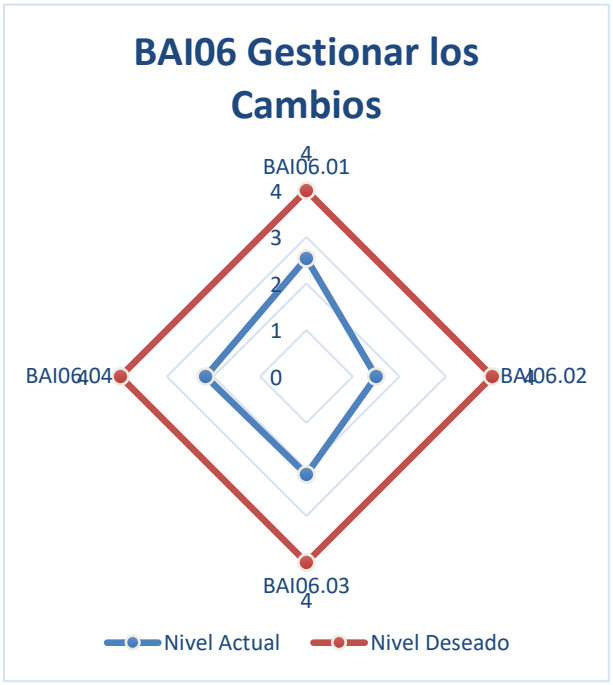
Fuente: Elaboración Propia

Gráfico 13: Brecha Gestión de Programas y Proyectos



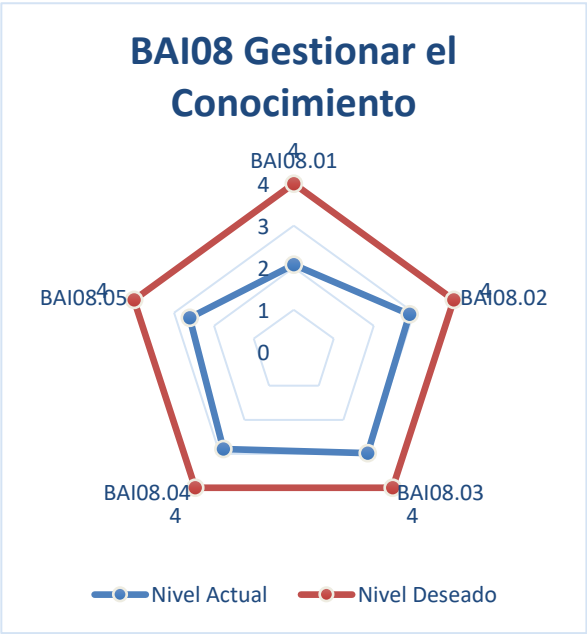
Fuente: Elaboración Propia

Gráfico 14: Brecha Gestionar los Cambios



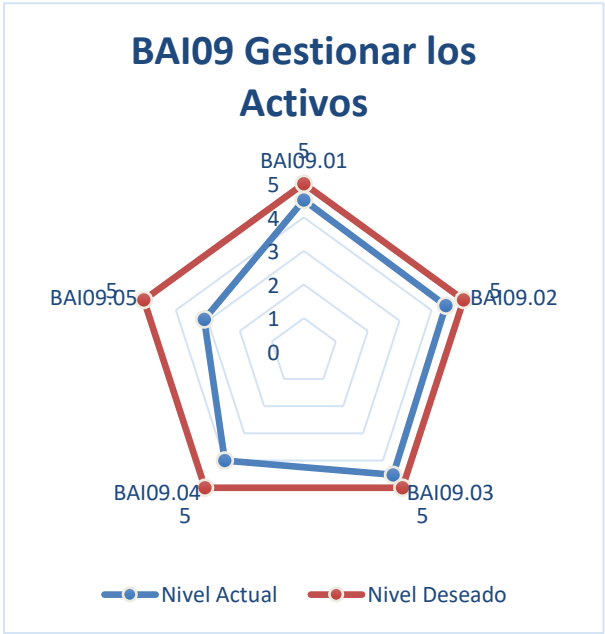
Fuente: Elaboración Propia

Gráfico 15: Brecha Gestionar el Conocimiento



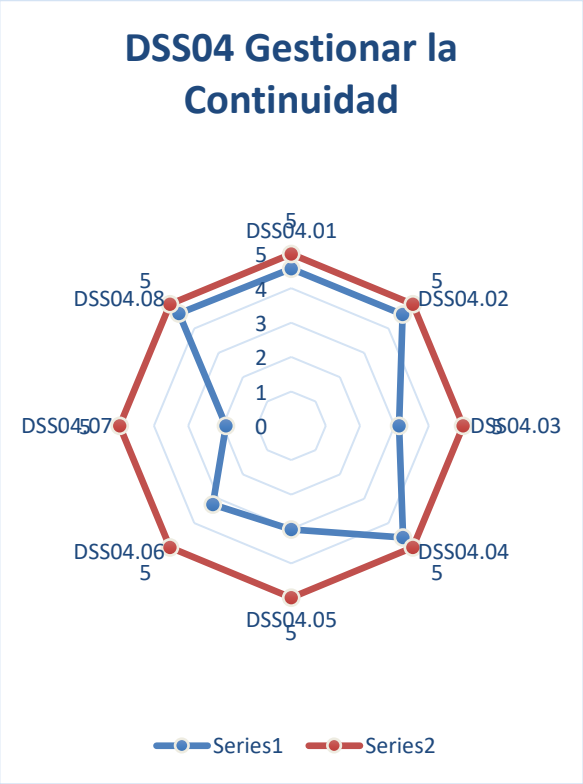
Fuente: Elaboración Propia

Gráfico 16: Brecha Gestionar los Activos



Fuente: Elaboración Propia

Gráfico 17: Brecha Gestionar la Continuidad



Fuente: Elaboración Propia

9.2. Análisis de datos

9.2.1. Situación actual

En la tabla 5 se detalla el nivel de capacidad actual y el nivel deseado, de acuerdo con COBIT y al manual de Gobierno Digital y en los párrafos siguientes, se describirá la situación actual de cada uno de los procesos:

Tabla 5: Nivel de Capacidad

Proceso COBIT	ID	Nivel de capacidad Actual					
		COBIT	Manual de Gobierno Digital	COBIT		Manual de Gobierno Digital	
				Corto	Mediano	Corto	Mediano
Gestionar el Marco de Gestión de TI	APO01	Definido	Desarrollo Intermedio	Medible	Optimizado	Desarrollo Robusto	Desarrollo Robusto
Gestionar el Portafolio	APO05	Definido	Desarrollo Intermedio	Medible	Optimizado	Desarrollo Robusto	Desarrollo Robusto
Gestionar el Presupuesto y los Costes	APO06	Administrado	Desarrollo Robusto	Optimizado	Optimizado	Desarrollo Robusto	Desarrollo Robusto
Gestionar los Acuerdos de Servicio	APO09	Repetible	Desarrollo Intermedio	Administrado	Optimizado	Desarrollo Robusto	Desarrollo Robusto
Gestionar los Proveedores	APO10	Administrad	Desarrollo Intermedio	Medible	Optimizado	Desarrollo Robusto	Desarrollo Robusto
Gestionar la Calidad	APO11	Definido	Desarrollo Intermedio	Medible	Optimizado	Desarrollo Robusto	Desarrollo Robusto
Gestionar el Riesgo	APO12	Definido	Desarrollo Intermedio	Medible	Optimizado	Desarrollo Robusto	Desarrollo Robusto
Gestionar la Seguridad	APO13	Definido	Desarrollo Intermedio	Medible	Optimizado	Desarrollo Robusto	Desarrollo Robusto
Gestión de Programas y Proyectos	BAI01	Definido	Desarrollo Intermedio	Medible	Optimizado	Desarrollo Robusto	Desarrollo Robusto
Gestionar los Cambios	BAI06	Repetible	Desarrollo Intermedio	Definido	Medible	Desarrollo Robusto	Desarrollo Robusto
Gestionar el Conocimiento	BAI08	Repetible	Desarrollo Intermedio	Definido	Medible	Desarrollo Robusto	Desarrollo Robusto
Gestionar los Activos	BAI09	Administrado	Desarrollo Robusto	Optimizado	Optimizado	Desarrollo Robusto	Desarrollo Robusto
Gestionar la Continuidad	DSS04	Definido	Desarrollo Intermedio	Medible	Optimizado	Desarrollo Robusto	Desarrollo Robusto

Fuente: Elaboración Propia

- **Gestionar el marco de gestión de TI:** Actualmente el proceso se encuentra definido, dado que, aunque están bien estructuradas algunas prácticas clave de gobierno, como la definición de roles y responsabilidades, los elementos catalizadores del sistema de gestión y la propiedad de la información y del sistema; otras no están bien definidas, siendo los más relevantes la mejora continua de los procesos y la conservación y el cumplimiento con las políticas y procedimientos.

  En este sentido, se observa que en el manual de funciones están documentados y comunicados los roles y responsabilidades relativos a TI para todo el personal, así como los procedimientos de gestión, el código ético y las prácticas profesionales de acuerdo con las necesidades y los objetivos de la institución. Así mismo, se observó que se implementan prácticas de socialización para que toda la organización comprenda e interiorice la visión, la cultura, la filosofía de gestión, la tolerancia al riesgo, la seguridad, los valores éticos, el código de conducta, la rendición de cuentas y los requisitos de integridad en la gestión. Finalmente, se identifica que la Jefatura de las Tecnologías de la Información y Comunicaciones, cuenta con un área de TI definida que incluye indicadores de desempeño de TI, instancias de decisión de TI definidas, roles y responsabilidades de TI y la estructura organizacional del área de TI.

- **Gestionar el portafolio:** Actualmente el proceso se encuentra definido. Al analizar este proceso, se identificó que están definidas de manera explícita la disponibilidad y las fuentes de fondos, toda vez que se tiene un control adecuado que permite al ordenador del gasto establecer la disponibilidad y el compromiso de los recursos actuales, el gasto actual aprobado y la cantidad real comprometida. Lo anterior, permite crear y mantener portafolios de programas de inversiones TI, servicios TI y activos TI, que constituyan la base del presupuesto actual de TI y soporten los planes estratégicos y tácticos de TI.

- **Gestionar el presupuesto y los costes:** El estado presente de este proceso es administrado, toda vez que actualmente están definidos los procesos, entradas, salidas y responsabilidades de manera alineada con las políticas y enfoques empresariales de presupuesto y contabilización de costes para administrar sistemáticamente el presupuesto

y asignación de costes de TI. Además, la asignación del presupuesto de TI obedece a la estructuración de los planes de compras, los cuales son elaborados para satisfacer las necesidades de TI de la organización. De igual manera, mediante el catálogo de rubros, se clasifican todos los costes de TI adecuadamente, incluidos los relativos a los proveedores de servicio, de acuerdo con el marco de contabilidad de la gestión de la Fuerza Aérea Colombiana.

- **Gestionar los acuerdos de servicio:** El estado actual de este proceso es repetible, considerando que en los resultados de la encuesta aplicada al personal de directores y subdirectores, se pudo observar que la Jefatura de las Tecnologías de la Información y Comunicaciones de la Fuerza Aérea Colombiana mantiene un catálogo de servicios de TI actualizado con información adecuada sobre su gestión, responsabilidad de la dirección de tecnología, estrategia para la prestación de los servicios y estrategia para tercerización de los servicios.

- **Gestionar los proveedores:** De acuerdo con la encuesta, actualmente el proceso se encuentra en estado administrado, toda vez que en JETIC se establecen y mantienen criterios relativos al tipo, relevancia y criticidad de los contratos y proveedores, focalizándose en aquellos de mayor importancia. De igual manera, se establecen criterios de evaluación de contratos y proveedores que permita una revisión general del rendimiento de los proveedores de manera consistente. Finalmente, se identifican, registran y categorizan los proveedores y contratos existentes de acuerdo con el criterio definido para mantener un registro detallado de los proveedores que deben ser gestionados cuidadosamente.

- **Gestionar la calidad:** El proceso actualmente se encuentra en estado definido. Se pudo identificar que en la Jefatura objeto de estudio, se están realizando algunas prácticas que permiten integrar la gestión de la calidad en los procesos y prácticas de desarrollo de soluciones, tales como la supervisión de manera continua de los niveles de servicio e incorporación de prácticas de gestión de la calidad en todos los procesos y prácticas de prestación de servicios. De igual meneara, se identifican y documentan las causas raíz de las no conformidades. Sin embargo, no se comunican los resultados a la dirección de TI y

otras partes interesadas de manera oportuna para permitir que se adopten las medidas correctivas oportunas.

- **Gestionar el riesgo de TI:** Actualmente el proceso se encuentra en un nivel de capacidad definido, debido a la falta de un gobierno de TI adecuado, para ello se realizó un diagnostico utilizando el marco de riesgos de TI y los procesos de COBIT 5 que cubren las actividades de gestión de riegos, esto con el fin de identificar las brechas a tratar y que sean la base para la definición de los principios y directrices para la gestión de riesgos a nivel estratégico y operativo, en el modelo de gobierno que se va a construir.

  De igual forma, dentro del análisis de la encuesta se identificaron actividades que cumplen un rol importante para la gestión de riesgos, tales como la definición del alcance de los esfuerzos y la asignación de recursos para la identificación y gestión de riesgos, construir y actualizar regularmente el mapa de riesgo de TI, comparar el riesgo residual con la tolerancia al riesgo e identificar exposiciones que puedan requerir una respuesta al riesgo, el analizar el coste-beneficio de las opciones de respuesta al riesgo potencial al especificar requerimientos de alto nivel para los proyectos o programas que implementarán las respuestas de riesgo seleccionadas, validar los resultados de análisis de riesgos antes de usarlos para la toma de decisiones, revisar los resultados de evaluaciones objetivas de terceras partes, auditorías internas y revisiones del aseguramiento de la calidad y mapearlos con el perfil de riesgo, revisar las diferencias y exposiciones identificadas para determinar la necesidad de análisis de riesgos adicionales, e identificar oportunidades relacionadas con TI que podrían permitir la aceptación de un mayor riesgo y un crecimiento y retorno mayores.

- **Gestionar la seguridad de TI:** La encuesta realizada al equipo de directores ayudó a identificar, no solo las falencias para la creación de oportunidades de mejora, sino también actividades que se realizan de forma adecuada y que ayudan a fortalecer el diseño del plan de gobierno de TI. Por estas razones, se clasifica en un nivel de capacidad definido con miras a un desarrollo robusto.

  En este sentido, se identificaron actividades que se están desarrollando en la Jefatura, tales como formular y mantener un plan de tratamiento de riesgos de seguridad de la

información, el cual está alineado con los objetivos estratégicos y la arquitectura de la empresa. Lo anterior, permite asegurar que el plan identifica las prácticas de gestión y las soluciones de seguridad apropiadas y óptimas, con la finalidad de mantener un inventario de componentes de la solución implementados para gestionar los riesgos relacionados con la seguridad como parte de la arquitectura de la empresa, desarrollar propuestas para implementar el plan de tratamiento de riesgos de seguridad de la información, sustentados en casos de negocio adecuados, integrar la planificación, el diseño, la implementación y la supervisión de los procedimientos de seguridad de información y otros controles que permitan la prevención y detección temprana de eventos de seguridad, así como la respuesta a incidentes de seguridad.

- **Gestionar los programas y proyectos de TI:** Actualmente el proceso se encuentra en un nivel de capacidad definido, con buenos lineamientos documentados al interior de la Jefatura. La encuesta realizada al equipo de directores ayudó a clarificar las actividades que cumplen su funcionalidad según los lineamientos de COBIT y que pueden ser reutilizados dentro de la definición del proyecto.

  Dentro de las actividades que se cumplen y cuentan con un buen desempeño, se pueden resaltar que se designa un gerente dedicado a cada proyecto con las competencias y habilidades adecuadas. De igual manera, los procedimientos establecidos permiten identificar, comprometer y gestionar a las partes interesadas, analizar los intereses y los requisitos de las mismas, planificar, dar recursos y asignar las responsabilidades requeridas, administrar cada programa o proyecto para asegurar que la toma de decisiones y las actividades de entrega están enfocadas en el valor mediante la consecución de los beneficios y las metas del negocio, así como crear un entendimiento común del alcance del proyecto entre las partes interesadas y asegurar que cada proyecto tenga uno o más patrocinadores con suficiente autoridad.

- **Gestionar los cambios de TI:** El proceso se encuentra en un nivel de capacidad repetible, dado que en la encuesta se evidencian grandes falencias en la ejecución de este proceso al interior de la Jefatura de las Tecnologías de la Información y Comunicaciones, por lo que dentro del proyecto se crearán lineamientos para que el gestionar los cambios

llegue a un nivel de desarrollo robusto donde se cumplan con estándares y actividades acordes a criterios de aceptación que serán definidos para la creación del modelo de gobierno de TI.

- **Gestionar el conocimiento de TI:** El proceso se encuentra en un nivel de capacidad repetible, donde la gestión del conocimiento ha sido relegada a un segundo plano. En la encuesta se evidencia la necesidad de definir un modelo de gestión del conocimiento que no solo sea diseñado sino comunicado al interior de la Jefatura de las Tecnologías de la Información y Comunicaciones, por lo que dentro del proyecto se dará una especial atención para que este proceso llegue a un nivel de desarrollo robusto.

- **Gestionar los activos de TI:** La gestión de activos es un proceso que es altamente controlado y que tiene gran importancia para la Jefatura de las Tecnologías de la Información y Comunicaciones, y, en consecuencia, a través de la encuesta se identificaron muchas actividades con un gran grado de desarrollo y aceptación en el área de TI.

  Las actividades que más impacto generan están enmarcadas en la identificación de todos los activos en propiedad en un registro que indique el estado actual, así como identificar los requisitos legales, reglamentarios o contractuales que deben ser abordados en la gestión de los activos, verificar la existencia de todos los activos en propiedad mediante la realización periódica de controles de inventario físicos y lógicos y su conciliación, comprobar que los activos se adecuan a sus objetivos, asegurar la contabilización de todos los activos, identificar los activos que son críticos, supervisar el rendimiento de los activos críticos examinando las tendencias de incidentes, considerar el riesgo de fallo o necesidad del reemplazo de cada activo crítico, mantener la resiliencia de los activos críticos, establecer un plan de mantenimiento preventivo para todo el hardware, establecer contratos de mantenimiento que impliquen el acceso de terceros a las instalaciones de TI, comunicar a los clientes y los usuarios afectados el impacto esperado, asegurar que los servicios de acceso remoto y perfiles de usuario están activos sólo cuando sea necesario, incorporar el tiempo de inactividad previsto en general en el calendario de producción, adquirir todos los activos basándose en solicitudes aprobadas y

de acuerdo con las políticas y las prácticas de adquisición de la empresa, identificar el origen, recibir, verificar, probar y registrar todos los activos de una manera controlada, incluyendo el etiquetado físico, aprobar los pagos y completar el proceso con proveedores según las condiciones acordadas por contrato, desplegar los activos siguiendo el ciclo de vida de implementación estándar, incluyendo la gestión de cambios y pruebas de aceptación, asignar activos a los usuarios, con aceptación y firma de responsabilidades, reasignar los activos siempre que sea posible cuando ya no sean necesarios debido a un cambio de función de rol del usuario, redundancia dentro de un servicio o finalización de un servicio, eliminar los activos cuando no sirvan a ningún propósito útil debido a la finalización de todos los servicios relacionados, tecnología obsoleta o falta de usuarios, revisar la base general de activos de forma regular, evaluar los costes de mantenimiento, revisar la base general para identificar oportunidades de normalización, abastecimiento único y otras estrategias que pueden disminuir los costes de adquisición, soporte y mantenimiento.

- **Gestionar la continuidad de TI:** Al igual que la gestión de activos, la gestión de la continuidad es un proceso crítico para el área de TI y el cual es propiamente controlado, debido a su importancia para la Jefatura de las Tecnologías de la Información y Comunicaciones, y del cual por medio de la encuesta se identificaron muchas actividades con un alto grado de desarrollo y aceptación en el área de TI, siendo las más relevantes la identificación de procesos de negocio internos y subcontratados y actividades de servicio que son críticas, así como la identificación de las partes interesadas clave y los roles y responsabilidades para definir y acordar la política de continuidad y su alcance, definir y documentar los objetivos y el alcance mínimos acordados de la política de continuidad del negocio, identificar procesos de soporte al negocio esenciales y servicios TI relacionados, identificar escenarios potenciales probables que puedan dar pie a eventos que puedan causar incidentes disruptivos importantes, realizar un análisis de impacto en el negocio en funciones críticas del negocio, establecer el tiempo mínimo necesario para recuperar un proceso de negocio y su soporte de TI, analizar la probabilidad de amenazas que puedan causar pérdidas de continuidad de negocio, analizar los requerimientos de continuidad para identificar las posibles estrategias de negocio y opciones técnicas,

determinar las condiciones y los responsables de decisiones clave que puedan causar la invocación de los planes de continuidad, identificar los requerimientos de recursos y costes para cada opción técnica estratégica y realizar recomendaciones estratégicas, obtener la aprobación de los ejecutivos de negocio para las opciones estratégicas seleccionadas, definir los objetivos para ejercitar y probar los sistemas, definir y acordar ejercicios que sean razonables con las partes interesadas, validar los procedimientos de continuidad, e incluir roles y responsabilidades y acuerdos de retención de datos que ocasionen la mínima disrupción en los procesos de negocio, asignar roles y responsabilidades para realizar ejercicios y pruebas del plan de continuidad, realizar un análisis y revisión posterior para considerar el logro, desarrollar recomendaciones para mejorar el plan de continuidad actual en base a los resultados de la revisión, evaluar la observancia del Plan de Continuidad de Negocio documentado, determinar la efectividad del plan capacidad de continuidad roles y responsabilidades, identificar debilidades u omisiones en el plan y las capacidades y hacer recomendaciones para la mejora y obtener la aprobación de la dirección para los cambios en el plan y aplicarlos mediante el proceso de control de cambios de la empresa.

