RESUMEN – TRABAJO DE GRADO

AUTORES	Erney Alberto Ramirez Camargo.
FACULTAD	**FACULTAD DE INGENIERIAS**
PLAN DE ESTUDIOS	**MAESTRIA EN GOBIERNO DE TI.**
DIRECTOR	Albeiro Alonso Rosado Gómez.
TÍTULO DE LA TESIS	Diseño del modelo de Gobierno de TI, dirigido a las Alcaldías de sexta categoría del sur del Departamento del Cesar, para la gestión de riesgos de la seguridad de la información.
TITULO EN INGLES	Design of the IT Governance model, aimed at the sixth-category Mayors' Offices in the south of the Department of Cesar, for information security risk management.

RESUMEN
(70 palabras)

Mediante la caracterización de la problemática actual, presente en las administraciones municipales de la región del sur del departamento del Cesar se procura plantear un modelo de gobierno de tecnologías de la información cuyo objetivo es dinamizar los procesos de TI del municipio de sexta categoría, cuya meta principal es el de armonizar los objetivos de la empresa con las tecnologías de la información.

RESUMEN EN INGLES

Through the characterization of the current problems, present in the municipal administrations of the southern region of the department of Cesar, an attempt is made to propose an information technology governance model whose objective is to streamline the IT processes of the sixth category municipalities, whose The main goal is to harmonize the company's objectives with information technologies, thus providing quality services, agile processes and linking regulations in information security risk management.

PALABRAS CLAVES	Gobierno de TI, Seguridad de la Información, Gestión de Riesgos, Gobierno Digital, IT4+, Políticas públicas.
PALABRAS CLAVES EN INGLES	IT Governance, Information Security, Risk Management, Digital Government, IT4+, Public Policies.

CARACTERÍSTICAS

PÁGINAS: 145	PLANOS:	ILUSTRACIONES:	CD-ROM:

Diseño del modelo de gobierno de TI, dirigido a las alcaldías de sexta categoría del sur del departamento del cesar, para la gestión de riesgos de la seguridad de la información.

Erney Alberto Ramirez Camargo.

Facultad de Ingenierías, Universidad Francisco de Paula Santander Ocaña.

Maestría en Gobierno de TI.

Msc. Alveiro Alonso Rosado Gómez.

25 enero de 2022.

Tabla de contenido

Lista de tablas

Lista de Figuras

Introducción

Las instituciones públicas tienen la obligación constitucional de proteger la información que se maneja de los ciudadanos, ya sean funcionarios públicos que contribuyen con el desarrollo del objetivo de la entidad pública o el usuario que llega a depositar sus datos personales en busca de acceso a la justicia o al gobierno en general, dado que existe peligro de difusión o mala utilización de los datos

La información es el activo más importante dentro de una empresa, la seguridad de la información está compuesta por un conjunto de normas, procedimientos y herramientas, que tienen como objetivo garantizar las características principales de la misma como lo son: la disponibilidad, integridad, confidencialidad[1], autenticidad, trazabilidad y no repudio, en un sistema de información; implementar políticas de seguridad de los datos se ha convertido en una necesidad para que las organizaciones salvaguarden su información de cualquier tipo de ataque, daño o perdida de la misma.

Las entidades del orden público en la república de Colombia deben tener altos niveles de protección en el tratamiento de datos, desde la exigibilidad de la normatividad, toda vez que la posibilidad de vulneración de derechos fundamentales y en general de toda la gama de derechos que emergen de la constitución y del bloque de constitucionalidad.

En la actualidad existen normas que garantizan el uso adecuado que se le debe dar a la información, los cuales acreditan a las Organizaciones en cuanto al manejo de la misma, ISO 27001 es un estándar en el que se encuentran enmarcados una serie de procedimientos, que establece las pautas para la implementación de los Sistemas de Gestión de Seguridad de la Información SGSI) dentro una Organización y para el tratamiento del riesgo existe metodologías para gestionarlo entre ellos cabe mencionar ISO 27005, MAGERIT, OCTAVE , entre otras.