9.2.2. Oportunidades de mejora

Las oportunidades de mejora identificadas a partir del diagnóstico realizado se describen con relación a las prácticas claves de gobierno asociadas a los procesos definidos en la tabla 3, mientras que las actividades específicas que deberían ser desarrolladas para reducir la brecha se relacionan en el anexo A.

- **Gestionar el marco de gestión de TI:** En este proceso, se evidenció la falta de un esquema de gobierno de TI alineado con un modelo integrado de planeación y gestión. De igual manera, se identificaron que algunas prácticas claves de Gobierno de TI no están implementadas o se están realizando de una manera superficial, siendo las más relevantes la gestión de la mejora continua de los procesos y mantener el cumplimiento con las políticas y procedimientos.

- **Gestionar el portafolio:** En el análisis de este proceso, se observó que las principales brechas son generadas porque no se revisa regularmente el portafolio para identificar y explotar sinergias, eliminar programas duplicados e identificar y mitigar el riesgo, y además, no se utilizan las métricas acordadas y no se realiza seguimiento sobre cómo los beneficios son obtenidos, cómo evolucionan a lo largo del ciclo de vida de programas y proyectos y cómo son entregados desde los servicios TI. En consecuencia, se identificaron que supervisar, optimizar e informar sobre el rendimiento del portafolio de inversiones y gestionar la consecución de los beneficios, son prácticas claves de gobierno que constituyen una oportunidad de mejora para el proceso.

- **Gestionar el presupuesto y los costes:** En este proceso se identificaron pocas brechas, sin embargo, las principales falencias están asociadas a la práctica clave de gobierno de priorizar la asignación de recursos, dado que no se tiene establecido el procedimiento para prevalecer las asignaciones presupuestarias de alto nivel para programas habilitados por TI y activos de TI conforme a lo establecido por los planes estratégicos y tácticos.

- **Gestionar los acuerdos de servicio:** Se pudo identificar que la principal brecha está definida porque no se realiza la práctica clave de gobierno de catalogar los servicios basados en TI, toda vez que el catálogo no mantiene una alineación con los acuerdos de nivel de servicio, que permitan asegurar a los servicios de tecnología una disponibilidad constante, métricas claras, rendimiento acorde con las necesidades de la institución, informes claros de su uso y disponibilidad, seguridad en todos sus niveles y servicios de soporte adecuados y oportunos.

- **Gestionar los proveedores:** Las oportunidades de mejora más relevantes en este proceso están orientadas a la práctica clave de gobierno de identificar y evaluar las relaciones y contratos con proveedores, toda vez que no se evidencia un procedimiento para establecer y mantener criterios relativos al tipo, relevancia y criticidad de los contratos y proveedores. De igual manera, no está documentado un procedimiento para realizar la evaluación de contratos y proveedores que permita una revisión general del rendimiento de los proveedores de manera consistente, además de evaluar y comparar periódicamente

el rendimiento de los proveedores actuales y alternativos para identificar oportunidades de mejora.

- **Gestionar la calidad:** La principal oportunidad de mejora identificada en este proceso radica en que, a pesar de que se identifican y documentan las causas raíz de las no conformidades, no existe un plan para comunicar los resultados a la dirección de TI y en especial, a las otras partes interesadas. De igual manera, se identificó que tampoco están definidas las normas, procedimientos y prácticas de gestión de la calidad en consonancia con los requisitos del marco de control TI. Finalmente, se observó que no se ejecutan prácticas que permitan supervisar la calidad de los procesos y servicios de forma permanente y sistemática mediante la descripción, las métricas, y los análisis.

- **Gestionar el riesgo de TI:** En este proceso se identificaron brechas significativas, dado que, aunque se elabora un plan de tratamiento de riesgos, se evidenció que no se comunica a todas las partes interesadas, no se actualiza de manera frecuente y tampoco se realiza un perfil de riesgo para diferentes escenarios, lo cual podría afectar la continuidad del negocio. Tampoco se realiza un registro de datos sobre eventos de riesgo que han causado impactos en la continuidad de los servicios de TI. Por otro lado, aunque en la práctica se realiza, no están documentados qué servicios de TI y recursos de infraestructuras de TI son esenciales para sostener la operación de procesos de negocio, lo cual impide analizar dependencias e identificar eslabones débiles.

- **Gestionar la seguridad de TI:** En las oportunidades de mejora de este proceso, se identificó que, aunque está definida y documentada la política de seguridad de la información, no se comunica a todas las partes interesadas. Por otro lado, no están definidos los indicadores que permitan realizar la medición de la efectividad de las prácticas de gestión seleccionadas y especificar la forma de utilizar estas mediciones para evaluar la efectividad y producir resultados reproducibles y comparables. De igual manera, aunque se realizan auditorias y revisiones periódicas, los resultados tampoco se comunican a las partes interesadas.

- **Gestionar los programas y proyectos de TI:** Las oportunidades de mejora identificadas en este proceso están relacionadas con las prácticas claves de gobierno de mantener un enfoque estándar para la gestión de programas y proyectos, gestionar los recursos y los paquetes de trabajo del proyecto, cerrar un proyecto o iteración y cerrar un programa, dado que, desde el inicio del proyecto no se comunican a todas las partes interesadas, aspectos relevantes durante el proyecto, tales como el alcance y las necesidades de recursos durante el ciclo de vida de estos, no se tiene un enfoque estándar para la gestión de programas y proyectos durante todo el ciclo de vida de estos, no se asignan responsabilidades de acuerdo a una matriz de habilidades, no se documentan las lecciones aprendidas y no se tiene definido un procedimiento para hacer revisiones posteriores a la implementación.

- **Gestionar los cambios de TI:** Las oportunidades de mejora del proceso están enmarcadas en las prácticas claves de gestión de evaluar, priorizar y autorizar peticiones de cambio, gestionar cambios de emergencia, hacer seguimiento a los cambios de estado y cerrar y documentar los cambios, toda vez que no está caracterizado el proceso de gestión de cambios, y en consecuencia tampoco los procedimientos para realizar peticiones de cambio formales en relación a la infraestructura, sistemas o aplicaciones, cambios de emergencia y seguimiento a los cambios realizados.

- **Gestionar el conocimiento de TI:** Durante el proceso de diagnóstico se observó que, aunque en la organización existe el conocimiento tácito para desarrollar los procesos, éste no es gestionado para evitar la pérdida y traducir el conocimiento tácito en explicito. En consecuencia, este proceso no se encuentra caracterizado, motivo por el cual, las oportunidades de mejora están definidas principalmente por prácticas claves de gestión como cultivar y facilitar una cultura de intercambio de conocimientos, identificar y clasificar las fuentes de información, organizar y contextualizar la información, transformarla en conocimiento, utilizar y compartir el conocimiento y evaluar y retirar la información.

- **Gestionar los activos de TI:** Aunque este proceso se encuentra bien caracterizado, se observó que la principal oportunidad de mejora está asociada a la práctica clave de

gobierno de administrar licencias, toda vez que, aunque está documentado el proceso, no se tienen centralizadas ni inventariadas todas las licencias del software adquirido y no se realiza una auditoria de forma regular del software instalado con licencia.

- **Gestionar la continuidad de TI:** Las oportunidades de mejora del proceso están enmarcadas en las prácticas claves de gestión de desarrollar e implementar una respuesta a la continuidad del negocio, revisar, mantener y mejorar el plan de continuidad, proporcionar formación en el plan de continuidad y gestionar acuerdos de respaldo, dado que, aunque se realiza en la práctica, no están documentados los planes de continuidad de negocio operativos que contengan los procedimientos que deben ser seguidos para permitir continuar operando los procesos críticos de negocio y planes temporales de proceso.

En síntesis, después de haber analizado los documentos rectores para la definición de un Gobierno de TI en las instituciones públicas en Colombia, identificar los requerimientos y homologarlos a los procesos definidos en COBIT, basados en la encuesta aplicada al personal directivo de JETIC, se identificó que en la institución objeto de estudio se ha definido una política de TI acorde con su contexto y misión, la cual ha sido aprobada por la alta dirección, la cual tiene implementada y la mantiene actualizada y su objetivo es orientar a la dirección de tecnologías y sistemas de la información, durante la elaboración de su plan estratégico de tecnologías de la información (PETI).

De manera similar, se utilizan metodologías y criterios de evaluación para la selección de alternativas de solución tecnológicas, a través del modelo de planeación, de los proyectos de evaluación y adopción de tecnología antes de realizar inversiones en TI, pero no utiliza los acuerdos marco de precios y contratos de agregación de demanda para bienes y servicios de TI.

Así mismo, se observó que la Jefatura tiene definidos indicadores de logro y resultados, en el que incluye el tipo de indicador, nombre, descripción, metas y valor esperado, con los cuales mide el desempeño de la gestión de TI a través de tableros de control, publicación de estadísticas de la institución pública, sector y territorio, los cuales son base para la formulación de acciones de mejora.

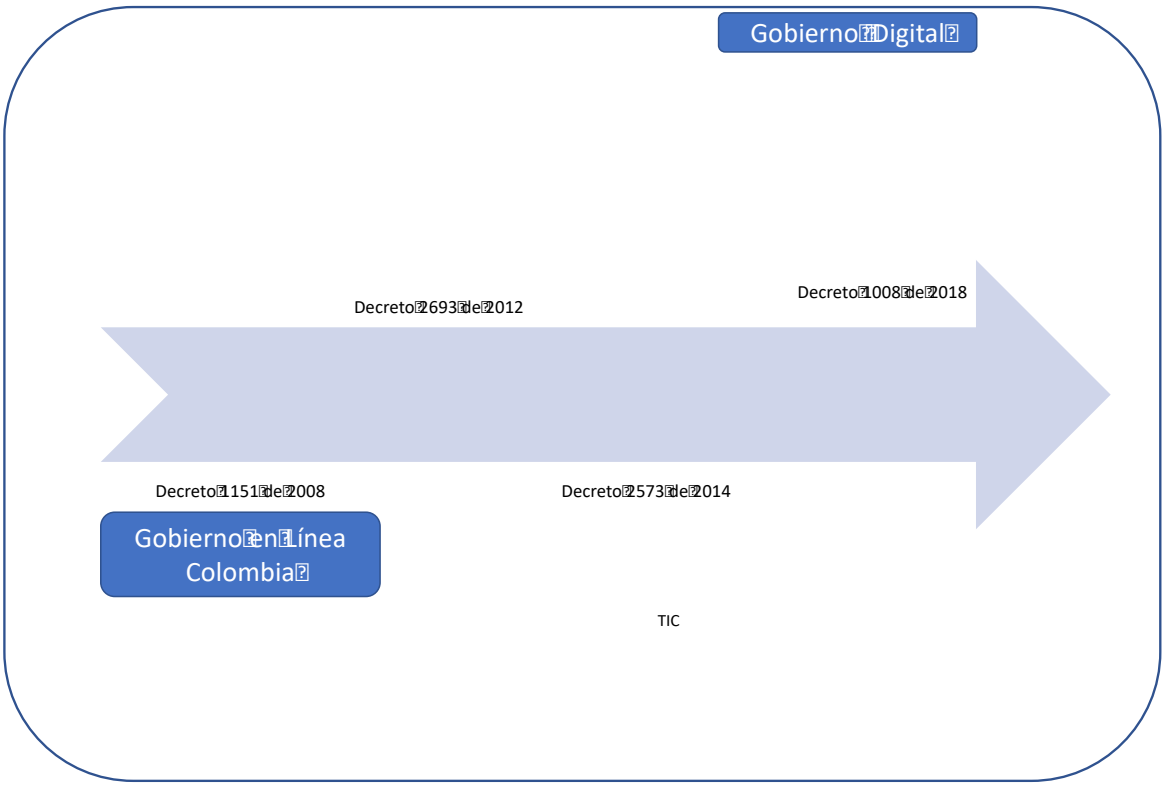
Finalmente, en relación con la ejecución de proyectos, se concluyó que los lineamentos establecidos permiten garantizar que cualquier iniciativa, proyecto o plan de la entidad que incorpora TI, es liderado en conjunto entre las áreas misionales y el área de TI de la entidad e incorpora desde el inicio la visión del usuario.

10. Análisis estratégico

10.1. Contexto del modelo

El Gobierno Nacional, en su intención de mejorar en materia de eficiencia administrativa, participación y servicios al ciudadano por medios electrónicos, en el 2008 inició con la implementación de la Estrategia de Gobierno en Línea en Colombia, no obstante, considerando la evolución constante de la sociedad y de la economía, en donde la tecnología juega un papel fundamental, ha evolucionado a la política de Gobierno Digital, como se describe en el gráfico 18, la cual fue establecida mediante el Decreto 1008 de 2018. Esta política está enfocada hacia la transformación digital del Estado, a fin de contar con entidades públicas orientadas a garantizar mejores condiciones de vida para los ciudadanos, así como satisfacer necesidades y problemáticas a través del aprovechamiento de la tecnología (Decreto 1008, 2018; Decreto 1078, 2015; Decreto 1151, 2008).

Gráfico 18: Evolución de la Política en Línea a Gobierno Digital



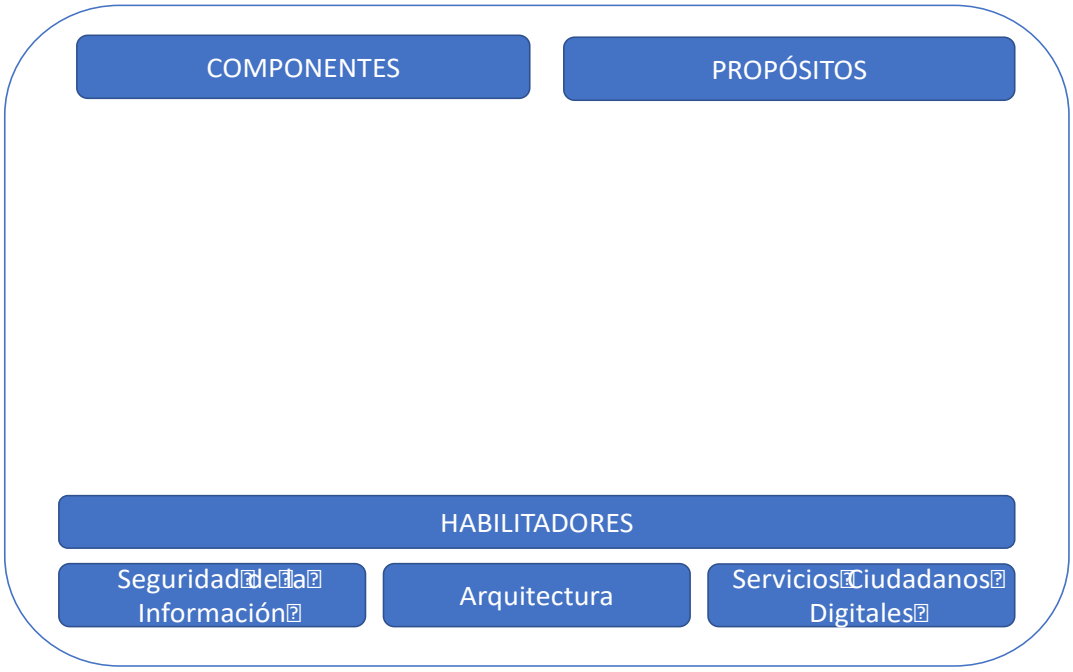
Fuente: Elaboración Propia a partir de MinTIC, 2018

Los aspectos claves de la estrategia de Gobierno en Línea, estaban orientadas principalmente en las acciones centradas en las entidades del Gobierno, la presencia en la web por parte de las entidades del Estado y en la priorización de la información en línea a través de sitios web para todas las entidades. Posteriormente, con la expedición del Decreto 2693 de 2012, se introdujeron elementos transversales a la estrategia, para fortalecer la identificación de usuarios, la caracterización de infraestructuras tecnológicas e incorporar la política de seguridad de la información (Decreto 2693, 2012). En consecuencia, en esta segunda versión de la estrategia se buscó construir una política que impulsara el uso estratégico de las TIC en la gestión de las entidades del Estado, así como desarrollar mejores servicios y espacios de interacción para ciudadanos y empresas.

Por su parte, considerando que en el escenario mundial de economía digital, factores como el conocimiento, la digitalización, la interconexión de redes de información y la innovación, juegan un papel transcendental en la transformación estructural de las sociedades, se hace la transición a Gobierno Digital, con el objetivo estratégico de transformar las entidades públicas y dotarlas de capacidades que les permitan responder a las necesidades que demanda un escenario de economía digital, así como al establecimiento y desarrollo de ciudades y territorios inteligentes que les ofrezcan mejores condiciones a los ciudadanos y un nivel superior de vida.

En este sentido, la política de Gobierno Digital plantea 5 grandes propósitos: (a) Habilitar y mejorar la provisión de servicios digitales de confianza y calidad, (b) Lograr procesos internos seguros y eficientes a través del fortalecimiento de las capacidades de gestión de tecnologías de información, (c) Tomar decisiones basadas en datos a partir del aumento en el uso y aprovechamiento de la información, (d) Empoderar a los ciudadanos a través de la consolidación de un Estado abierto y (e) Impulsar el desarrollo de territorios y ciudades inteligentes para la solución de retos y problemáticas sociales, a través del aprovechamiento de tecnologías de la información y las comunicaciones. Finalmente, para la implementación de la Política de Gobierno Digital, se han definido dos componentes: TIC para el Estado y TIC para la Sociedad, que son habilitados por tres elementos transversales: Seguridad de la Información, Arquitectura y Servicios Ciudadanos Digitales, como se ilustra en el gráfico 19 (MinTIC, 2018).

Gráfico 19: Modelo Gobierno Digital

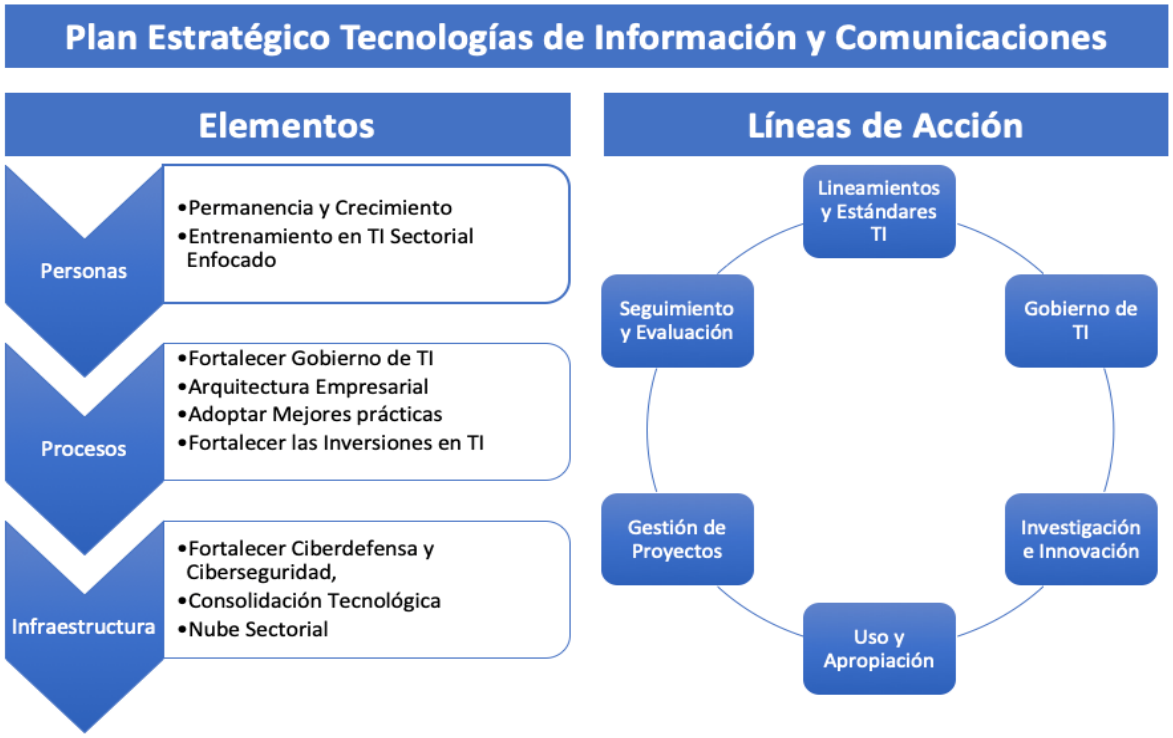


Fuente: Elaboración Propia a partir de MinTIC, 2018

Por otro lado, la Fuerza Aérea Colombiana en alineación con las políticas establecidas en el marco de Gobierno Digital, y considerando que mediante la disposición 061 del 22 de diciembre de 2017, se reestructura la Fuerza Aérea Colombiana, y crea la Jefatura de las Tecnologías de la Información y Comunicaciones, la cual recibe la misión de asegurar el desarrollo, sostenimiento y protección de la arquitectura de TIC para apoyar el logro de los objetivos estratégicos de la FAC, motivo por el cual, se crea el Plan Estratégico de Tecnologías de Información y Comunicaciones 2019- 2022.

En el marco de la transformación de la FAC, uno de los principales ejes fue el establecer criterios institucionales definidos para poder estandarizar todos los temas asociados a las tecnologías y las comunicaciones, y de esta manera, generar una mejor integración de los mismos, aumentar las capacidades y establecer mecanismos de uso y apropiación tendientes a optimizar los procesos de la institución y poder establecer mecanismos de control y tableros para toma de decisiones acertadas, informadas y en tiempo real (Fuerza Aérea Colombiana, 2019). En este sentido, la estrategia de la Jefatura de las Tecnologías de la Información y Comunicaciones se fundamenta en tres elementos y seis líneas de acción, como se describe en el gráfico 20.

Gráfico 20: Plan Estratégico Tecnologías de Información y Comunicaciones



Fuente: Elaboración Propia partir de PETI, 2019

10.2. Análisis estratégico de la Jefatura de las Tecnologías de la Información y Comunicaciones

De acuerdo a los términos estratégicos de la política de Gobierno Digital y el Plan Estratégico de información y comunicaciones, la estrategia de la Jefatura está orientada a la gestión de TI en las dependencias de la Fuerza Aérea Colombiana en concordancia con los lineamientos nacionales, a través de la definición de políticas, estrategias, modelo de gestión y planeación que permitan implementar las tecnologías de información como eje transversal a toda la institución, con el propósito de facilitar el uso de los sistemas de información para la solución de la gestión operacional y administrativa.

En este sentido, del análisis de la misión declarada por la Jefatura, se destaca que, para apoyar el logro de los objetivos de la FAC, se requiere direccionar estratégicamente la implementación y operación de tecnologías de información y comunicación que sean seguras, eficientes y oportunas, de manera que el área de TI suministre servicios de TI a toda la organización, con seguridad, efectividad y oportunidad para el desarrollo de las operaciones aéreas

multidimensionales que realice la Fuerza Aérea. Así mismo, de la visión se resalta que la gestión de los recursos de TI debe estar soportada en las buenas prácticas del sector y debe ser realizada por un talento humano cualificado, que permita potencializar la implementación, el uso y la apropiación de los recursos de TI para soportar los objetivos institucionales.

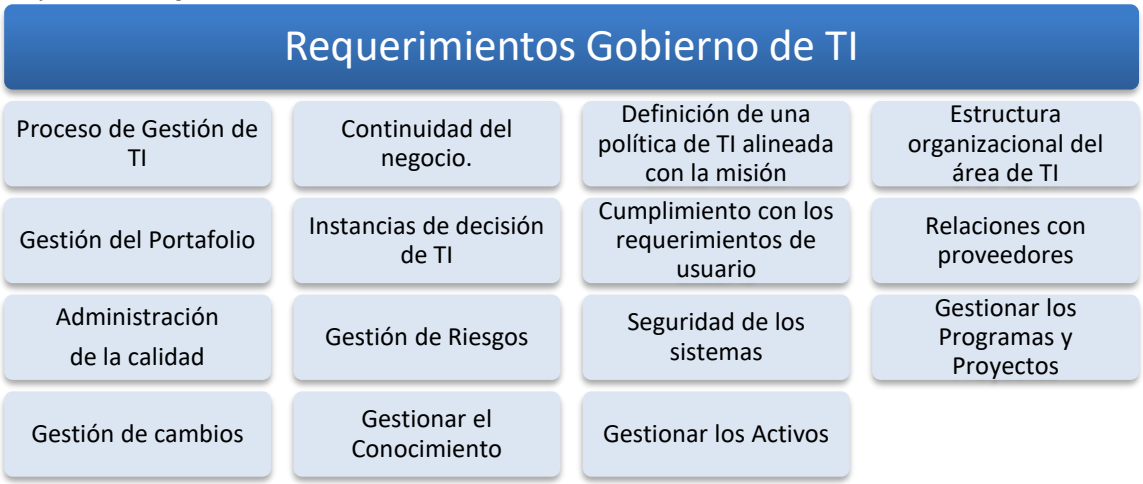
Continuando con el análisis de los objetivos estratégicos, se resalta que, para implementar las tecnologías de la información como eje transversal a toda la institución y soportar la estrategia de la organización, se deben identificar los requerimientos de TI de la organización y definir los acuerdos de servicio con relación a las capacidades actuales de TI y cumplir con los acuerdos pactados en la prestación de servicios de TI. En consecuencia, del análisis de la estrategia de la Jefatura de las Tecnologías de la información y Comunicaciones, se concluye que los lineamientos generales para la estructuración de un Gobierno de TI son:

- **Direccionamiento Estratégico de TI:** Direccionar la implementación y operación de tecnologías de información y comunicación que sean eficientes y oportunas para el cumplimiento de la misión institucional.
- **Calidad en los servicios de TI:** Suministrar servicios de TI en toda la organización, con efectividad y oportunidad para el desarrollo de las operaciones aéreas multidimensionales que realice la Fuerza Aérea.
- **Alineamiento Estratégico:** Prestación de servicios TI con oportunidad y efectividad partiendo de los lineamientos emanados por el Ministerio de las TIC y por el Ministerio de Defensa Nacional.
- **Gestión de TI soportada en buenas prácticas:** Promover el uso y apropiación de buenas prácticas que se estén desarrollando en el sector y que sean aplicables en la Fuerza Aérea Colombiana.
- **Cumplimiento de los acuerdos de servicio**: Definición con el usuario final de los acuerdos de nivel de servicio (ANS) para la prestación de los servicios de TI al interior de la FAC.
- **Gestión de los activos de TI:** Gestionar y realizar el soporte técnico en sus diferentes niveles para asegurar la disponibilidad y calidad de los servicios de TI.

- **Seguridad de los recursos de TI:** Administrar los recursos de TI de modo tal que se contrarreste toda amenaza e incidente de naturaleza cibernética que afecte los activos de información y la infraestructura crítica de la Fuerza Aérea Colombiana, además de conservar la integridad, disponibilidad y confiabilidad de la información.
- **Talento humano cualificado**: Desarrollar el potencial del talento humano, evaluar las competencias y habilidades requeridas para cada rol, retroalimentar al funcionario y gestionar el conocimiento para reducir la fuga de información, implementado prácticas para traducir el conocimiento tácito en conocimiento explicito, que garantice la continuidad del saber hacer al interior de la organización.
- **Catálogo de servicios de TI:** Diseñar y mantener actualizado el catálogo de servicios de TI con los Acuerdos de Nivel de Servicio (ANS) asociados.
- **Evaluación del desempeño de la gestión de TI**: Realizar el monitoreo y evaluación de desempeño de la gestión de TI a partir de las mediciones de los indicadores del proceso y demás que haya definido la Fuerza Aérea Colombiana.

Finalmente, de acuerdo con los lineamentos identificados en la estrategia de la Jefatura de las Tecnologías de la Información y las Comunicaciones y en la revisión del marco normativo, se definieron los requerimientos que deben ser considerados en el modelo de Gobierno de TI a proponer, de manera que exista una alineación entre Gobierno de TI y la Estrategia, los cuales se describen en el gráfico 21.

Gráfico 21: Requerimientos Gobierno de TI



Fuente: Elaboración Propia

11. Diseño de Modelo de Gobierno de TI

Por otro lado, una vez finalizada la identificación de los requerimientos, en adelante se realiza un análisis con la finalidad de identificar la manera en que los requerimientos definidos, están relacionados con los elementos que se deben considerar en el modelo de gobierno a proponer, tales como procesos, servicios, tecnología, datos y personas. En consecuencia, los resultados de la correlación realizada se ilustran en el gráfico 22, en el cual se observa que todos los requerimientos identificados previamente, están relacionados con al menos uno de los elementos definidos en los objetivos planteados al inicio de la investigación, como se describe a continuación:

Gráfico 22: Correlación de requerimientos

Fuente: Elaboración Propia

- **Procesos:** Este elemento será incluido a partir del desarrollo de los requerimientos de gestión de riesgos, gestión de cambios, administración de la calidad, definición de una política de TI alineada con la misión, gestión de los programas y proyectos, proceso de gestión de TI, instancias de decisión, gestión del portafolio y continuidad del negocio, toda vez que están orientados a mejorar los procesos en los cuales se basa la gestión de tecnología de la Jefatura.
- **Servicios:** A partir del desarrollo de los requerimientos de gestión de riesgos, gestión de cambios, administración de la calidad, definición de una política de TI alineada con la

misión, gestión de los programas y proyectos y cumplimiento de los requerimientos de usuario, se incluye este elemento, toda vez que proporcionan una adecuada gestión de la calidad, aumenta su eficiencia, los alinea con la infraestructura de TI y reduce los riesgos asociados de estos para cumplir con los alineamientos estratégicos y entrega de valor del área de TI.

- **Tecnología:** Este elemento será incluido a partir del desarrollo de los requerimientos de gestión de riesgos, gestión de cambios, administración de la calidad, definición de una política de TI alineada con la misión, gestión de los programas y proyectos, gestión del conocimiento y gestión de los activos, toda vez que están orientados a administrar su escalabilidad, conectividad, mantenibilidad, costos y calidad que estos prestan a la Jefatura.
- **Datos:** Este elemento será incluido a partir del desarrollo de los requerimientos de gestión de riesgos, gestión de cambios, administración de la calidad, seguridad de los sistemas, gestión del conocimiento y gestión de los activos, toda vez que estos requerimientos permiten administrar de manera eficaz la información estratégica y operativa de la Jefatura, garantizando su seguridad, optimizando su uso y dando a apoyo a la toma de decisiones, todo esto alineado a la misión, visión y objetivos estratégicos.
- **Personas:** Este elemento será incluido a partir del desarrollo de los requerimientos de estructura organizacional, relación con proveedores, gestión de riesgos, gestión de cambios y gestión de conocimiento, toda vez que son requerimientos que están relacionados con la administración del talento humano.

11.1. Propuesta de Modelo de Gobierno de TI

Continuando con el desarrollo del plan de intervención, para la creación del modelo de Gobierno de TI se seleccionó un marco de referencia, el cuál será la base del modelo a proponer, pero además se tomaron otros elementos de un marco diferente que apoya las estrategias de Gobierno de TI. En consecuencia, el marco de Gobierno de TI seleccionado fue el ISO 38500:2009, debido a que es una norma internacional que provee un estándar para que la dirección de las organizaciones evalúe, dirija y monitoree el uso de las tecnologías de la información, y el marco de apoyo que complementa el marco principal y apoya las estrategias de Gobierno de TI seleccionado fue COBIT 5.

De acuerdo con lo anteriormente expuesto, para determinar la relación entre los requerimientos identificados, el marco de referencia seleccionado y el marco de apoyo, se realizó una relación entre los requerimientos, los principios de ISO 38500:2009 y los procesos de COBIT, cómo se detalla en la tabla 6.

Tabla 6: Mapeo de requerimientos

ID	Requerimiento	ISO 38500	COBIT 5
01	Proceso de gestión de TI	Estrategia	APO01 Gestionar el Marco de Gestión de TI
02	Definición de una política de TI alineada con la misión	Estrategia	
03	Estructura organizacional del área de TI	Responsabilidad	
04	Gestión del Portafolio	Adquisición	APO05 Gestionar el Portafolio
05	Instancias de decisión de TI	Estrategia	APO06 Gestionar el Presupuesto y los Costes
06	Cumplimiento con los requerimientos de usuario	Cumplimiento	APO09 Gestionar los Acuerdos de Servicio
07	Relaciones con proveedores.	Adquisición	APO10 Gestionar los Proveedores
08	Administración de la calidad	Desempeño	APO11 Gestionar la Calidad
09	Gestión de Riesgos	Desempeño	APO12 Gestionar el Riesgo
10	Seguridad de los sistemas	Desempeño	APO13 Gestionar la Seguridad
11	Gestionar los Programas y Proyectos	Estrategia	BAI01 Gestión de Programas y Proyectos
12	Gestión de cambios	Desempeño	BAI06 Gestionar los Cambios
13	Gestionar el Conocimiento	Comportamiento Humano	BAI08 Gestionar el Conocimiento
14	Gestionar los Activos	Adquisición	BAI09 Gestionar los Activos
15	Continuidad del negocio	Desempeño	DSS04 Gestionar la Continuidad

Fuente: Elaboración Propia

Así mismo, en relación a lo documentado hasta este punto, en el gráfico 23 se ilustra el modelo de Gobierno de TI, el cual contempla los requerimientos previamente definidos como entrada, así como las tareas principales y los principios definidos en el modelo base adoptado, de modo tal que permita a los directivos de TI evaluar el uso actual y futuro de la Tecnología de la Información, incluyendo estrategias, propuestas y acuerdos de suministro, dirigir las inversiones en los proyectos y operaciones de Tecnología de la Información y monitorear a través de sistemas de medición, el desempeño de la Tecnología de la Información. Finalmente, se incluyen las practicas claves de gobierno y los indicadores de gestión que permitan valorar el cumplimento de los 6 principios de ISO 38500:2009 y cerrar las brechas identificadas en el diagnóstico.

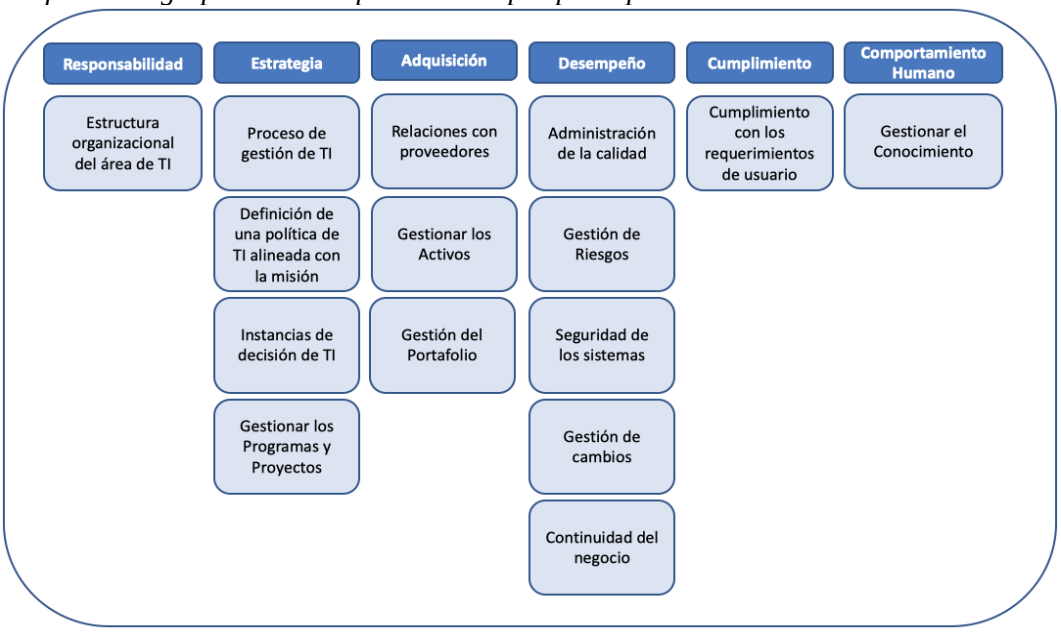
Gráfico 23: Modelo de Gobierno de TI

Fuente: Elaboración Propia

11.2. Descripción del Modelo

Una vez elaborado el modelo de Gobierno de TI, se realizará la segmentación de los requerimientos, de modo tal que se describa de manera detallada cada uno de ellos, con relación al principio de ISO 38500:2009 asociado, como se ilustra en el gráfico 24.

Gráfico 24: Agrupación de requerimientos por principios.



Fuente: Elaboración Propia

De este modo, cada requerimiento es analizado desde el punto de vista del principio de ISO 38500:2009 asociado, lo cual es la base para definir qué aspectos específicos deberían los directores de TI evaluar, dirigir y controlar, así como las prácticas clave de gobierno que se deberían desarrollar y los indicadores de gestión con los cuales se mediría el éxito de la gestión para cumplir el requerimiento identificado, como se describe a continuación.

11.2.1. Responsabilidad

Tabla 7: Descripción Estructura organizacional del área de TI

Estructura organizacional del área de TI			
		Responsable	**Tecnología**
Evaluar	Las necesidades de requerimientos de TI de la organización con la finalidad de establecer una estructura organizativa que refleje las necesidades del negocio, los roles, las responsabilidades y las prioridades de TI.	Jefe de Estado Mayor Fuerza Aérea. Comandante de Apoyo a la Fuerza. Jefe Tecnologías de la Información y Comunicaciones. Jefe Oficina de Gobierno Corporativo TIC.	Manual de Gobierno Digital. Plan Estratégico Institucional. Plan Estratégico Tecnologías de Información. Manual de Gobierno Digital.
Dirigir	Los planes para que la elaboración de la estructura organizativa se realice de acuerdo con las responsabilidades de tecnología de la información asignadas, estableciendo las estructuras de gestión requeridas para permitir que la toma de decisiones se lleve a cabo de la forma más eficaz y eficiente posible.		
Controlar	Que cada quién entienda su rol y tenga claras sus responsabilidades dentro de la organización.		
	El desempeño de aquellos a quienes se ha asignado responsabilidad en el gobierno de TI.		
	Que se comuniquen los roles y responsabilidades del personal de TI, así como de otras partes interesadas con responsabilidades en las TI corporativas.		
Prácticas Clave de Gobierno	Definir la estructura organizativa de TI.		
	Establecer roles y responsabilidades.		
Indicadores de Gestión	Porcentaje de cargos definidos en la estructura organizativa que están ocupados por profesionales competentes superior al 90%.		
	Porcentaje del personal satisfecho con su función de TI superior al 80%.		

Fuente: Elaboración Propia

11.2.2. Estrategia

Tabla 8: Descripción Proceso de Gestión de TI

Proceso de gestión de TI			
		Responsable	**Tecnología**
Evaluar	Que la caracterización del proceso de Gestión de TI cumpla con los requerimientos de la Jefatura de las Tecnologías de la información y Comunicaciones, considerando el objetivo, alcance, entradas, actividades, salidas y responsables. Además, que proporcione un enfoque de gestión consistente, que permita cumplir los requisitos de gobierno corporativo e incluya procesos de gestión y estructuras.	Jefe Tecnologías de la Información y Comunicaciones.	Plan Estratégico Tecnologías de Información. Manual de Gobierno Digital.
Dirigir	Los planes y proyectos para que la Jefatura de la Información y Comunicaciones elabore la caracterización del proceso de gestión de TI considerando objetivo, alcance, entradas, actividades, salidas y responsables.		
	La preparación y la utilización de los planes que aseguren que la organización se beneficie de los desarrollos de la tecnología de la información.		
Controlar	El cumplimiento de las actividades definidas en la caracterización del proceso de gestión de TI, con el fin de asegurar que la tecnología de la información brinde soporte a las necesidades actuales y futuras del negocio.		
	El uso de la tecnología de la información para asegurar que ésta obtiene los beneficios previstos.		
	El progreso de las propuestas de tecnología de la información aprobadas para asegurar que se están cumpliendo los objetivos en los marcos temporales exigidos, utilizando los recursos asignados.		
Prácticas Clave de Gobierno	Mantener los elementos catalizadores en la caracterización del proceso de gestión de TI, tales como personas, procesos, estructuras organizativas, cultura ética y comportamiento, información y servicios.		
	Comunicar los objetivos, el alcance, las actividades, los indicadores y las responsabilidades a todas las partes interesadas.		
	Gestionar la mejora continua del proceso de gestión de TI, mediante revisiones periódicas.		
Indicadores de Gestión	Cumplimiento de las revisiones periódicas al proceso de gestión de TI equivalente al 100%.		
	Tendencia de los resultados de las evaluaciones de las actividades definidas en el proceso de gestión de TI superior al 85%.		
	Número de incidentes relacionados con el incumplimiento de las actividades definidas en la caracterización del proceso inferior al 5%.		
	Porcentaje de las partes interesadas a los cuales se ha comunicado la caracterización del proceso, y reconocen los objetivos, el alcance, las actividades, los indicadores y las responsabilidades equivalente al 100%.		

Fuente: Elaboración Propia

Tabla 9: Definición de una política de TI alineada con la misión

Definición de una política de TI alineada con la misión			
		Responsable	**Tecnología**
Evaluar	El alineamiento de la política TI con la estrategia de la organización, de modo tal que las actividades desarrolladas por el área de TI soporten los procesos de la FAC para el cumplimento de la misión, visión y objetivos estratégicos de la organización.	Jefe Tecnologías de la Información y Comunicaciones. Jefe Oficina de Gobierno Corporativo TIC.	Plan Estratégico Institucional. Plan Estratégico Tecnologías de Información. Manual de Gobierno Digital.
Dirigir	El desarrollo de la política de TI para catalizar la ejecución de los procesos claves de la organización, de manera que se logre una gestión optima de los recursos de TI.		
Controlar	El progreso de las actividades de tecnología de la información para asegurar que se están cumpliendo los objetivos objetos de TI y se están potencializando el desarrollo de los procesos de la organización para cumplir con los objetivos organizacionales.		
Prácticas Clave de Gobierno	Definir una política de TI, la cual deberá estar alineada con la estrategia de la Jefatura de las Tecnologías de la información y Comunicaciones.		
	Mantener la alineación de la política de TI con la estrategia de negocio.		
Indicadores de Gestión	Porcentaje de las metas y requerimientos estratégicos de la empresa soportados por las metas estratégicas para TI equivalente al 100%.		
	Número de incidentes relacionados con el incumplimiento de la política de TI inferior al 5%.		
	Porcentaje de políticas soportadas por estándares y buenas prácticas de trabajo efectivas equivalente al 100%.		
	Cumplimiento de revisión y actualización de las políticas equivalente al 100%.		