Para diseñar el modelo de gobierno de TI dirigido a las alcaldías de sexta categoría[2] del sur del departamento del cesar, para la gestión de riesgos de la

[1] https://mintic.gov.co/gestionti/615/articles-5482_G5_Gestion_Clasificacion.pdf

[2] La ley 1551 de 2012, por la cual se dictan normas para modernizar la organización y el funcionamiento de los municipios, establece que los distritos y municipios se clasificarán atendiendo su población, ingresos corrientes de libre destinación, importancia económica y situación geográfica. Para efectos de lo previsto en la ley y las demás normas que expresamente lo dispongan, los de sexta categoría serán aquellos que su población es igual o inferior a diez mil (10.000) pobladores, sus ingresos corrientes de libre destinación anuales: No superiores a quince mil (15.000) salarios mínimos legales mensuales. Importancia Económica grado siete.

seguridad de la información, ISO 27005, en su versión más reciente lanzada en el año 2018, enmarca lo lineamientos sobre cómo sortear estas exigencias al mismo tiempo que proporciona un marco de trabajo para gestionar de forma efectiva los riesgos relacionados con la seguridad de la información. Para ello se pretende establecer el diagnostico de vulnerabilidades de las alcaldías de sexta categoría del sur del departamento del cesar, mediante una metodología de análisis de riesgo en donde se evidencie vulnerabilidades a las que puede estar expuesta actualmente, diseño del modelo de gobierno de TI dirigido a las alcaldías de sexta categoría del sur del departamento del cesar, para la gestión de riesgos de la seguridad de la información.

Lo que les permitiría a las alcaldías de sexta categoría del sur del departamento del cesar, identificar claramente sus activos, amenazas y riesgos que se deben salvaguardar para poder en un mediano plazo aspirar a la implementación del SGSI, en miras a lo que establece el gobierno nacional con las estrategias de Gobierno en Línea (GEL) e IT4+[3].

Adicional obtener la certificación y desarrollar una imagen favorable ante la ciudadanía y en general ante el público en general, conlleva a elevar los estándares de calidad, pero fundamentalmente a tener tranquilidad en los procesos y en futuras eventualidad.

Título

Diseño del modelo de gobierno de TI dirigido a las alcaldías de sexta categoría del sur del departamento del cesar, para la gestión de riesgos de la seguridad de la información.

1. Planteamiento del problema

Los municipios de Colombia se clasifican de acuerdo a su población, ingresos corrientes de libre destinación y situación geográfica, tal como lo establece el decreto 2106 de 2019 (SUIN, 2019), específicamente en su artículo 153; definiendo además tres grupos, así: Grandes municipios, municipios intermedios y municipios básicos; en este último grupo se tienen los de quinta y sexta categoría. Siendo la sexta categoría la última en clasificación de los municipios, es importante aclarar cuáles son sus características, respecto a la población tienen diez mil (10.000) o menos habitantes y en relación a sus ingresos corrientes de libre destinación anuales, éstos no son superiores a quince mil (15.000) salarios mínimos legales mensuales vigentes, equivalentes para la vigencia 2021 a trece mil millones seiscientos veintisiete mil ochocientos noventa pesos corrientes ($13.627.890.000 MCT) (Contaduría General Nación, 2021).

De los 25 municipios que el departamento del Cesar posee, son ocho los localizados en la Subregión Sur (Aguachica, Gamarra, González, La Gloria, Pelaya, Río de Oro, San Alberto, San Martín) y de estos seis se encuentran en sexta categoría. A pesar que estos municipios presentan menos ingresos para cubrir sus obligaciones legales y satisfacer las necesidades de sus comunidades, a sus alcaldías le son atribuibles iguales retos en su desempeño institucional; entre las cuales se encuentran las funciones y actividades de las Tecnologías de la Información (TI). En los tiempos actuales, es decir, en toda la era de desarrollo de las ciencias computacionales el activo vital más importante de cualquier organización es la información, debido al gran auge que ha tenido las áreas relacionadas, las tecnologías de información en la actualidad cumple un rol cada vez más importante en cualquier organización tanto del sector público o privado alrededor del mundo (Marulanda C, ECHEVERRY, 2017), es por ello que la automatización de la información para las organización, ha venido creciendo exponencialmente en las últimas décadas, lo cual ha provocado que las mismas sean cada vez más eficientes y productivas (Baena., 2015).