Fuente: Elaboración Propia

Tabla 10: Definición Instancias de decisión de TI

Instancias de decisión de TI			
		Responsable	**Tecnología**
Evaluar	Los criterios y metodologías que direccionen la toma de decisiones de adopción y compra de Tecnologías de la Información, incluyendo personas, hardware, software y servicios, buscando el beneficio económico y de servicio de la institución.	Director de Apoyo al Comando y Control. Director de Tecnología. Director de Seguridad Informática. Director de Sistemas de Información.	Plan Estratégico Institucional. Plan Estratégico Tecnologías de Información.
Dirigir	Los planes y programas que le permitan a los directivos de TI la toma de decisiones de adopción y compra de Tecnologías de la Información.		
	Las actividades financieras relacionadas con las TI, abarcando presupuesto, coste y gestión del beneficio.		
	Los planes y programas que le permitan priorizar el gasto en adopción y compra de Tecnologías de la Información, mediante el uso de prácticas presupuestarias formales y un sistema justo y equitativo de reparto de costes a la empresa.		

Fuente: Elaboración Propia

Tabla 11: Definición Instancias de decisión de TI (Continuación)

Instancias de decisión de TI			
		Responsable	**Tecnología**
Controlar	Que la asignación de presupuesto para la adquisición de recursos de TI sea realizada con base en los planes de priorización.	Jefe Tecnologías de la Información y Comunicaciones. Jefe Oficina de Gobierno Corporativo TIC. Director de Apoyo al Comando y Control. Director de Tecnología. Director de Seguridad Informática. Director de Sistemas de Información.	Plan Estratégico Institucional. Plan Estratégico Tecnologías de Información.
	Que se realice de manera periódica el seguimiento y control de la ejecución del presupuesto de TI.		
	Los costes totales y los beneficios en el contexto de los planes estratégicos y tácticos de TI, e iniciar acciones correctivas cuando sea necesario.		
Prácticas Clave de Gobierno	Desarrollar el procedimiento general de adquisiciones de recursos de TI, que incluya instalaciones, hardware, software y servicios necesarios por la organización.		
	Gestionar las finanzas y la contabilidad.		
	Priorizar la asignación de recursos de acuerdo con las necesidades de la organización.		
Indicadores de Gestión	Porcentaje de inversiones de TI en los que el beneficio se monitoriza a través de la vida útil de los activos superior al 80%.		
	Porcentaje del cumplimento del plan de priorización de proyectos superior al 85%.		
	Porcentaje de servicios de TI en los que se obtienen los beneficios esperados superior al 95%.		
	Porcentaje de la alineación de los recursos de TI con iniciativas de alta prioridad superior al 90%.		

Fuente: Elaboración Propia

Tabla 12: Definición Gestionar los Programas y Proyectos

Gestionar los Programas y Proyectos			
		Responsable	**Tecnología**
Evaluar	Los planes y proyectos para alcanzar los beneficios de negocio y reducir el riesgo de retrasos y costes inesperados y el deterioro del valor, mediante la mejora de las comunicaciones y la involucración de usuarios finales y de negocio, asegurando el valor y la calidad de los entregables del proyecto y maximizando su contribución al portafolio de servicios e inversiones.	Director de Apoyo al Comando y Control. Director de Tecnología. Director de Seguridad Informática. Director de Sistemas de Información.	Plan Estratégico Institucional. Plan Estratégico Tecnologías de Información. Ley 80 de 1993.
Dirigir	Los programas y proyectos del portafolio de inversiones de forma coordinada y en línea con la estrategia corporativa.		
	La creación de un marco de trabajo de programas y proyectos para la administración de todos los proyectos de TI, que garantice la correcta asignación de prioridades y la coordinación de todos los proyectos.		
Controlar	Que las inversiones en el área de TI permitan soportar la estrategia actual y cumplir con las exigencias futuras de la organización.		
	Que los programas y proyectos se desarrollen con base a una metodología o mejores prácticas.		

Fuente: Elaboración Propia

Tabla 13: Definición Gestionar los Programas y Proyectos (Continuación)

Gestionar los Programas y Proyectos			
		Responsable	**Tecnología**
Prácticas Clave de Gobierno	Diseñar un marco de trabajo para la administración de proyectos, que incluya el alcance y los límites de la administración de proyectos, así como las metodologías a ser adoptadas y aplicadas al proyecto.	Jefe Oficina de Gobierno Corporativo TIC. Director de Apoyo al Comando y Control. Director de Tecnología. Director de Seguridad Informática. Director de Sistemas de Información.	Plan Estratégico Institucional. Plan Estratégico Tecnologías de Información. Ley 80 de 1993.
	Establecer un enfoque de administración de proyectos que corresponda al tamaño, complejidad y requerimientos regulatorios de cada proyecto.		
	Obtener el compromiso y la participación de los interesados afectados en la definición y ejecución del proyecto.		
	Definir y documentar la naturaleza y alcance del proyecto para confirmar y desarrollar, entre los interesados, un entendimiento común del alcance del proyecto y cómo se relaciona con otros proyectos dentro del programa global de inversiones facilitadas por TI.		
	Definir las responsabilidades, relaciones, autoridades y criterios de desempeño de los miembros del equipo del proyecto y especificar las bases para adquirir y asignar a los miembros competentes del equipo y/o a los contratistas al proyecto.		
	Eliminar o minimizar los riesgos específicos asociados con los proyectos individuales por medio de un proceso sistemático de planeación, identificación, análisis, respuesta, monitoreo y control de las áreas o eventos que tengan el potencial de ocasionar cambios no deseados.		
	Preparar un plan de administración de la calidad que describa el sistema de calidad del proyecto y cómo será implantado.		
	Establecer un sistema de control de cambios para cada proyecto, de tal modo que todos los cambios a la línea base del proyecto se revisen, aprueben e incorporen de manera apropiada al plan integrado del proyecto.		
	Medir el desempeño del proyecto contra los criterios clave del mismo y solicitar que, al finalizar cada proyecto, los interesados se cercioren de que el proyecto haya proporcionado los resultados y los beneficios esperados.		
Indicadores de Gestión	Porcentaje de proyectos que satisfacen las expectativas de los interesados con relación al alcance, tiempo, y presupuesto superior al 90%.		
	Porcentaje de proyectos con revisión posteriores a la implantación equivalente al 100%.		
	Porcentaje de proyectos ejecutados siguiendo las metodólogas propuestas por estándares y prácticas de administración de proyectos equivalente al 100%.		
	Porcentaje de partes interesadas satisfechas con la calidad del programa / proyecto superior al 90%. .		

Fuente: Elaboración Propia

11.2.3. Adquisición

Tabla 14: Definición Relaciones con proveedores.

Relaciones con proveedores			
		Responsable	**Tecnología**
Evaluar	Las opciones para el suministro de la Tecnología de la información con el fin de realizar las propuestas aprobadas, equilibrando los riesgos y el valor del dinero de las inversiones propuestas.	Jefe Oficina de Gobierno Corporativo TIC. Director de Apoyo al Comando y Control. Director de Tecnología. Director de Seguridad Informática. Director de Sistemas de Información.	Plan Estratégico Institucional. Plan Estratégico Tecnologías de Información. Ley 80 de 1993.
	Evaluar y seleccionar los proveedores en función de su capacidad para suministrar productos de acuerdo con los requisitos de la organización.		
Dirigir	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.		
	Todos los contratos asociados con los proyectos y operación de TI.		
	Un plan de dirección, supervisión, seguimiento, control y recibo a satisfacción de los bienes y servicios contratados		
Controlar	Que las inversiones en tecnología de la información puedan asegurar que éstas proporcionan las capacidades requeridas.		
	Que los proveedores sean seleccionados en función de su capacidad para suministrar productos de acuerdo con los requisitos de la organización.		
	Que el producto adquirido cumple los requisitos de compra especificados.		
Prácticas Clave de Gobierno	Identificar y evaluar las relaciones y contratos con proveedores.		
	Seleccionar proveedores en función de su capacidad para suministrar productos de acuerdo con los requisitos de la organización.		
	Gestionar contratos y relaciones con proveedores.		
	Gestionar el riesgo en el suministro.		
	Supervisar el cumplimiento y el rendimiento del proveedor.		
Indicadores de Gestión	Porcentaje de proveedores que cumplen con los requisitos acordados superior al 95%.		
	Número de infracciones de servicio causadas por los proveedores inferiores al 5%.		
	Número de eventos de riesgo que conducen a incidentes del servicio generados por los proveedores inferiores al 5%.		

Fuente: Elaboración Propia

Tabla 15: Definición Gestionar los Activos

Gestionar los Activos			
		Responsable	**Tecnología**
Evaluar	Las necesidades de adquisición de activos de TI, para determinar el valor que aportará al desempeño de los procesos que soportan la estrategia de la organización.	Jefe de Logística	SAP R3. Manual de Abastecimientos.
Dirigir	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.		
Controlar	Que los activos de Tecnología de la Información se adquieran de la manera correcta, incluida la preparación de la documentación adecuada, a la vez que se asegura el suministro de las capacidades requeridas.		
Prácticas Clave de Gobierno	Identificar y registrar activos actuales.		
	Gestionar activos críticos.		
	Gestionar el ciclo de vida de los activos.		
	Optimizar el coste de los activos.		
	Administrar licencias.		
Indicadores de Gestión	Porcentaje de identificación de los activos de TI equivalente al 100%.		
	Porcentaje de activos no utilizados inferior al 15%.		
	Porcentaje de activos obsoletos inferior al 1%.		

Fuente: Elaboración Propia

Tabla 16: Definición Gestión del Portafolio

Gestión del Portafolio			
		Responsable	**Tecnología**
Evaluar	El conjunto de direcciones estratégicas para la inversión alineada con la visión de la arquitectura empresarial.	Jefe Oficina de Gobierno Corporativo TIC. Director de Apoyo al Comando y Control. Director de Tecnología. Director de Seguridad Informática. Director de Sistemas de Información.	Plan Estratégico Institucional. Plan Estratégico Tecnologías de Información. Ley 80 de 1993.
	Las características deseadas de inversión y los portafolios de servicios relacionados.		
	Las capacidades actuales y requeridas de TI, para asegurar que los recursos de TI soporten los procesos actuales y futuros de la institución.		
Dirigir	Los programas y proyectos para asegurar que los recursos de TI soporten los procesos actuales y futuros de la institución.		
	Los programas y proyectos para asegurar que el portafolio de servicios se conserve actualizado de acuerdo con los requerimientos actuales y futuros de la institución.		
	Programas y servicios para gestionar la demanda con los recursos y restricciones de fondos, basados en su alineamiento con los objetivos estratégicos, así como en su valor y riesgo corporativo.		

Fuente: Elaboración Propia

Tabla 17: Definición Gestión del Portafolio (Continuación)

Gestión del Portafolio			
		Responsable	**Tecnología**
Controlar	El rendimiento global del portafolio de servicios y programas, proponiendo ajustes si fuesen necesarios en respuesta al rendimiento de programas y servicios o al cambio en las prioridades corporativas.	Jefe Oficina de Gobierno Corporativo TIC. Director de Apoyo al Comando y Control. Director de Tecnología. Director de Seguridad Informática. Director de Sistemas de Información.	Plan Estratégico Institucional. Plan Estratégico Tecnologías de Información. Ley 80 de 1993.
	Que el portafolio de servicios de TI se mantenga actualizado, de manera que el área de TI cumpla con los Acuerdos de Nivel de Servicio (ANS) asociados.		
Prácticas Clave de Gobierno	Determinar la disponibilidad y las fuentes de fondos.		
	Evaluar y seleccionar los programas a financiar.		
	Supervisar, optimizar e informar sobre el rendimiento del portafolio de inversiones.		
	Mantener los portafolios.		
	Gestionar la consecución de beneficios.		
Indicadores de Gestión	Porcentaje de inversiones de TI que tienen trazabilidad con la estrategia de la organización equivalente al 100%.		
	Porcentaje de las inversiones en TI donde los beneficios demandados son alcanzados o excedidos superior al 90%.		
	Nivel de satisfacción con los informes de satisfacción del portafolio superior al 90%.		
	Porcentaje de servicios de TI en los que se realizan los beneficios esperados superior al 100%.		

Fuente: Elaboración Propia

11.2.4. Desempeño

Tabla 18: Definición Administración de la calidad

Administración de la calidad			
		Responsable	**Tecnología**
Evaluar	Las necesidades de requerimientos de TI de la organización con la finalidad de establecer y mantener un sistema de gestión de la calidad para la información, la tecnología y los procesos institucionales.	Inspección General	Modelo Estándar de Control Interno Sistema de Gestión de la Calidad.
	Oportunidades de mejora en los procesos de TI, de modo que pueda focalizar esfuerzos en la optimización de estos a través de las TI para contribuir con el cumplimiento de los objetivos institucionales.		
Dirigir	La implementación de un plan de calidad de los servicios de TI que incluya etapas de aseguramiento, control e inspección, medición de indicadores de calidad, actividades preventivas, correctivas y de mejoramiento continuo.		
Controlar	Las actividades preventivas, correctivas y de mejoramiento continuo de la calidad de los procesos.		
	Que se cumpla con los requerimientos del negocio y con la gestión de la calidad a nivel corporativo.		

Fuente: Elaboración Propia

Tabla 15: Definición Administración de la calidad (Continuación)

Administración de la calidad			
		Responsable	**Tecnología**
Prácticas Clave de Gobierno	Establecer un sistema de gestión de la calidad.	Inspección General	Modelo Estándar de Control Interno Sistema de Gestión de la Calidad.
	Definir y gestionar los estándares, procesos y prácticas de calidad.		
	Supervisar y hacer controles y revisiones de calidad.		
	Integrar la gestión de la calidad en la implementación de soluciones y la entrega de servicios.		
	Mantener una mejora continua.		
Indicadores de Gestión	Porcentaje de partes interesadas satisfechas con el cumplimiento del servicio de TI entregado respecto a los niveles de servicio acordados superior al 95%.		
	Número de interrupciones del negocio debidas a incidentes en el servicio de TI inferiores al 5%.		
	Porcentaje de procesos de TI revisados de manera formal por aseguramiento de calidad de modo periódico que satisfaga las metas y objetivos de calidad equivalente al 100%.		

Fuente: Elaboración Propia

Tabla 19: Definición Gestión de riesgos

Gestión de riesgos			
		Responsable	**Tecnología**
Evaluar	Los riesgos relacionados con TI de forma continua, dentro de niveles de tolerancia establecidos por la dirección ejecutiva de la organización.	Inspección General Jefe Oficina de Gobierno Corporativo TIC. Director de Seguridad Informática.	Modelo Estándar de Control Interno Sistema de Gestión de la Calidad.
Dirigir	Planes y programas para asegurar la integración de la gestión de riesgos relacionados con TI con la gestión de riesgos de la organización.		
	Equilibrar los costes y beneficios de gestionar riesgos organizacionales relacionados con TI.		
Controlar	Que se documente adecuadamente cada una de las etapas surtidas para el proceso de Gestión de Riesgos.		
	Que se cumpla con el plan de tratamientos de riesgos definido para el área de TI.		
	A los responsables de toma de decisiones apropiados y asegurarse de que la causa, los requerimientos de respuesta y la mejora del proceso se incluyan en los procesos de gobierno del riesgo.		
Prácticas Clave de Gobierno	Recopilar datos.		
	Analizar el riesgo.		
	Mantener un plan de tratamiento del riesgo.		
	Expresar el riesgo.		
	Definir un portafolio de acciones para la gestión de riesgos.		
	Responder al riesgo.		
Indicadores de Gestión	Porcentaje de procesos de negocio claves incluidos en el plan de tratamiento de riesgo equivalente al 100%.		
	Número de incidentes significativos no identificados e incluidos en el portafolio de gestión de riesgos inferior al 5%.		
	Porcentaje de planes de acción para riesgos de TI ejecutados de la forma que fueron diseñados superior al 90%.		

Fuente: Elaboración Propia

Tabla 20: Definición Seguridad de los sistemas

Seguridad de los sistemas			
		Responsable	**Tecnología**
Evaluar	Los marcos de referencia y las mejores prácticas de seguridad de los sistemas.	Jefe Oficina de Gobierno Corporativo TIC. Director de Seguridad Informática. Jefe de Ciberseguridad y Ciberdefensa.	Política de Seguridad de la Información
	Los procedimientos de la organización con la finalidad de determinar si se cumple la política de seguridad de los sistemas.		
Dirigir	Al equipo de TI en el camino correcto para mantener el impacto y ocurrencia de los incidentes de la seguridad de los sistemas dentro de los niveles de tolerancia de riesgo de la organización.		
	La planificación e implementación de la política de seguridad de los sistemas.		
Controlar	El cumplimiento de la política de seguridad de los sistemas.		
	El cumplimiento y soporte de acuerdo con las leyes y regulaciones externas.		
	La preservación de la confidencialidad, integridad, disponibilidad de la información.		
Prácticas Clave de Gobierno	Establecer y mantener un SGSI.		
	Definir y gestionar un plan de tratamiento del riesgo de la seguridad de los sistemas.		
	Supervisar y revisar el SGSI.		
Indicadores de Gestión	Número de incidentes de seguridad causantes de pérdidas financieras, interrupciones del negocio o pérdida de imagen pública inferior al 1%.		
	Cumplimiento de la evaluación de seguridad frente a los últimos estándares y mejores prácticas equivalente al 100%.		
	Nivel de satisfacción de las partes interesadas con el plan de seguridad de los sistemas superior al 95%.		
	Número de incidentes de seguridad causados por la no observancia del plan de seguridad inferior al 3%.		

Fuente: Elaboración Propia

Tabla 21: Definición Gestión de cambios

Gestión de cambios			
		Responsable	**Tecnología**
Evaluar	Las necesidades de cambios, incluyendo cambios estándar de mantenimiento de emergencia en relación con los procesos de negocio, aplicaciones e infraestructura.	Jefe Tecnologías de la Información y Comunicaciones. Jefe Oficina de Gobierno Corporativo TIC. Jefe Comportamiento Humano	Manual de Gestión del Cambio
Dirigir	Al equipo de TI de forma que se asegure el cumplimiento de las normas y procedimientos de cambio, análisis de impacto, priorización y autorización.		
	A la institución para abordar y adaptarse al cambio, y gestionar los efectos generados por éste.		
Controlar	El monitoreo y evaluación del impacto del uso y apropiación de cambios realizados en TI.		
	Los cambios aprobados, realizando seguimiento durante todo el proceso.		
	Como se comunica el estado de cambios aprobados, en proceso y completados.		

Fuente: Elaboración Propia

Tabla 22: Definición Gestión de cambios (Continuación)

Gestión de cambios			
		Responsable	**Tecnología**
Prácticas Clave de Gobierno	Evaluar, priorizar y autorizar peticiones de cambio.	Jefe Tecnologías de la Información y Comunicaciones. Jefe Oficina de Gobierno Corporativo TIC. Jefe Comportamiento Humano	Manual de Gestión del Cambio
	Gestionar cambios de emergencia.		
	Hacer seguimiento de cambios de estado.		
	Cerrar y documentar los cambios.		
Indicadores de Gestión	Porcentaje de cambios sin éxito debido a evaluaciones de impacto inadecuadas inferior al 3%.		
	Porcentaje sobre el total de cambios que corresponde a cambios de emergencia inferior al 5%.		
	Ratios de satisfacción de las partes interesadas con las comunicaciones de los cambios superior al 95%.		

Fuente: Elaboración Propia

Tabla 23: Definición Continuidad del negocio

Continuidad del negocio			
		Responsable	**Tecnología**
Evaluar	Procedimientos específicos que respondan a interrupciones del servicio, con el fin de proteger y recuperar las funciones críticas de la organización y responder a incidentes e interrupciones de servicio.	Jefe Tecnologías de la Información y Comunicaciones. Jefe Oficina de Gobierno Corporativo TIC. Director de Apoyo al Comando y Control. Director de Tecnología. Director de Seguridad Informática. Director de Sistemas de Información.	Plan Estratégico Institucional. Plan Estratégico Tecnologías de Información. Política de Seguridad de la Información
Dirigir	La operación continua de los procesos críticos para el negocio y los servicios de TI requeridos.		
	Al personal clave interno y externo requerido para la operación de las actividades críticas de la organización.		
Controlar	La disponibilidad de la información a un nivel aceptable para la organización ante el evento de una interrupción significativa.		
	Los tiempos mínimos de recuperación requeridos en los que no se vea afectado la continuidad de la operación de la organización.		
Prácticas Clave de Gobierno	Definir la política de continuidad del negocio, objetivos y alcance.		
	Mantener una estrategia de continuidad.		
	Desarrollar e implementar una respuesta a la continuidad del negocio.		
	Ejercitar, probar y revisar el plan de continuidad.		
	Revisar, mantener y mejorar el plan de continuidad.		
	Proporcionar formación en el plan de continuidad.		
	Gestionar acuerdos de respaldo.		
	Ejecutar revisiones posteriores a la reanudación.		
Indicadores de Gestión	Interrupciones del negocio debido a incidentes en el servicio de TI inferiores al 5%.		
	Porcentaje de servicios de TI que cumplen los requisitos de tiempos de funcionamiento superiores al 95%.		
	Porcentaje de sistemas críticos para el negocio no cubiertos por el plan inferiores al 1%.		
	Porcentaje de ejercicios y pruebas que han conseguido los objetivos de recuperación equivalente al 100%.		
	Porcentaje de asuntos identificados que se han incluido satisfactoriamente en el plan equivalente al 100%.		

Fuente: Elaboración Propia

11.2.5. Cumplimiento

Tabla 24: Definición Cumplimiento con los requerimientos de usuario

Cumplimiento con los requerimientos de usuario			
		Responsable	**Tecnología**
Evaluar	Los mecanismos que permitan cuantificar y monitorear los tiempos y costos de los requerimientos de los usuarios, a través de una base de conocimiento y registro de requerimientos.	Jefe Oficina de Gobierno Corporativo TIC. Director de Apoyo al Comando y Control. Director de Tecnología. Director de Seguridad Informática. Director de Sistemas de Información	Plan Estratégico Institucional. Plan Estratégico Tecnologías de Información. Sistema de Gestión de la Calidad.
Dirigir	Los planes que permitan identificar, especificar, diseñar, publicar los acuerdos de servicio.		
	La identificación, la especificación y el análisis de las necesidades funcionales y no funcionales.		
Controlar	La trazabilidad de los requerimientos a través del ciclo de vida de los sistemas de información.		
	Los niveles de servicio e indicadores de rendimiento para garantizar el cubrimiento de las necesidades presentes y futuras de la empresa.		
Prácticas Clave de Gobierno	Identificar servicios TI.		
	Catalogar servicios basados en TI.		
	Definir y preparar acuerdos de servicio.		
	Supervisar e informar de los niveles de servicio.		
	Revisar acuerdos de servicio y contratos.		
Indicadores de Gestión	Porcentaje de procesos de negocio con acuerdo de servicio sin definir inferior al 5%.		
	Porcentaje de servicios de TI activos cubiertos por acuerdos de servicio superior al 95%.		
	Porcentaje de servicios monitorizados para cumplir los acuerdos de servicio equivalente al 100%.		

Fuente: Elaboración Propia

11.2.6. Comportamiento Humano

Tabla 25: Definición Gestionar el conocimiento

Gestionar el conocimiento			
		Responsable	**Tecnología**
Evaluar	Las necesidades de conocimiento de la empresa y mantener la disponibilidad de conocimiento relevante, actual, validado y fiable, donde se valoren los distintos elementos que lo componen, a fin de determinar el papel que desempeña cada uno de ellos y cómo beneficia su inclusión y participación.	Jefatura de Educación Aeronáutica Jefe Oficina de Gobierno Corporativo TIC.	Plan de Capacitación.
Dirigir	Cómo se soportan todas las actividades de los procesos y facilitar la toma de decisiones.		
	Un equipo de multiplicadores de los procesos de aprendizaje que apoyen al desarrollo del Sistema de Gestión de Conocimiento, mediante la creación de contenidos o la transferencia de conocimiento.		
Controlar	El conocimiento adquirido sobre un proceso, a través de la reflexión y el análisis crítico sobre los factores que pueden haber afectado positiva o negativamente.		
	La identificación, recopilación, organización y controlar su mantenimiento, uso y retirada de conocimiento.		

Fuente: Elaboración Propia

Tabla 26: Definición Gestionar el conocimiento (Continuación)

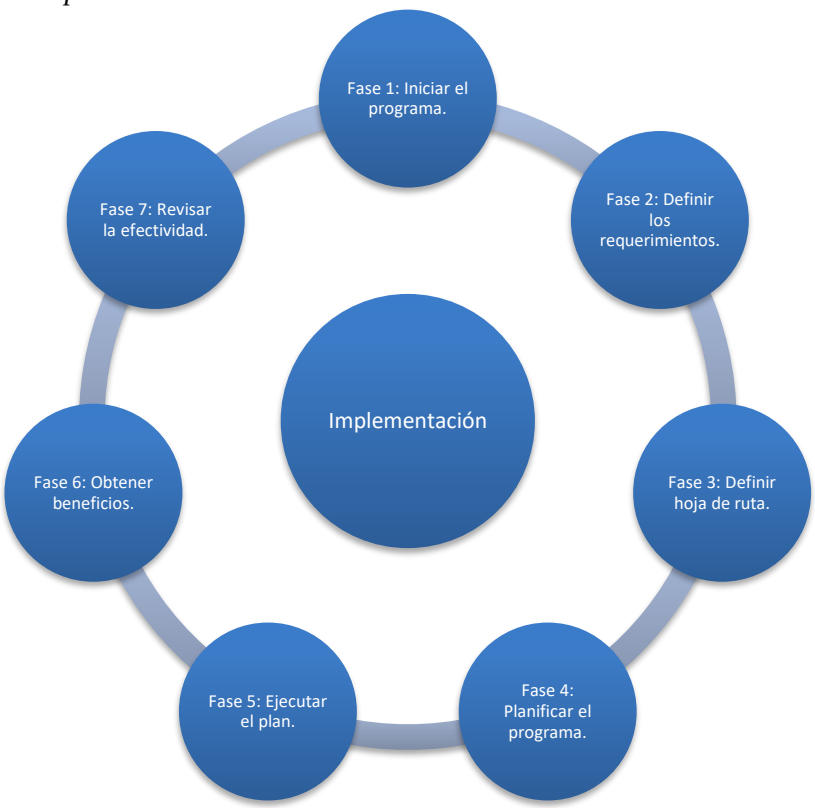
Gestionar el conocimiento			
		Responsable	**Tecnología**
Prácticas Clave de Gobierno	Cultivar y facilitar una cultura de intercambio de conocimientos.	Jefatura de Educación Aeronáutica Jefe Oficina de Gobierno Corporativo TIC.	Plan de Capacitación.
	Identificar y clasificar las fuentes de información.		
	Organizar y contextualizar la información, y transformarla en conocimiento.		
	Utilizar y compartir el conocimiento.		
	Evaluar y retirar la información.		
Indicadores de Gestión	Volumen de información clasificado superior al 90%.		
	Porcentaje cubierto de categorías de información superior al 90%.		
	Número de usuarios formados en el uso y compartición de información superior al 90%.		
	Porcentaje del repositorio de conocimiento utilizado superior al 90%.		

Fuente: Elaboración Propia

12. Plan de implementación del modelo

Para diseñar el plan de implementación del modelo propuesto se tomó como referencia la guía de implementación de COBIT 5, toda vez que su objetivo es proveer un enfoque de buenas prácticas a la hora de implementar un modelo de gobierno de TI basado en un ciclo de vida de mejora continua, el cual debe adaptarse a las necesidades específicas de la Fuerza Aérea Colombiana. En este sentido, el alcance del plan de implementación está delimitado por la definición de las fases, como se ilustra en el gráfico 25, así como el objetivo, las actividades y entregables para cada una de ellas. Por otro lado, el indicador de cumplimiento de cada fase estará definido por la elaboración de cada entregable y su correspondiente validación y aceptación por parte de la Jefatura de las Tecnologías de la Información y Comunicaciones. En este sentido vale la pena resaltar que el desarrollo de todos los entregables de cada fase son prerrequisito para continuar con la siguiente.

Gráfico 25: Plan de Implementación



Fuente: Elaboración Propia

Tabla 27: Fase 1: Iniciar el programa

Fase 1: Iniciar el programa	
Objetivo	Identificar y comunicar a la dirección ejecutiva y a las partes interesadas, el motivador para iniciar con la implementación de un modelo de Gobierno de TI en la Jefatura de las Tecnologías de la Información y Comunicaciones, así como obtener el apoyo de la alta dirección y el compromiso de las partes interesadas. En este sentido, el marco normativo para las entidades públicas, tendencias, deficiencias en el desempeño, e incluso los objetivos de la institución pueden actuar como motivadores del cambio.
Actividades	Identificar los problemas que desencadenan la necesidad de actuar.
	Identificar las prioridades y estrategias organizacionales que afectan a la TI.
	Conseguir el acuerdo de la dirección para actuar y obtener apoyo ejecutivo.
	Definir los roles y los responsables de la implementación del proyecto.
	Definir la política, objetivos, principios rectores y objetivos de alto nivel de mejora de Gobierno de TI.
Entregables	Estrategia de TI.
	Políticas de TI.
	Roles y responsabilidades.

Fuente: Elaboración Propia

Tabla 28: Fase 2: Definir los requerimientos

Fase 2: Definir los requerimientos	
Objetivo	Se debe asegurar que el equipo de TI conoce y entiende la estrategia organizacional, los objetivos, y el marco normativo, así como identificar los procesos críticos que se abordarán en el plan de mejora, identificando los requerimientos y las prácticas de gestión adecuadas para cada proceso seleccionado.
Actividades	Evaluar el estado actual.
	Evaluar las necesidades de TI para apoyar los objetivos de la organización.
	Evaluar el desempeño actual.
	Formar un equipo de implementación.
	Definir los requerimientos.
Entregables	Calificación de la capacidad actual para los procesos seleccionados.
	Mapa de Capacidades de TI.
	Especificaciones funcional y no funcional de los requerimientos.

Fuente: Elaboración Propia

Tabla 29: Fase 3: Definir hoja de ruta

Fase 3: Definir hoja de ruta	
Objetivo	Establece los objetivos de mejora seguidos por un análisis comparativo para identificar las potenciales soluciones. Determinar la capacidad objetivo para cada uno de los procesos seleccionados. Determinar las diferencias entre las posiciones actuales y futuras de los procesos seleccionados y traducir estas diferencias en oportunidades de mejora.
Actividades	Establecer la dirección, alcance, beneficios y objetivos de alto nivel del programa.
	Asegurar el alineamiento de los objetivos de TI con la estrategia de la organización.
	Considerar los riesgos y ajustar el alcance.
	Considerar las implicaciones de la habilitación del cambio.
	Obtener los presupuestos necesarios y definir las responsabilidades del programa.
Entregables	Calificación de capacidad objetivo para los procesos seleccionados.
	Descripción de las oportunidades de mejora.
	Estrategia de comunicación.
	Métricas clave que se utilizarán para realizar el seguimiento del programa y del desempeño operativo.

Fuente: Elaboración Propia

Tabla 30: Fase 4: Planificar el programa

Fase 4: Planificar el programa	
Objetivo	Traducir oportunidades de mejora en proyectos justificables que contribuyan al cumplimiento de los requerimientos identificados. Priorizar y centrarse en los proyectos de alto impacto. Integrar los proyectos de mejora en la planificación general.
Actividades	Priorizar y seleccionar las oportunidades de mejora.
	Definir los proyectos a desarrollar para alcanzar el nivel de capacidad deseado.
Entregables	Matriz de priorización de requerimientos.
	Plan de implementación

Fuente: Elaboración Propia

Tabla 31: Fase 5: Ejecutar el plan

Fase 5: Ejecutar el plan	
Objetivo	Implementar los proyectos de mejora detallados, aprovechando las capacidades, normas y prácticas de gestión de programa y proyectos. Monitorizar, medir e informar sobre los avances del proyecto.
Actividades	Desarrollar soluciones que incluyan el alcance completo de las actividades definidas en el plan.
	Dirigir y supervisar la contribución de todos los proyectos en el programa para asegurar la entrega de los resultados esperados.
	Aprobar la iniciación de cada fase importante del programa y comunicarlo a todas las partes.
Entregables	Informe de seguimiento y evaluación del avance del proyecto.
	Informe de hallazgos y riesgos identificados en la implementación del plan.

Fuente: Elaboración Propia

Tabla 32: Fase 6: Obtener beneficios

Fase 6: Obtener beneficios	
Objetivo	Integrar las métricas de desempeño del proyecto y la realización de los beneficios del programa global de mejora del gobierno en el sistema de medición del desempeño para su seguimiento regular y continuo.
Actividades	Operar las soluciones y obtener retroalimentación sobre el rendimiento.
	Realizar el seguimiento del cambio y evaluar la eficacia de los planes de respuesta al cambio, vinculando los resultados a los objetivos de cambio y las metas originales.
	Comunicar los resultados positivos y negativos de las medidas de rendimiento a todas las partes
Entregables	Evaluación de los indicadores de gestión.
	Informes explicando los resultados de los cuadros de mando.

Fuente: Elaboración Propia

Tabla 33: Fase 7: Revisar la efectividad

Fase 7: Revisar la efectividad	
Objetivo	Supervisar continuamente el rendimiento, asegurar que los resultados se notifican regularmente y se transfiere el compromiso y la titularidad de todas las responsabilidades y obligaciones.
Actividades	Mantener una campaña de comunicación continua.
	Documentar lecciones aprendidas.
	Comparar los resultados obtenidos con los criterios de éxito iniciales.
	Identificar los nuevos objetivos y requisitos de gobierno basados en la experiencia adquirida, los objetivos actuales de negocio para TI.
	Compartir el conocimiento de la iniciativa con la organización.
	Mantener y reforzar los cambios.
Entregables	Lecciones aprendidas.
	Recomendaciones para actividades adicionales de Gobierno de TI.
	Encuesta de satisfacción a las partes interesadas.

Fuente: Elaboración Propia

Finalmente, de acuerdo con las fases propuestas para la implementación del gobierno de TI, en la tabla 29 se ilustra el cronograma, en el cual se detalla el tiempo que puede ser empleado en el desarrollo de cada una de las fases propuestas.

Tabla 34: Cronograma de implementación

Fase	**Tiempo del proyecto en meses**																			
	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	Responsable	Presupuesto
Iniciar el programa																			Jefe de tecnologías de la información y comunicaciones	$5.000.000
Definir los requerimientos																			Jefe oficina gobierno corporativo de TIC	$50.000.000
Definir hoja de ruta																			Jefe oficina gobierno corporativo de TIC	$15.000.000
Planificar el programa																			Jefe oficina gobierno corporativo de TIC	$15.000.000
Ejecutar el plan																			Jefe oficina gobierno corporativo de TIC	$45.000.000
Obtener beneficios																			Jefe oficina gobierno corporativo de TIC	$15.000.000
Revisar la efectividad																			Jefe de tecnologías de la información y comunicaciones	$5.000.000

Fuente: Elaboración Propia

13. Validación del modelo

Para realizar la validación del modelo de Gobierno de TI, inicialmente se diseñó un resumen ejecutivo, y además se creó una encuesta, la cual fue aplicada a profesionales con experiencia laboral en la oficia de Gobierno Corporativo de TIC o en la gestión de TI en la Fuerza Aérea Colombiana.

Tabla 35: Ficha técnica de la encuesta de validación

FICHA TECNICA DE LA ENCUESTA	
Dirección	La encuesta de esta investigación fue realizada por Carlos Alberto Velásquez Pineda y Andrei Bahamon Páez, estudiantes de Maestría en Gerencia de Sistemas de Información y Proyectos Tecnológicos de la Universidad EAN.
Técnica	El tipo de encuesta utilizada fue de preguntas cerradas tipo si/no, selección múltiple y una pregunta de tipo abierta para sugerencias sobre el modelo de gobierno de TI propuesto en el presente proyecto.
Fecha de realización	La encuesta fue realizada el 7 de septiembre de 2020.
Cantidad de entrevistados	5 oficiales con experiencia laboral en la oficia de Gobierno Corporativo de TIC o en la gestión de TI en la Fuerza Aérea Colombiana.

Fuente: Elaboración Propia

Lo anterior, con la finalidad de que a través de un juicio de expertos se avale el modelo diseñado. El personal de profesionales de la Fuerza Aérea Colombiana que cumplen con el perfil para validar el modelo de Gobierno de TI es:

Tabla 36: Validadores del Modelo

Nombre	Cargo
Coronel Nilssen Janeth Gutiérrez Suarez	Jefe de las Tecnologías de la Información y Comunicaciones
Coronel José Miguel Borraez Álvarez	Director de Tecnología
Teniente Coronel Luisa Fernanda Díaz Carvajal	Jefe Oficina Gobierno Corporativo de TIC
Teniente Coronel Oscar Fernando Arias Suarez	Director de Apoyo al Comando y Control
Mayor Jairo Andrés Lasso Moreno	Especialista Operacional Desarrollo Tecnológico de TIC

Fuente: Elaboración Propia

Por otro lado, los principales aspectos que se quieren validar son:

- Los lineamientos definidos a partir del análisis estratégico realizado.
- Los requerimientos sobre los cuales se diseñó el modelo de Gobierno de TI.
- La correlación de los requerimientos con los elementos que se deben considerar en el modelo de gobierno de TI propuesto, tales como personas, procesos, tecnología, servicios y datos.

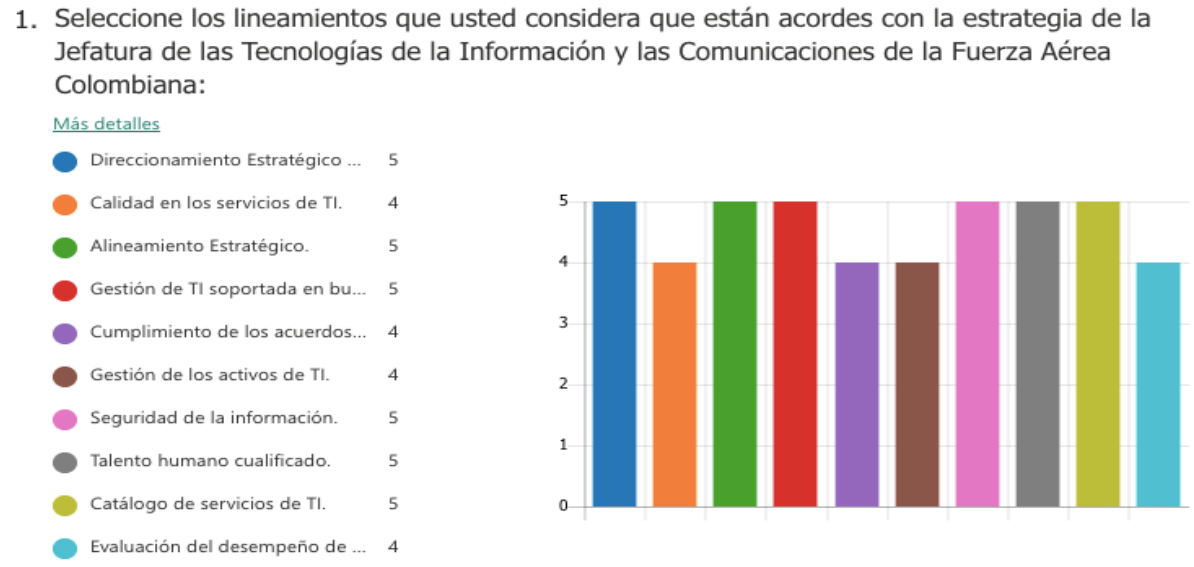
- El modelo de Gobierno de TI propuesto.
- El plan de implementación del modelo de Gobierno de TI en la Jefatura de las Tecnologías de la Información y Comunicaciones.

13.1. Resultados Obtenidos

Una vez aplicada la encuesta al personal de oficiales seleccionados para validar los elementos anteriormente descritos, se obtuvieron los siguientes resultados:

En el gráfico 26 se observa que 6 lineamientos fueron avalados por el 100% de los expertos encuestados, mientras que 4 de ellos, obtuvieron el 80% de los votos. Lo anterior permite concluir que los lineamientos definidos a partir del análisis estratégico realizado están acordes con la misión, la visión y los objetivos de la Jefatura de las Tecnologías de la Información y Comunicaciones.