Según el artículo de colaboración de la universidad nacional mayor de San Marcos de Lima Perú, escrito por Juan Díaz y David Mauricio, 2019 se han identificado cinco factores que inhiben la implementación del Gobierno de las TI; la falta de comunicación, el inadecuado involucramiento de los interesados, la falta de principios y políticas claros de Gobierno de TI, la

falta de procesos, e inadecuado soporte de recursos financieros.

Los riesgos tecnológicos que pueden inferir en el desarrollo de una entidad suponen sean más altos en municipios de sexta categoría, en donde los recursos financieros son limitados para invertir en campos como la ciencia y tecnología, como lo destaca José Miguel Roca, 2021 Uno de los aspectos de las tecnologías de la información que más importancia tiene en la actualidad es el de la seguridad, puesto que se ha hecho necesario la búsqueda de mecanismos que puedan evitar accesos indeseados a los centros de datos, a los ordenadores y a los programas e información contenidos en ellos, que se vienen haciendo más propensos a interferencias por el fácil acceso a las redes y a todos los sistemas que impliquen el uso de internet (Roca Chillida, 2019).

Actualmente la Función Pública mide el desempeño Institucional de los municipios de Colombia a través de un Modelo Integrado de Gestión y Desempeño, éste compuesto por 7 dimensiones y 18 políticas, entre las cuales se encuentran las de Gobierno Digital y Seguridad Digital, en las cuales se desarrollas acciones de fortalecimiento de las TIC's; para la gestión de la vigencia 2020, en la información publicada por la Función Pública se encuentra que de los seis municipio que conforman la subregión sur del departamento del Cesar y que se encuentran en sexta categoría se tienen los siguientes resultados (Función Pública, 2020):

Tabla 1. Medición de políticas de Gobierno de Seguridad Digital de la vigencia

Municipio	**Gobierno Digital**	**Seguridad Digital**
Gamarra	40,8	60,7
González	61,4	49,1
La Gloria	72,6	66,6
Pelaya	66,7	71
Río de Oro	37,9	32,5
SAN ALBERTO	58,9	64,4

Fuente: Función pública (2021)

Estos resultados evidencian la baja capacidad de los municipios de sexta categoría localizados en el sur del departamento del Cesar de avanzar en su estructura de TI y en los mecanismos de Seguridad Digital. Los departamentos de TI de las Alcaldías del Departamento del Cesar generalmente tienen problemas en sus operaciones diarias; esto se debe a múltiples factores, entre los cuales se encuentra el desconocimiento de políticas y normas de Seguridad de la Información y de los riesgos de TI (Arévalo Ascanio, 2016).

Por tanto, estos municipios, no están alineados a los parámetros que instaura el Gobierno Nacional, donde se establece por parte del Ministerio de Tecnologías de la Información y las Comunicaciones - Min TIC a través de la Dirección de Estándares y Arquitectura de TI y la Subdirección de Seguridad y Privacidad de TI, parámetros para dar cumplimiento a sus funciones públicas, como es El Modelo de Seguridad y Privacidad de la Información (MSPI), el cual se encuentra alineado con el Marco de Referencia de Arquitectura TI y soporta transversalmente los otros componentes de la Estrategia GEL: TIC para Servicios, TIC para Gobierno Abierto y TIC para Gestión (Mintic, 2014).