Gráfico 26: Resultados Pregunta 1

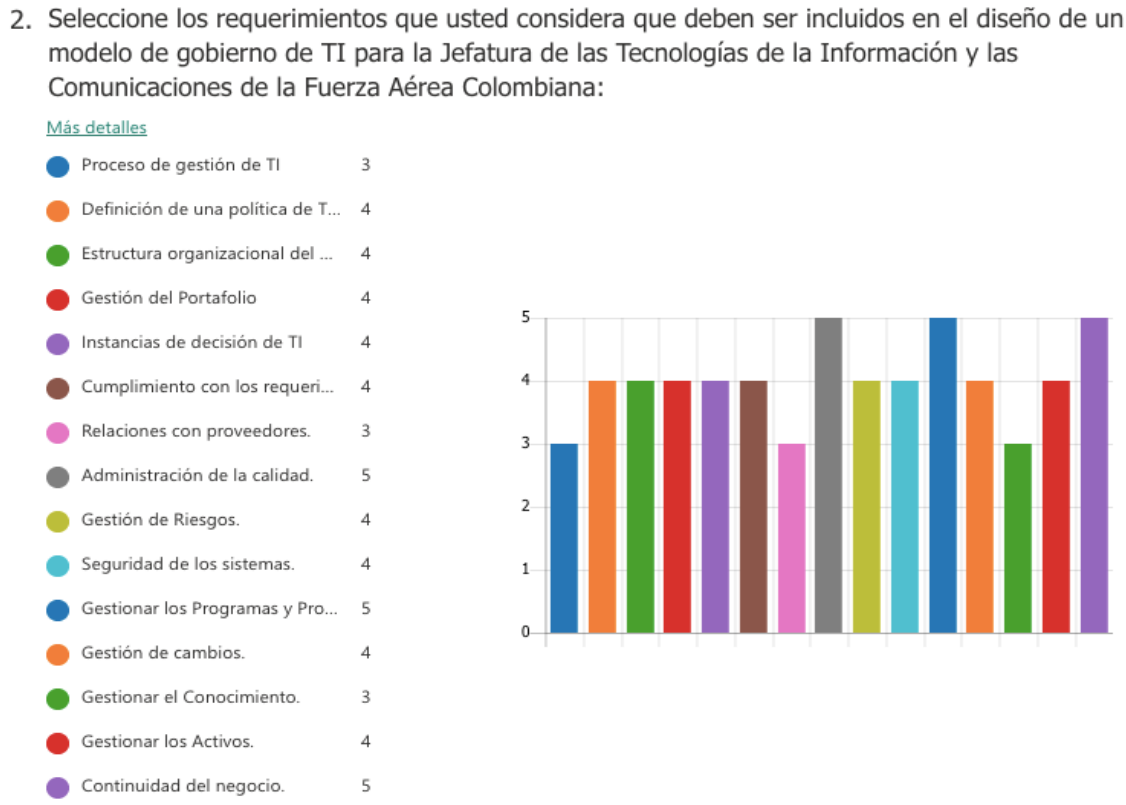


Fuente: Elaboración Propia

De igual manera, en el gráfico 27 se observa que 3 de los requerimientos fueron avalados por el 100% de los encuestados, 9 por el 80% y 3 por el 60%. Lo anterior permite concluir que, de acuerdo con el juicio de expertos, los requerimientos definidos cumplen con lo estipulado en la

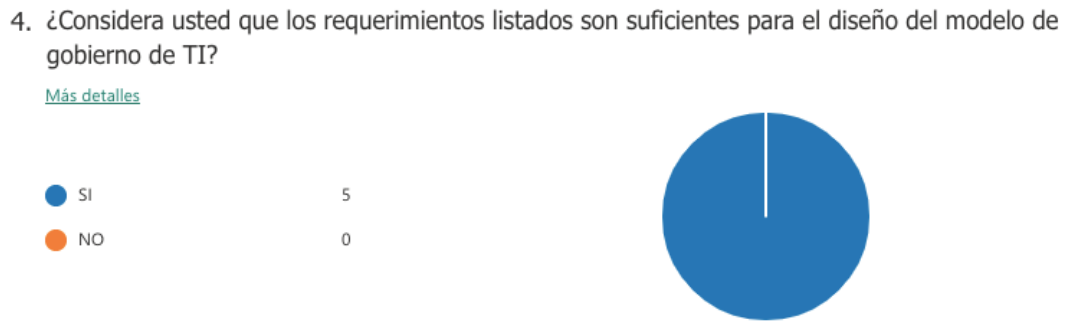
política de Gobierno Digital y en el Plan Estratégico de Tecnologías de Información PETI. Así mismo, el gráfico 28 indica que, de acuerdo con los resultados de la encuesta, los requerimientos identificados son suficientes para diseñar el modelo de gobierno de TI.

Gráfico 27 Resultados Pregunta 2



Fuente: Elaboración Propia

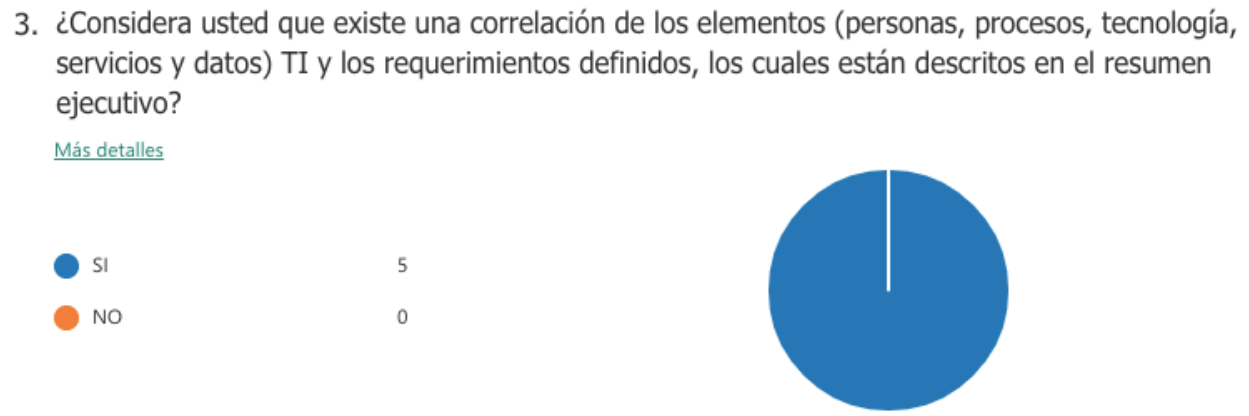
Gráfico 28: Resultados Pregunta 4



Fuente: Elaboración Propia

Por otro lado, el gráfico 29 ilustra que el 100% de los encuestados consideran que existe una correlación entre los requerimientos definidos y las personas, procesos, tecnología, servicios y datos.

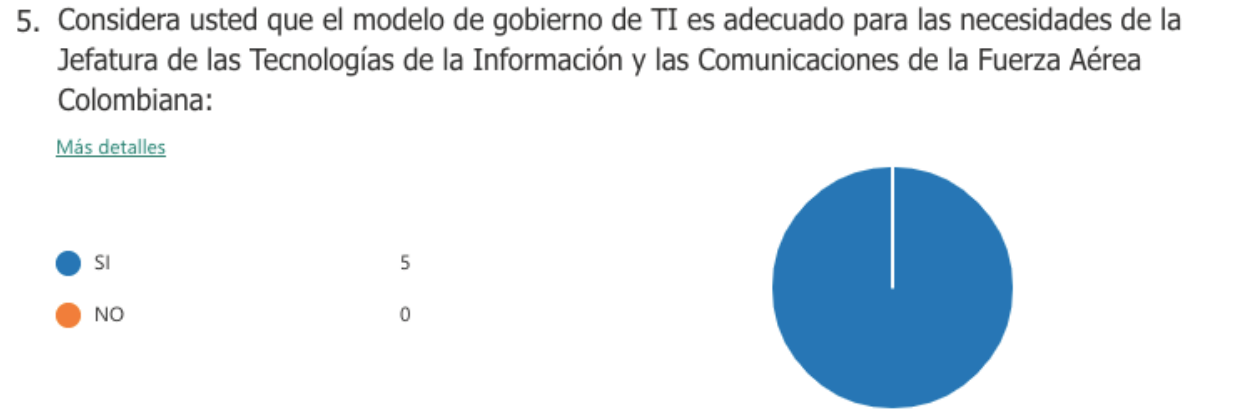
Gráfico 29: Resultados Pregunta 3



Fuente: Elaboración Propia

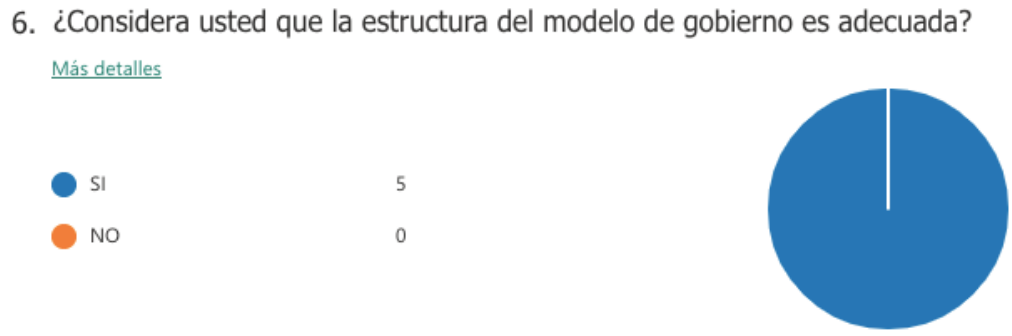
Con relación al modelo de gobierno propuesto, en el gráfico 30 se puede observar que todos los expertos encuestados consideran que el modelo propuesto es adecuado para las necesidades de la Jefatura, que su estructura es adecuada, ver gráfico 31, que involucra las estructuras, procedimientos y políticas, ver gráfico 32 y que, además, la estructura permite que el modelo sea escalable, de manera que se puedan incluir futuros requerimientos, ver gráfico 33.

Gráfico 30: Resultados Pregunta 5



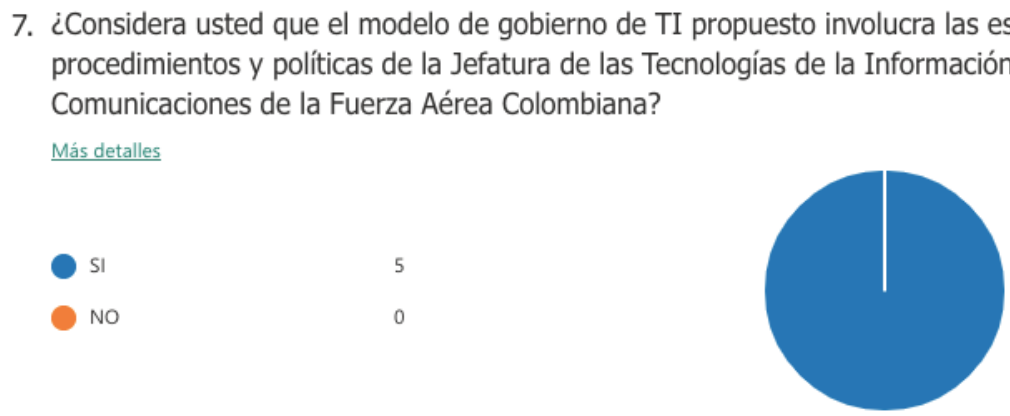
Fuente: Elaboración Propia

Gráfico 31: Resultados Pregunta 6



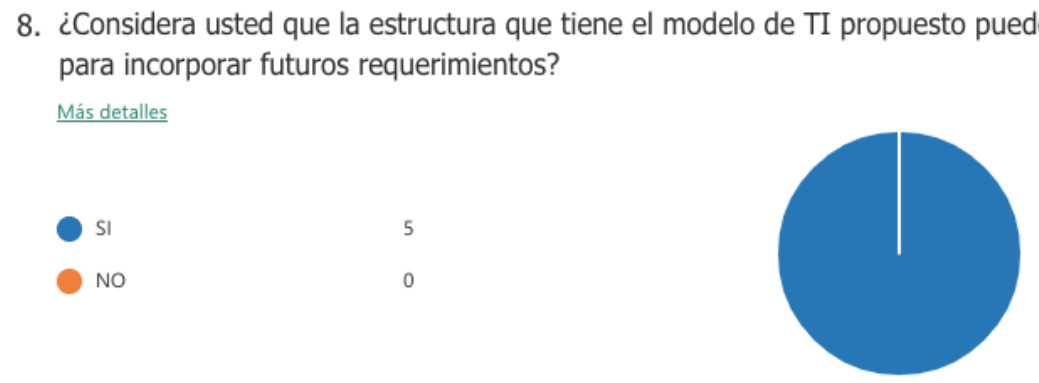
Fuente: Elaboración Propia

Gráfico 32: Resultados Pregunta 7



Fuente: Elaboración Propia

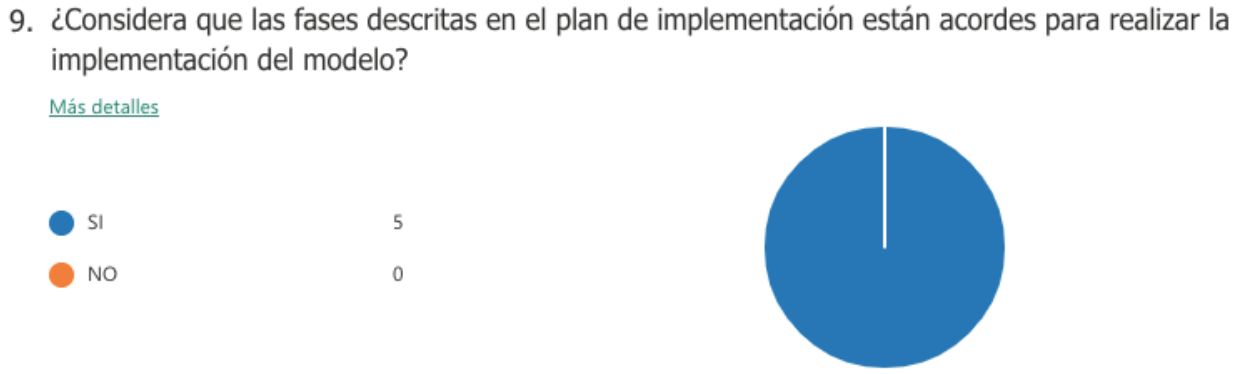
Gráfico 33: Resultados Pregunta 8



Fuente: Elaboración Propia

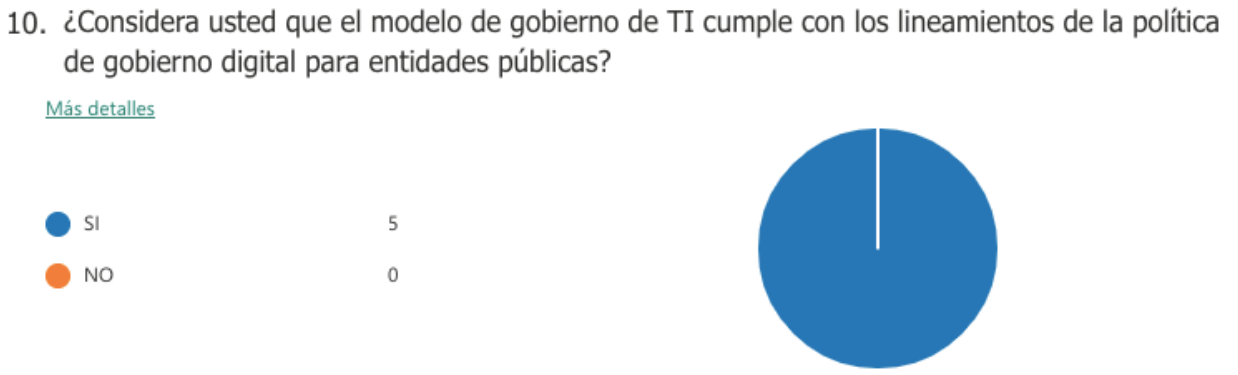
Finalmente, en el gráfico 34 se observa que todos los encuestados avalan las fases propuestas para la implementación del modelo propuesto. El cual cumple con los lineamientos de la política de Gobierno Digital para entidades públicas, como se observa en el gráfico 35.

Gráfico 34: Resultados Pregunta 9



Fuente: Elaboración Propia

Gráfico 35: Resultados Pregunta 10



Fuente: Elaboración Propia

14. Recomendaciones y conclusiones

14.1. Recomendaciones

- La Jefatura de las Tecnologías de la Información y Comunicaciones, para dar cumplimiento a la política de Gobierno Digital, debe implementar un Gobierno TI, toda vez que es un elemento habilitador del dominio de Infraestructura.

- De los requerimientos identificados en el diagnóstico, se recomienda dar prioridad a gestionar los Acuerdos de Servicio, Gestionar el Conocimiento y Gestión de Cambios, toda vez que son los que actualmente están menos desarrollados.

- Se deben realizar revisiones periódicas del modelo propuesto, toda vez que, dada la evolución constante de la política de Gobierno Digital, se pueden generar futuros requerimientos.

- De acuerdo con la validación del modelo por parte de los expertos, se recomienda incluir dentro de los lineamientos, la estrategia para el uso y apropiación de TI en la FAC y la gestión de las no conformidades con los servicios de TI.

- Se recomienda considerar la seguridad de la información en todos los componentes de TI, por ello es necesario establecer seguridad de la información desde una visión de cobertura general a todos los activos de TI.

- En el tratamiento del requerimiento de gestión de la continuidad del negocio, se recomienda complementar su desarrollo, de modo tal que se incluyan escenarios de guerra, toda vez que la Fuerza Aérea Colombiana es una organización militar, que pertenece al sector defensa.

- Para el éxito en la implementación del Gobierno de TI en la Jefatura de las Tecnologías de la Información y Comunicaciones, se recomienda la participación y compromiso de la alta dirección de la Fuerza Aérea Colombiana, de manera que se asignen los recursos necesarios para lleva a cabo su implementación.

14.2. Conclusiones

- De acuerdo con lo planteado en el proyecto, fue posible desarrollar cada uno de los objetivos propuestos desde el diagnóstico y el análisis estratégico, para realizar el modelo de gobierno TI con su plan de implementación y validación.

- De acuerdo con el marco normativo para el sector público, es necesaria la implementación de un marco de Gobierno de TI en la Jefatura de las Tecnologías de la Información y Comunicaciones, de manera que la entidad cumpla con las directrices de la política de Gobierno Digital.

- De acuerdo con los resultados obtenidos en la valoración de expertos, se concluye que la arquitectura del modelo de Gobierno de TI propuesto es adecuada y escalable, cumple con las necesidades de la Jefatura de las Tecnologías de la Información y las Comunicaciones de la Fuerza Aérea Colombiana para la gestión de los recursos de TI, involucra las estructuras, procedimientos y políticas y cumple con los lineamientos de la política de Gobierno Digital para entidades públicas.

- Del análisis de la estrategia de la Jefatura de las Tecnologías de la Información y Comunicaciones se identificaron los lineamientos que, complementados con el marco normativo y la política de Gobierno Digital, aportaron los requerimientos adecuados para la elaboración de un modelo de gobierno de TI que armonice la estrategia de la Jefatura con la institucional.

- La implementación de un Gobierno de TI en la Jefatura de las Tecnologías de la Información y Comunicaciones, permite emitir las políticas y lineamientos para la adquisición, implementación, uso y apropiación de los recursos de TI, de manera que potencialice el rendimiento de servicios de TI.

- El gobierno corporativo de TI permite administrar los servicios de TI, con la finalidad de proteger los activos y garantizar que los recursos sean usados responsablemente bajo un marco regulatorio.

- Una organización que implemente un gobierno de TI asegura que las inversiones en tecnologías de información y comunicaciones generen valor agregado para el negocio y que los riesgos asociados sean mitigados.

- Considerando que los servicios de TI cada vez influyen más en el desarrollo de los procesos de las organizaciones, se hace necesario implementar un gobierno de TI basado en buenas prácticas y marcos de referencia, de manera que se potencialice el aporte de los servicios de TI al cumplimento de los objetivos organizacionales.

- La adopción de estándares promueve la eficiencia y buena gestión de los procesos de tecnología, permitiendo comparar y mejorar acorde a los objetivos del negocio, además de identificar y gestionar los riesgos potenciales que afecten el cumplimiento de los objetivos.

15. Referencias

Argudo, S. (2013). *Mejorar las búsquedas de información*. Editorial UOC. https://books.google.com.co/books?id=LzrFAgAAQBAJ&printsec=frontcover&dq=argudo+2012&hl=es&sa=X&ved=0ahUKEwiNmf-989noAhVPmuAKHe62Cb4Q6AEIKDAA#v=onepage&q=argudo 2012&f=false

Bhatt, G. D., & Grover, V. (2005). Types of information technology capabilities and their role in competitive advantage: An empirical study. *Journal of Management Information Systems*, *22*(2), 253–277. https://doi.org/10.1080/07421222.2005.11045844

Ceipa, C. (2011). *Continuidad TI Bancolombia*. Wordpress.Com. https://cristinaysandraceipa.wordpress.com/2011/03/29/27/

Cordero, W. (2011). *Asegurar la continuidad de los procesos administrativos de servicios basados en ITIL y COBIT*.

Corona, L. (2002). Innovación y competitividad empresarial. *Feder*, *VII*, 55–65.

Decreto 1008. (2018). *Ministerio de Tecnologias de la Informacion y las Comunicaciones.* 1–7.

Decreto 1078. (2015). Ministerio de Tecnologias de la Informacion y las Comunicaciones. *Mintic*, 172. https://www.mintic.gov.co/portal/604/w3-article-9528.html%0Ahttps://www.mintic.gov.co/portal/604/articles-9528_documento.pdf

Decreto 1151. (2008). Ministerio de Tecnologias de la Informacion y las Comunicaciones. *Esevictoria.Gov.Co*, *2003*(45), 1–10. http://www.esevictoria.gov.co/sitio2/mapaProcesos/procedGerencia/REHABILITACION/NORMATIVIDAD/NORMAS SALUD MENTAL/DECRETO 559.pdf%5Cnhttp://programa.gobiernoenlinea.gov.co/apc-aa-files/e5203d1f18ecfc98d25cb0816b455615/decreto1151abril14de2008_1.pdf%5Cnhttp

Decreto 2693. (2012). *Ministerio de Tecnologias de la Informacion y las Comunicaciones*.

Defensa.com. (2017). *Fuerza Aérea Colombiana se transforma para asumir nuevos retos-noticia defensa.com - Noticias Defensa defensa.com Colombia*.

Earth & Sky. (2016). *IT Governance and IT Management; What's the difference*. http://www.esfine.com/it-governance-it-management-definitioned/

FAC. (2011). *Haz de la estrategia* (Fuerza Aérea Colombiana (ed.)).

Fuerza Aérea Colombiana. (2019). *PLAN ESTRATÉGICO TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIONES 2019- 2022 FAC* (pp. 1–74).

Fuerza Aérea Colombiana. (2020). *3.1. Misión y Visión Fuerza Aérea Colombiana | Fuerza Aérea Colombiana*. 2020. https://www.fac.mil.co/transparencia-y-acceso-informacion-publica/3-estructura-organica-y-talento-humano/mision-vision

Furrer, O. (2010). Corporate level strategy: Theory and applications. In *Corporate Level Strategy: Theory and Applications* (pp. 1–250). https://doi.org/10.4324/9780203844526

Galeano M, M. E. (2003). *Diseño de proyectos en la investigación cualitativa* (U. Eafit (ed.)). https://books.google.com.co/books?id=Xkb78OSRMI8C&pg=PA36&dq=Técnicas+de+recolección&hl=es&sa=X&ved=0ahUKEwixi_bM69noAhXEmOAKHbQyDkUQ6AEIRDAD#v=onepage&q=Técnicas de recolección&f=false

Hernandez, R. (2014). *Metodologia de la investigacion* (6a ed.). Mc Graw Hill.

ICONTEC. (2009). COLOMBIANA NTC-ISO / IEC 38500. 571.

ISACA. (2012). *Implementación COBIT 5* (5th ed.).

IT Governance Institute. (2007). Marco de Trabajo Objetivos de Control Directrices Gerenciales Modelos de Madurez. *Cobit*, *4.1*, 211.

Ley 1341. (2009). *Congreso de la República de Colombia*.

Luka, B. (2019). *ISO 27001 – INFORMATION SYSTEMS SECURITY , DEVELOPMENT , TRENDS , TECHNICAL AND ECONOMIC CHALLENGES*. 45–49.

Marulanda Echeverry, C. E., López Trujillo, M., & Valencia Duque, F. J. (2017). Gobierno y gestión de ti en las entidades públicas. *AD-Minister*, *31*, 75–92. https://doi.org/10.17230/ad-minister.31.5

Ministerio de defensa. (2020). *Indicadores del Plan de Desarrollo - Ministerio de Defensa Nacional de la República de Colombia*. Indicadores Del Plan de Desarrollo. https://www.mindefensa.gov.co/irj/portal/Mindefensa/contenido/buscador?QueryString=presupuesto&SearchType=quick

Ministerio de Defensa. (2015). Política de Defensa y Seguridad. *Todos Por Un Nuevo País*, 1–37.

Ministerio de Defensa. (2020). *Ministerio de Defensa Nacional de la República de Colombia*. Ministerio de Defensa Nacional de La República de Colombia.

https://www.mindefensa.gov.co/irj/portal/Mindefensa

Ministerio de Defensa Nacional. Departamento Nacional de Planeacion. (2008). *Metodología para el calculo del gasto en defensa y seguridad*. 82.

MinTIC. (2018). *MANUAL DE GOBIERNO DIGITAL*. *5*.

MinTIC. (2019). Este documento está en construcción. In *Plan Estratégico Institucional MINTIC 2019 -2022* (pp. 1–76). https://www.mintic.gov.co/portal/604/articles-82084_plan_estrategico_institucional_mintic_2019_2022.pdf

Muñoz, I., & Ulloa, G. (2011). *Gobierno de TI – Estado del arte*.

OCDE. (2004). Principios de Gobierno Corporativo de la OCDE 2004. *Principios de Gobierno Corporativo de La OCDE 2004*, 1–41. https://doi.org/10.1787/9788485482726-es

Porter, M. E. (1990). *Competitive advantage of nations* (Vol. 3, Issue 2). http://repositorio.unan.edu.ni/2986/1/5624.pdf

Prieto, J. (2012). *Jorge Eliécer Prieto Herrera* (Ecoe Ediciones (ed.); Cuarta).

Pulso País. (2018). *2018*.

Rahimi, F., Møller, C., & Hvam, L. (2016). Business process management and IT management: The missing integration. *International Journal of Information Management*, *36*(1), 142–154. https://doi.org/10.1016/j.ijinfomgt.2015.10.004

Rodenes, A., & Bauset, M. C. (2009). *Gestion de los servicios de tecnologia de la información : modelo de aporte de valor basado en ITIL e ISO / IEC 20000*. 54–62.

Ruiz Olabuénaga, J. I. (2012). *Metodología de la investigación cualitativa* (Universidad de Deusto (ed.)). https://books.google.com.co/books?hl=es&lr=&id=WdaAt6ogAykC&oi=fnd&pg=PA9&dq=metodologia+de+la+investigacion&ots=sGv7bHA5MT&sig=AyPysHbdLjMRV9eLkNSKZ7a2FeM&redir_esc=y#v=onepage&q&f=false

Schiavo, E. (2007). *Investigación científica y tecnológica en el campo de las TIC-¿conocimientos técnicos, contextuales o transversales.pdf* (pp. 91–113).

Shin, N. (2007). Information technology and diversification: How their relationship affects firm performance. *Proceedings of the Annual Hawaii International Conference on System Sciences*, *October*. https://doi.org/10.1109/HICSS.2007.275

Stern, N. (2002). A Strategy for Development. In *A Strategy for Development*.

https://doi.org/10.1596/0-8213-4980-5

Verhoef, C. (2007). *Quantifying the effects of IT-governance rules*. *67*, 247–277. https://doi.org/10.1016/j.scico.2007.01.010

Vidal, E. (2004). *Libro_diagnostico_organizacional_elizabe.pdf* (ECOE Ediciones (ed.); 2nd ed.).

Webb, P., Pollard, C., & Ridley, G. (2006). Attempting to define IT governance: Wisdom or folly? *Proceedings of the Annual Hawaii International Conference on System Sciences*, *8*(September). https://doi.org/10.1109/HICSS.2006.68

Wolf, & Pilat. (2004). ICT production and ICT use: what role in aggregate productivity growth? *OECD*, *284*, 85–104. https://lib.unnes.ac.id/17153/1/1201408017.pdf

Anexos

Anexo A: Oportunidades de Mejora

Tabla 1: Oportunidades de Mejora

Proceso	Práctica Clave de Gobierno	Actividad
Gestionar el marco de gestión de TI	Gestión de la mejora continua de los procesos.	Identificar los procesos críticos de negocio basándose en el rendimiento, cumplimiento y los riesgos relacionados, evaluando la capacidad del proceso e identificar objetivos de mejora. Analizar las diferencias en la capacidad y control del proceso. Identificar las opciones de mejora y rediseño de procesos. Priorizar iniciativas para la mejora de procesos basados en el potencial coste – beneficio.
		Implementar las mejoras acordadas, funcionando como una práctica normal del negocio y establecer objetivos y métricas de rendimiento que permitan el seguimiento de las mejoras del proceso.
		Considerar las maneras de mejorar la eficiencia y eficacia.
		Aplicar prácticas de gestión de calidad para la actualización de procesos.
		Retirar procesos, componentes o catalizadores desactualizados.
	Mantener el cumplimiento con las políticas y procedimientos.	Hacer un seguimiento del cumplimiento con políticas y procedimientos.
		Analizar los incumplimientos y adoptar las acciones apropiadas.
		Integrar rendimiento y cumplimiento dentro de los objetivos individuales del personal.
		Evaluar periódicamente el desempeño de los catalizadores del marco de referencia y adoptar las acciones necesarias.
		Analizar las tendencias en el funcionamiento y cumplimiento y adoptar las acciones apropiadas.
Gestionar el portafolio	Supervisar, optimizar e informar sobre el rendimiento del portafolio de inversiones.	Revisar regularmente el portafolio para identificar y explotar sinergias, eliminar programas duplicados e identificar y mitigar el riesgo.
		Cuando sucedan cambios, volver a evaluar y a priorizar el portafolio para asegurar que está alineado con la estrategia del negocio y que la mezcla de inversión objetivo se mantiene, de modo que el portafolio esté optimizando el valor global. Esto puede requerir que los programas cambien, se aplacen, se retiren o bien que nuevos programas se inicien.

Elaboración propia

Tabla 1: Oportunidades de Mejora (Continuación)

Proceso	Práctica Clave de Gobierno	Actividad
Gestionar el portafolio	Supervisar, optimizar e informar sobre el rendimiento del portafolio de inversiones.	Ajustar los objetivos, previsiones, presupuestos y, si fuese necesario, el grado de monitorización empresarial para reflejar los gastos en que se incurriría y los beneficios de la empresa que se obtendrían gracias a los programas del portafolio de inversiones activas. Incorporar los gastos del programa en el mecanismo de prorrateo de costes.
		Aportar informes ejecutivos para la revisión por parte de la alta dirección de los progresos de la empresa hacia las metas identificadas, estableciendo que debe seguir siendo gastado y conseguido sobre qué franjas temporales.
		Incluir en la supervisión periódica del rendimiento, información sobre en qué medida los objetivos planificados han sido alcanzados, el riesgo mitigado, las capacidades creadas, los entregables obtenidos y las metas de rendimiento, conseguidas.
	Gestionar la consecución de beneficios.	Utilizar las métricas acordadas y realizar seguimiento sobre cómo los beneficios son obtenidos, cómo evolucionan a lo largo del ciclo de vida de programas y proyectos, cómo son entregados desde los servicios TI y cómo resultan al someterlos a un análisis comparativo interno y de la industria. Comunicar los resultados a las partes interesadas.
		Implementar acciones correctivas cuando los beneficios alcanzados se desvían significativamente de los esperados. Actualizar los casos de negocio para las nuevas iniciativas e implementar procesos de negocio y mejoras del servicio según se requiera.
		Considerar obtener orientación de expertos externos, líderes de la industria y datos de análisis comparativos para probar y mejorar las métricas y los objetivos.
Gestionar el presupuesto y los costes	Gestionar el presupuesto y los costes.	Establecer un órgano de toma de decisiones para priorizar recursos de TI y del negocio, incluyendo el uso de proveedores de servicio externos dentro de las asignaciones presupuestarias de alto nivel para programas habilitados por TI y activos de TI conforme a lo establecido por los planes estratégicos y tácticos. Considerar las opciones para la compra o desarrollo de activos y servicios capitalizados frente a la utilización de activos externos y de servicios sobre una base de pago por uso.

Elaboración propia

Tabla 1: Oportunidades de Mejora (Continuación)

Proceso	Práctica Clave de Gobierno	Actividad
Gestionar el presupuesto y los costes	Gestionar el presupuesto y los costes.	Posicionar todas las iniciativas de TI sobre la base de los casos de negocio y planes estratégicos y tácticos, y establecer procedimientos para determinar las asignaciones presupuestarias y cortes. Establecer un procedimiento para comunicar las decisiones presupuestarias y revisar con los responsables del presupuesto de las unidades de negocio.
		Identificar, comunicar y resolver los impactos más significativos de las decisiones presupuestarias en los casos de negocios, carteras y planes estratégicos.
		Obtener la ratificación del comité ejecutivo para los cambios generales en el presupuesto de TI que afecten negativamente a los planes estratégicos y tácticos de la entidad y ofrecer acciones sugeridas para resolver estos impactos.
Gestionar los acuerdos de servicio	Catalogar servicios basados en TI.	Publicar los servicios TI, paquetes de servicios y opciones de nivel del servicio activos de la cartera de servicios en los catálogos relevantes.
		Asegurar de forma continua que los componentes de servicio en el portafolio y en los catálogos de servicio relacionados, están completos y actualizados.
		Informar al gestor de relaciones del negocio de las actualizaciones en los catálogos de servicios.
Gestionar los proveedores	Identificar y evaluar las relaciones y contratos con proveedores.	Establecer y mantener criterios relativo al tipo, relevancia y criticidad de los contratos y proveedores, focalizándose en aquellos de mayor importancia.
		Establecer y mantener un criterio de evaluación de contratos y proveedores que permita una revisión general del rendimiento de los proveedores de manera consistente.
		Identificar, registrar y categorizar los proveedores y contratos existentes de acuerdo con el criterio definido, para mantener un registro detallado de los proveedores que deben ser gestionados cuidadosamente.
		Evaluar y comparar periódicamente el rendimiento de los proveedores actuales y alternativos para identificar oportunidades de mejora o la necesidad forzosa de reconsiderar los contratos con los proveedores actuales.

Elaboración propia

Tabla 1: Oportunidades de Mejora (Continuación)

Proceso	Práctica Clave de Gobierno	Actividad
Gestionar la calidad	Definir y gestionar los estándares, procesos y prácticas de calidad.	Definir las normas, procedimientos y prácticas de gestión de la calidad en consonancia con los requisitos del marco de control TI. Hacer uso de las mejores prácticas de la industria como referencia para la mejora y adaptación de los procesos de gestión de la calidad de la empresa.
		Considerar los costes y los beneficios de las certificaciones de calidad.
	Supervisar y hacer controles y revisiones de calidad.	Supervisar la calidad de los procesos y servicios de forma permanente y sistemática mediante la descripción, las métricas y los análisis; la mejora/Ingeniería y controles de los procesos.
		Preparar y llevar a cabo revisiones de calidad.
		Informar de los resultados de las revisiones y poner en marcha las mejoras necesarias.
		Supervisar la calidad de los procesos, así como el valor proporcionado por la calidad. Garantizar que la medición, supervisión y registro de la información es utilizada por los propietarios de los procesos para tomar las acciones correctivas y preventivas necesarias.
		Supervisar las métricas de calidad basadas en objetivos alineados con los objetivos generales de calidad y cubriendo la calidad de todos los servicios y los proyectos individuales.
		Garantizar que la dirección y los propietarios de los procesos, revisen periódicamente el rendimiento de la gestión respecto a las métricas de calidad definidas.
		Analizar los resultados del rendimiento de la gestión de la calidad global.
Gestionar el riesgo de TI	Recopilar Datos.	Registrar datos relevantes sobre el entorno de operación interno y externo de la empresa que pudieran jugar un papel significativo en la gestión del riesgo de TI.
		Medir y analizar los datos históricos de TI y de pérdidas experimentadas tomados de datos y tendencias externas disponibles, empresas similares de la industria - basados en eventos registrados, base de datos y acuerdos de la industria sobre divulgación de eventos comunes.
		Registrar datos sobre eventos de riesgo que han causado o pueden causar impactos al beneficio/valor facilitado por TI, a la entrega de programas y proyectos de TI y/o a las operaciones y entrega de servicio de TI. Capturar datos relevantes sobre asuntos relacionados, incidentes problemas e investigaciones.

Elaboración propia

Tabla 1: Oportunidades de Mejora (Continuación)

Proceso	Práctica Clave de Gobierno	Actividad
Gestionar el riesgo de TI	Recopilar Datos.	Para clases o eventos similares, organizar los datos recogidos y destacar factores contribuyentes. Determinar los factores contribuyentes comunes para eventos múltiples
		Determinar las condiciones específicas que existían o faltaban cuando ocurrieron los eventos de riesgo y la forma en la cual las condiciones afectaban la frecuencia del evento y la magnitud de la pérdida.
		Ejecutar análisis periódicos de eventos y de factores de riesgo para identificar asuntos nuevos o emergentes relacionados con el riesgo y para obtener un entendimiento de los asociados factores de riesgo internos y externos.
	Mantener un perfil del riesgo.	Inventariar los procesos de negocio, incluyendo el personal de soporte, aplicaciones, infraestructura, instalaciones, registros manuales críticos, vendedores, proveedores y externalizados y documentar la dependencia de los procesos de gestión de servicio TI y de los recursos de infraestructuras TI.
		Determinar y acordar qué servicios TI y recursos de infraestructuras de TI son esenciales para sostener la operación de procesos de negocio. Analizar dependencias e identificar eslabones débiles.
		Agregar escenarios de riesgo actuales, por categoría, línea de negocio y área funcional.
		De forma regular, capturar toda la información sobre el perfil de riesgo y consolidarla dentro de un perfil.
		Sobre la base de todos los datos del perfil de riesgo, definir un conjunto de indicadores de riesgo que permitan la identificación rápida y la supervisión del riesgo actual y las tendencias de riesgo.
		Capturar información sobre eventos de riesgo de TI que se han materializado, para su inclusión en el perfil de riesgo de TI de la empresa.
		Capturar información sobre el estado del plan de acción del riesgo, para la inclusión en el perfil.
	Expresar el riesgo.	Informar de los resultados del análisis de riesgos a todas las partes interesadas afectadas, en términos y formatos útiles para soportar las decisiones de empresa. Cuando sea posible, incluir probabilidades y rangos de pérdida o ganancia junto con niveles de confianza que permitan a la dirección equilibrar el retorno del riesgo.
		Proporcionar a los responsables de toma de decisiones un entendimiento de los escenarios peor y más probable, exposiciones de diligencia debida y consideraciones sobre la reputación, legales y regulatorias significativas.

Elaboración propia

Tabla 1: Oportunidades de Mejora (Continuación)

Proceso	Práctica Clave de Gobierno	Actividad
Gestionar el riesgo de TI	Expresar el riesgo.	Informar el perfil de riesgo actual a todas las partes interesadas, incluyendo la efectividad del proceso de gestión de riesgos, la efectividad de los controles, diferencias, inconsistencias, redundancias, estado de la remediación y sus impactos en el perfil de riesgo.
	Determinar un portafolio de acciones para la gestión de riesgos.	Mantener un inventario de actividades de control que estén en marcha para gestionar al riesgo y que permitan que el riesgo que se tome esté alineado con el apetito y tolerancia al riesgo. Clasificar las actividades de control y mapearlas con las declaraciones de riesgo específicas de TI y agrupaciones de riesgo de TI.
		Determinar si cada entidad organizativa supervisa el riesgo y acepta la responsabilidad para operar dentro de sus niveles de tolerancia individuales.
		Definir un conjunto de propuesta de proyecto equilibradas diseñadas para reducir el riesgo y/o proyectos que permiten oportunidades estratégicas empresariales, considerando costes/beneficios, el efecto en el perfil de riesgo actual y las regulaciones.
	Responder al riesgo.	Preparar, mantener y probar planes que documenten los pasos específicos a tomar, cuando un evento de riesgo pueda causar un incidente significativo operativo o evolucionar en un incidente con un impacto de negocio grave. Garantizar que los planes incluyan vías de escalado a través de la empresa.
		Categorizar los incidentes y comparar las exposiciones reales con los umbrales de tolerancia al riesgo. Comunicar los impactos en el negocio a los responsables de toma de decisiones como parte de la notificación y actualizar el perfil de riesgo.
		Aplicar el plan de respuesta apropiado para minimizar el impacto cuando ocurren incidentes.
		Examinar eventos adversos/pérdidas del pasado y oportunidades perdidas y determinar sus causas raíz. Comunicar la causa raíz y definir requerimientos adicionales para el riesgo y mejoras de proceso a los responsables de toma de decisiones apropiados y asegurarse de que la causa, los requerimientos de respuesta y la mejora del proceso se incluyan en los procesos de gobierno del riesgo.
Gestionar la seguridad de TI	Establecer y mantener un SGSI.	Definir un SGSI de acuerdo con la política de empresa, alineada con la empresa, la organización, su localización, activos y tecnología.
		Preparar y mantener una declaración de aplicabilidad que describa el alcance del SGSI.
		Definir y comunicar roles y responsabilidades de la gestión de la seguridad de la información.

Elaboración propia

Tabla 1: Oportunidades de Mejora (Continuación)

Proceso	Práctica Clave de Gobierno	Actividad
Gestionar la seguridad de TI	Supervisar y revisar el SGSI.	Realizar revisiones periódicas del SGSI incluyendo aspectos de políticas objetivos y prácticas de seguridad del SGSI. Considerar los resultados de auditorías de seguridad, incidentes, resultados de mediciones de efectividad, sugerencias y retroalimentación de todas las partes interesadas.
		Realizar auditorías internas al SGSI a intervalos planificados.
		Realizar revisiones periódicas del SGSI por la dirección para asegurar que el alcance sigue siendo adecuado y que se han identificado mejoras en el proceso del SGSI.
		Proporcionar información para el mantenimiento de los planes de seguridad para que consideren las incidencias de las actividades de supervisión y revisión periódica.
		Registrar las acciones y los eventos que podrían tener un impacto en la efectividad o el desempeño del SGSI.
Gestionar los programas y proyectos de TI	Mantener un enfoque estándar para la gestión de programas y proyectos.	Mantener y reforzar un enfoque estándar de la gestión de programas y proyectos alineado al entorno específico de la empresa y a las buenas prácticas basadas en procesos definidos y el uso de tecnología apropiada. Garantizar que el enfoque cubra todo el ciclo de vida y las disciplinas a utilizar, incluyendo la gestión de alcance, recursos, riesgos, costes, calidad, tiempo, comunicaciones, involucración de las partes interesadas, adquisiciones, control de cambios, integración y generación de beneficios.
		Actualizar el enfoque de gestión de programas y proyectos sobre la base de las lecciones aprendidas en su uso.
	Gestionar los recursos y los paquetes de trabajo del proyecto.	Identificar las necesidades de recursos del negocio y TI para el proyecto y mapear claramente los perfiles y responsabilidades, con los compromisos para el escalado y toma de decisiones que han sido acordadas y entendidas.
		Identificar los requerimientos de habilidades y tiempo para todos los individuos involucrados en las fases del proyecto con relación a sus perfiles definidos. Asignar personal a los roles basándose en la información sobre las habilidades disponibles.
		Utilizar un gestor de proyecto experimentado y un líder de equipo con habilidades apropiadas al tamaño, complejidad y riesgo del proyecto.
		Considerar y definir claramente los roles y responsabilidades de otras partes involucradas, incluyendo financiero, legal, compras, RRHH, auditoría interna y cumplimiento.

Elaboración propia

Tabla 1: Oportunidades de Mejora (Continuación)

Proceso	Práctica Clave de Gobierno	Actividad
Gestionar los programas y proyectos de TI	Gestionar los recursos y los paquetes de trabajo del proyecto.	Definir y acordar claramente la responsabilidad sobre la compra y gestión de productos y servicios de terceras partes, así como la gestión de las relaciones.
		Identificar y autorizar la ejecución del trabajo de acuerdo con el plan de proyecto.
		Identificar las diferencias con el plan de proyecto y dar realimentación al jefe de proyecto para su remediación.
	Cerrar un proyecto o iteración.	Definir y aplicar los pasos claves para el cierre del proyecto, incluyendo revisiones posteriores a la implementación que evalúen si el proyecto obtuvo los resultados y beneficios deseados.
		Planificar y ejecutar revisiones posteriores a la implementación para determinar si los proyectos entregaron los beneficios esperados y para la metodología de gestión de proyecto y el proceso de desarrollo de sistemas.
		Identificar, asignar, comunicar y rastrear las actividades incompletas, necesarias para lograr los resultados y beneficios planeados del programa del proyecto.
		Recolectar las lecciones aprendidas de los participantes del proyecto regularmente y hasta la finalización del proyecto. Revisar e identificar las actividades claves que llevaron a los beneficios y valor entregados - Analice los datos y haga recomendaciones para mejorar los proyectos actuales, así como el método de gestión para proyectos futuros.
		Obtenga la aceptación de los entregables y la transferencia de propiedad del proyecto de las partes interesadas. Práctica de Gestión Entradas Salidas.
	Cerrar un programa.	Llevar el programa a un cierre ordenado, incluyendo una aprobación formal, desmantelamiento de la organización del programa y la función de apoyo, validación de los entregables y comunicación de la retirada.
		Revisar y documentar las lecciones aprendidas. Una vez que el programa ha sido retirado, elimínelo del portafolio de inversiones activas.
		Establecer la responsabilidad y los procesos para asegurar que la organización continúe la optimización del valor de los servicios, activos o recursos. Pueden ser necesarias inversiones adicionales en el futuro para asegurarse que esto ocurra.

Elaboración propia

Tabla 1: Oportunidades de Mejora (Continuación)

Proceso	Práctica Clave de Gobierno	Actividad
Gestionar los Cambios	Evaluar, priorizar y autorizar peticiones de cambio.	Utilizar peticiones de cambio formales para posibilitar que los propietarios de procesos de negocio y soliciten cambios en procesos de negocio, infraestructura, sistemas o aplicaciones. Garantizar que todos estos cambios surgen solo a través del proceso de gestión de las peticiones de cambio.
		Categorizar todas las peticiones de cambio y relacionarlas con los elementos de configuración afectados.
		Priorizar todas las peticiones de cambio sobre la base de los requisitos técnicos y de negocio, recursos necesarios, así como las razones contractuales, legales o de regulación que motivan el cambio.
		Planificar y evaluar todas las peticiones de una manera estructurada. Incluir un análisis de impacto sobre los procesos de negocio, infraestructura, sistemas y aplicaciones, planes de continuidad de negocio y proveedores de servicios, para asegurar que todos los componentes afectados han sido debidamente identificados.
		Aprobar formalmente cada cambio por parte de los propietarios de los procesos de negocio, gestores de servicio y partes interesadas.
		Planificar y programar todos los cambios aprobados.
		Considerar el impacto en los proveedores de servicios contratados en el proceso de gestión del cambio, incluyendo la integración de la gestión de cambios organizativos con los procesos de gestión de cambios de los proveedores de servicios y el impacto en términos contractuales y ANS.
	Gestionar cambios de emergencia.	Garantizar que hay un procedimiento documentado para declarar, evaluar, aprobar de formar preliminar y autorizar una vez hecho el cambio y registrar el cambio de emergencia.
		Verificar que los accesos de emergencia acordados para realizar los cambios, están debidamente autorizados y documentos y son revocados una vez se han aplicado los cambios.
		Supervisar todos los cambios de emergencia y realizar revisiones posteriores a la implementación, involucrando a todas las partes interesadas. Considerar e iniciar acciones correctivas basadas en causas raíz, tales como problemas en los procesos de negocio, desarrollo y mantenimiento de sistemas de aplicación, entornos de desarrollo y pruebas, documentación y manuales e integridad de datos.

Elaboración propia

Tabla 1: Oportunidades de Mejora (Continuación)

Proceso	Práctica Clave de Gobierno	Actividad
Gestionar los Cambios	Hacer seguimiento de cambios de estado.	Categorizar las peticiones de cambio en el proceso de seguimiento.
		Elaborar informes de cambios de estado que incluyan métricas de rendimiento para facilitar la revisión y el seguimiento de la dirección del detalle del estado de los cambios y del estado global.
		Supervisar los cambios abiertos para asegurar que los cambios aprobados son cerrados en los plazos previstos, de acuerdo con su prioridad.
		Mantener un sistema de seguimiento e informe para todas las peticiones de cambio.
	Cerrar y documentar los cambios.	Incluir los cambios en la documentación en el procedimiento de gestión del cambio como parte integral del cambio.
		Definir un periodo apropiado de conservación de la documentación del cambio, la documentación del sistema antes y después del cambio y la documentación de usuario.
		Someter a la documentación a la misma revisión que al cambio en sí mismo.
Gestionar el conocimiento	Cultivar y facilitar una cultura de intercambio de conocimientos.	Comunicar proactivamente el valor del conocimiento para impulsar la creación, uso, reutilización y compartición de conocimiento.
		Impulsar la compartición y transferencia de conocimiento mediante la identificación de factores que influyan en la motivación.
		Crear un entorno, herramientas y elementos que den soporte a la compartición y transferencia de conocimientos.
		Integrar prácticas de gestión del conocimiento en otros procesos de TI.
		Establecer expectativas de la dirección y demostrar la actitud adecuada acerca de la utilidad del conocimiento y la necesidad de compartir el conocimiento corporativo.
	Identificar y clasificar las fuentes de información.	Identificar usuarios potenciales de conocimiento, incluyendo propietarios de información que pueden necesitar contribuir y aprobar conocimiento. Obtener requisitos de conocimiento y fuentes de información de los usuarios identificados.
		Clasificar las fuentes de información basándose en un esquema de clasificación de contenido (ej. modelo de arquitectura de información). Trazar un mapa de fuentes de información con el esquema de clasificación.

Elaboración propia

Tabla 1: Oportunidades de Mejora (Continuación)

Proceso	Práctica Clave de Gobierno	Actividad
Gestionar el conocimiento	Organizar y contextualizar la información, transformadora en conocimiento.	Identificar atributos compartidos y casar fuentes de información, creando relaciones entre conjuntos de información.
		Crear vistas para conjuntos de datos relacionados, considerando requisitos organizativos y de las partes interesadas.
		Concebir e implantar un esquema para gestionar la información no estructurada que no esté disponible a partir de fuentes formales.
		Publicar y hacer accesible el conocimiento a las partes interesadas relevantes, basándose en roles y mecanismos de acceso.
	Utilizar y compartir el conocimiento.	Identificar usuarios potenciales de conocimiento mediante la clasificación de la información.
		Transferir el conocimiento a los usuarios de conocimientos, basándose en un análisis de necesidades técnicas de aprendizaje efectivas y herramientas de acceso.
		Educar y entrenar a los usuarios en el conocimiento disponible, en el acceso al conocimiento y en el uso de herramientas de acceso al conocimiento.
	Evaluar y retirar la información.	Medir el uso y evaluar la utilidad, relevancia y valor de los elementos de conocimiento. Identificar información relacionada que ya no es relevante para cubrir las necesidades de conocimiento de la organización.
		Definir las reglas para la retirada de conocimiento y retirar el mismo de forma acorde.
Gestionar los Activos	Administrar licencias.	Mantener un registro de todas las licencias de software adquiridas y sus acuerdos de licencia asociados.
		De forma regular llevar a cabo una auditoria, para identificar todas las copias de software instalado con licencia.
		Comparar el número de copias de software instalado con el número de licencias en propiedad.
		Cuando las copias sean inferiores al número en propiedad, decidir si existe una necesidad de mantener o cancelar licencias, considerando el potencial.
		Ahorrar en mantenimiento innecesario, información y otros gastos.
		Cuando las copias sean superiores al número en propiedad, considerar primero la posibilidad de desinstalar copias que no sean ya necesarias o no estén justificadas, y después, si es necesario, adquirir licencias adicionales para cumplir con los acuerdos de licencia.

Elaboración propia

Tabla 1: Oportunidades de Mejora (Continuación)

Proceso	Práctica Clave de Gobierno	Actividad
Gestionar la continuidad de TI	Desarrollar e implementar una respuesta a la continuidad del negocio.	Definir las acciones y comunicaciones de respuesta a incidentes que deben ser realizadas en un evento de disrupción. Definir los roles y responsabilidades relacionados, incluyendo la responsabilidad para la política y la implementación.
		Desarrollar y mantener planes de continuidad de negocios operativos que contengan los procedimientos que deben ser seguidos, para permitir continuar operando los procesos críticos de negocio y planes temporales de proceso, incluyendo enlaces a los planes de proveedores de servicio externalizado
		Se debe asegurar que los proveedores y socios externos clave, tengan implantados planes de continuidad efectivos. Obtener evidencias auditadas si es necesario.
		Definir las condiciones y procedimientos de recuperación que permitan la reanudación de los procesos de negocio, incluyendo la actualización y conciliación de las bases de datos para preservar la integridad de la información.
		Definir y documentar los recursos necesarios para soportar los procedimientos de continuidad y recuperación, considerando personas, instalaciones e infraestructura de TI.
		Definir y documentar los requerimientos de información de respaldo para soportar los planes, incluyendo planes y documentos en papel, así como ficheros de datos y considerar las necesidades de seguridad y almacenamiento en otra ubicación.
		Determinar las habilidades necesarias para los individuos implicados en las ejecuciones de los planes y procedimientos.
		Distribuir los planes y la documentación de soporte de modo seguro a las partes interesadas y apropiadamente autorizadas y asegurar que estén accesibles en escenarios de desastre.
	Revisar, mantener y mejorar el plan de continuidad.	Revisar el plan y la capacidad de continuidad de forma regular frente a las asunciones hechas y los objetivos de negocio actuales, tanto estratégicos como operativos.
		Considerar si es necesario una revisión del análisis de impacto en el negocio, dependiendo en la naturaleza de los cambios.
		Recomendar y comunicar los cambios en la política, planes, procedimientos, infraestructura, roles y responsabilidades para la aprobación de la dirección y su realización mediante el proceso de gestión.;

Elaboración propia

Tabla 1: Oportunidades de Mejora (Continuación)

Proceso	Práctica Clave de Gobierno	Actividad
Gestionar la continuidad de TI	Proporcionar formación en el plan de continuidad.	Definir y mantener los planes y requerimientos de formación para quienes realicen de manera continua la planificación de la continuidad, análisis de impacto, evaluaciones de riesgos, comunicación con los medios y respuesta a incidentes. Hay que asegurar que los planes de formación consideren la frecuencia de formación y los mecanismos de entrega de la formación.
		Desarrollar competencias basadas en formación práctica que incluyan la participación en ejercicios y pruebas.
		Supervisar las habilidades y competencias basándose en los resultados de los ejercicios y las pruebas.
	Gestionar acuerdos de respaldo.	Hacer copias de seguridad de sistemas, aplicaciones, datos y documentación de acuerdo con una planificación definida, considerando: Frecuencia, Modos de copia de seguridad, Tipos de copia de seguridad, Tipo de soporte, Tipos de datos, Creación de registros, Localización física y lógica de la fuente de datos, Seguridad y derechos de acceso, Cifrado.
		Hay que asegurar que los sistemas, aplicaciones, datos y documentación mantenidos o procesados por terceras partes, están adecuadamente respaldados o asegurados, de otra forma, considerar el hecho de requerir el retorno de las copias de seguridad de terceras partes; considerar acuerdos de depósito.
		Definir los requerimientos del almacenamiento de las copias de seguridad, dentro y fuera de la propia ubicación, que satisfagan los requerimientos del negocio. Considerar la accesibilidad requerida a las copias de seguridad.
		Extender la concienciación y la formación en planes de continuidad de negocio.
		Probar y mantener legibles las copias de seguridad y las archivadas periódicamente.

Elaboración propia

Anexo B: Cuestionario de Validación

1. Seleccione **los lineamientos** que usted considera que están acordes con la estrategia de la Jefatura de las Tecnologías de la Información y las Comunicaciones de la Fuerza Aérea Colombiana:

   - Direccionamiento Estratégico de TI.
   - Calidad en los servicios de TI.
   - Alineamiento Estratégico.
   - Gestión de TI soportada en buenas prácticas.
   - Cumplimiento de los acuerdos de servicio.
   - Gestión de los activos de TI.
   - Seguridad de la información.
   - Talento humano cualificado.
   - Catálogo de servicios de TI.
   - Evaluación del desempeño de la gestión de TI.

2. Seleccione los requerimientos que usted considera que deben ser incluidos en el diseño de un modelo de gobierno de TI para la Jefatura de las Tecnologías de la Información y las Comunicaciones de la Fuerza Aérea Colombiana:

   - Proceso de gestión de TI.
   - Definición de una política de TI alineada con la misión.
   - Estructura organizacional del área de TI.
   - Gestión del Portafolio.
   - Instancias de decisión de TI.
   - Cumplimiento con los requerimientos de usuario.
   - Relaciones con proveedores.
   - Administración de la calidad.
   - Gestión de Riesgos.

- Seguridad de los sistemas.
- Gestionar los Programas y Proyectos.
- Gestión de cambios.
- Gestionar el Conocimiento.
- Gestionar los Activos.
- Continuidad del negocio.

3. ¿Considera usted que existe una correlación de los elementos (personas, procesos, tecnología, servicios y datos) TI y los requerimientos definidos en el resumen ejecutivo?

   - SI
   - NO

4. ¿Considera usted que los requerimientos listados son suficientes para el diseño del modelo de gobierno de TI?

   - SI
   - NO

5. Considera usted que el modelo de gobierno de TI es adecuado para las necesidades de la Jefatura de las Tecnologías de la Información y las Comunicaciones de la Fuerza Aérea Colombiana:

   - SI
   - NO

6. ¿Considera usted que la estructura del modelo de gobierno es adecuada?
   - SI
   - NO

7. ¿Considera usted que el modelo de gobierno de TI propuesto involucra las estructuras, procedimientos y políticas de la Jefatura de las Tecnologías de la Información y las Comunicaciones de la Fuerza Aérea Colombiana?

   - SI
   - NO

8. ¿Considera usted que la estructura que tiene el modelo de TI propuesto puede ser escalable para incorporar futuros requerimientos?
   - SI
   - NO

9. ¿Considera que las fases descritas en el plan de implementación están acordes para realizar la implementación del modelo?

   - SI
   - NO

10. ¿Considera usted que el modelo de gobierno de TI cumple con los lineamientos de la política de gobierno digital para entidades públicas?
    - SI
    - NO

11. Teniendo en cuenta que el objetivo del cuestionario es validar los lineamientos, los requerimientos, el modelo de gobierno y el plan de acción, por favor indique qué elementos adicionales deberían ser incluidos.

Anexo C: Resultados del nivel de capacidad actual de los procesos COBIT en JETIC

Tabla 2: Resultados del nivel de capacidad actual de los procesos COBIT en JETIC

Proceso COBIT 5.0	Práctica Clave de Gobierno	Nivel Actual
APO01 Gestionar el Marco de Gestión de TI	APO01.01: Definir la estructura organizativa.	3,37
	APO01.02: Establecer roles y responsabilidades.	3,99
	APO01.03: Mantener los elementos catalizadores del sistema de gestión.	3,52
	APO01.04 Comunicar los objetivos y la dirección de gestión	2,36
	APO01.05: Optimizar la ubicación de la función de TI.	3,40
	APO01.06: Definir la propiedad de la información (datos) y del sistema.	3,95
	AP001.07: Gestionar la mejora continua de los procesos	2,91
	APO01.08: Mantener el cumplimiento con las políticas y procedimientos.	3,06
APO05 Gestionar el Portafolio	APO05.01: Establecer la mezcla del objetivo de inversión.	3,53
	APO05.02: Determinar la disponibilidad y las fuentes de fondos.	4,39
	APO05.03: Evaluar y seleccionar los programas a financiar.	3,32
	APO05.04: Supervisar, optimizar e informar sobre el rendimiento del portafolio de inversiones.	2,96
	APO05.05: Mantener los portafolios.	4,39
	APO05.06: Gestionar la consecución de beneficios.	2,98
APO06 Gestionar el Presupuesto y los Costes	APO06.01: Gestionar las finanzas y la contabilidad.	4,44
	APO06.02: Priorizar la asignación de recursos.	2,89
	APO06.03: Crear y mantener presupuestos.	4,24
	APO06.04: Modelar y asignar costes.	4,49
	APO06.05: Gestionar Costes	4,48
APO09 Gestionar los Acuerdos de Servicio	APO09.01: Identificar servicios TI	3,15
	APO09.02: Catalogar servicios basados en TI	2,48
	APO09.03: Definir y preparar acuerdos de servicio.	3,01
	APO09.04: Supervisar e informar de los niveles de servicio.	3,01
	APO09.05: Revisar acuerdos de servicio y contratos.	2,64
APO10 Gestionar los Proveedores	APO10.01: Identificar y evaluar las relaciones y contratos con proveedores.	3,91
	APO10.02: Seleccionar proveedores.	4,53
	APO10.03: Gestionar contratos y relaciones con proveedores	4,46
	APO10.04: Gestionar el riesgo en el suministro	4,04
	APO10.05: Supervisar el cumplimiento y el rendimiento del proveedor.	4,48
APO11 Gestionar la Calidad	APO011.01: Establecer un sistema de gestión de la calidad	3,42
	APO11.02: Definir y gestionar los estándares, procesos y prácticas de calidad.	2,54
	APO11.03: Enfocar la gestión de la calidad en los clientes.	3,89
	APO11.04 Supervisar y hacer controles y revisiones de calidad.	2,51
	APO11.05: Integrar la gestión de la calidad en la implementación de soluciones y la entrega de servicios.	4,12
	APO11.06: Mantener una mejora continua	4,18

Elaboración propia

Tabla 2: Resultados del nivel de capacidad actual de los procesos COBIT en JETIC (Continuación)

Proceso COBIT 5.0	Práctica Clave de Gobierno	Nivel Actual
APO12 Gestionar el Riesgo	APO12.01: Recopilar datos	2,91
	APO12.02: Analizar el riesgo	4,07
	APO12.03: Mantener un perfil del riesgo	2,90
	APO12.04: Expresar el riesgo	3,99
	APO12.05: Definir un portafolio de acciones para la gestión de riesgos.	2,24
	APO12.06: Responder al riesgo.	2,11
APO13 Gestionar la Seguridad	APO13.01: Establecer y mantener un SGSI	3,56
	APO13.02: Definir y gestionar un plan de tratamiento del riesgo de la seguridad de la información.	4,14
	APO13.03: Supervisar y revisar el SGSI.	3,47
BAI01 Gestionar los Programas y Proyectos	BAI01.01: Mantener un enfoque estándar para la gestión de programas y proyectos	2,46
	BAI01.02: Iniciar un programa	3,21
	BAI01.03: Gestionar el compromiso de las partes interesadas.	3,96
	BAI01.04: Desarrollar y mantener el plan de programa	3,46
	BAI01.05: Lanzar y ejecutar el programa.	3,99
	BAI01.06: Supervisar, controlar e informar de los resultados del programa.	3,58
	BAI01.07: Lanzar e iniciar proyector dentro de un programa.	4,55
	BAI01.08: Planificar proyectos.	3,05
	BAI01.09: Gestionar la calidad de los programas y proyectos.	3,04
	BAI01.010: Gestionar el riesgo de los programas y proyectos.	3,10
	BAI01.011: Supervisar y controlar proyectos.	4,01
	BAI01.012: Gestionar los recursos y los paquetes de trabajo del proyecto.	2,87
	BAI01.013: Cerrar un proyecto o iteración.	2,44
	BAI01.014: Cerrar un programa.	2,45
BAI06 Gestionar los Cambios	BAI06.01: Evaluar, priorizar y autorizar peticiones de cambio.	2,54
	BAI06.02: Gestionar cambios de emergencia.	1,50
	BAI06.03: Hacer seguimiento de cambios de estado.	2,11
	BAI06.04: Cerrar y documentar los cambios.	2,17
BAI08 Gestionar el Conocimiento	BAI08.01: Cultivar y facilitar una cultura de intercambio de conocimientos.	2,07
	BAI08.02: Identificar y clasificar las fuentes de información.	2,89
	BAI08.03: Organizar y contextualizar la información, transformadora en conocimiento.	2,98
	BAI08.04: Utilizar y compartir el conocimiento.	2,86
	BAI08.05: Evaluar y retirar la información.	2,61
BAI09 Gestionar los Activos	BAI09.01: Identificar y registrar activos actuales.	4,51
	BAI09.02: Gestionar activos críticos	4,44
	BAI09.03: Gestionar el ciclo de vida de los activos	4,52
	BAI09.04: Optimizar el coste de los activos.	4,00
	BAI09.05: Administrar licencias.	3,11

Elaboración propia

Tabla 2: Resultados del nivel de capacidad actual de los procesos COBIT en JETIC (Continuación)

Proceso COBIT 5.0	Práctica Clave de Gobierno	Nivel Actual
DSS04 Gestionar la Continuidad	DSS04.01: Definir la política de continuidad del negocio, objetivos y alcance.	4,57
	DSS04.02: Mantener una estrategia de continuidad.	4,58
	DSS04.03: Desarrollar e implementar una respuesta a la continuidad del negocio.	3,13
	DSS04.04: Ejercitar, probar y revisar el plan de continuidad.	4,60
	DSS04.05: Revisar, mantener y mejorar el plan de continuidad.	3,02
	DSS04.06: Proporcionar formación en el plan de continuidad.	3,24
	DSS04.07: Gestionar acuerdos de respaldo.	1,90
	DSS04.08: Ejecutar revisiones posteriores a la reanudación.	4,63

Elaboración propia