Desde el Ministerio TIC, se ha ofrecido a los municipios del país un modelo con el cual se pretende que se mejoren los servicios que se prestan a los habitantes de los territorios, desde el mejoramiento de los mecanismos de comunicación, de la gestión de la información interna y externa, hasta el control de los recursos de las entidades. Este modelo es conocido como el Modelo de Gestión IT4+, creado en el año 2014 y que a la fecha no ha logrado tener el efecto esperado en los municipios de sexta categoría (Mintic , 2020).

A pesar que existen diversos conjuntos de marcos de referencia y metodologías para trabajar en la seguridad de la información y gestión de riesgos de TI, que se irán desarrollando a lo largo del texto, no se ha logrado proveer a los municipios de sexta categoría de una guía, de un método o modelo que se ajuste a las fortalezas y debilidades con que deben accionar este tipo de municipios frente a los diversos riesgos informáticos y tecnológicos que amenazan su gestión. Por tanto, se considera que la presente investigación reviste importancia y brinda un aporte a la región al diseñar un modelo de Gobierno TI dirigido a los municipios en mención.

1.1 Formulación del problema:

¿Qué elementos deben considerarse para el diseño de un modelo de gobierno TI enfocado en las alcaldías se sexta categoría del Sur del Departamento del Cesar, de modo tal que contribuya a la gestión de riesgos de la seguridad de la información?

2. Objetivos

2.1 Objetivo General:

Diseñar el modelo de gobierno de TI, dirigido a las alcaldías de sexta categoría del sur del departamento del Cesar para la gestión de riesgos de la seguridad de la información.

2.2 Objetivos específicos

- Realizar un diagnóstico sobre la situación actual de los municipios de sexta categoría del sur del Departamento del Cesar.
- Analizar los componentes del modelo gobierno TI con base en los requerimientos normativos.
- Proponer una guía para el gobierno TI orientada a los municipios de sexta categoría del sur del Departamento del Cesar.
- Definir un mecanismo de seguimiento y control al modelo de gobierno TI para los municipios de sexta del sur del Departamento del Cesar.

3. Justificación

La tecnología llegó para cambiar los modelos de negocio y mejorar la calidad de vida de las personas, al ofrecer herramientas que facilitan las tareas y que también propician la comunicación, por tanto, se considera un generador de desarrollo constante, donde día a día se muestran las innovaciones tecnológicas que contribuyen al fortalecimiento de los procesos en las organizaciones. Por tanto, el reto que tiene cada institución se fundamenta en el deber de estructurar la gestión de tecnología, teniendo dentro de sus principales objetivos el aprovechamiento de la misma para generar ventajas sustentables que le permitan generar valor para sus clientes o usuarios.

Las entidades del Estado no son ajenas a los procesos de las tecnologías de la información y la comunicación, por tanto, el gobierno ha dispuesto un conjunto de procesos que permiten dirigir y controlar de manera eficiente los procesos administrativos, con el propósito que esta logre los objetivos propuestos, apoyados en infraestructuras y conocimiento que maximicen la atención de los ciudadanos y la protección de los datos como un valor constitucional y promesa de valor de las administraciones públicas en todos los temas referentes a tecnología de la información.

Teniendo en cuenta que los entes territoriales de sexta categoría en el Departamento del Cesar, presentan falencias en sus procesos de tecnología de información, especialmente en cuanto a la protección de información y prevención de posibles ataques, se hace necesario llevar a cabo la adaptación de un modelo de gobierno en TI como apoyo a los gobernantes y los entes territoriales, específicamente en el municipio de González, en el cual se produzca una gerencia direccionada para la toma de decisiones y la protección de datos personales y de archivos de datos electrónicos (Gobernación Cesar, 2020).

Uno de los principales objetivos para querer adoptar un modelo de gobierno en las áreas de desarrollo informático, es alinear los objetivos de las áreas de tecnologías de la información con los objetivos estratégicos de los entes territoriales, donde la implementación de dicho

modelo puede conducir a una reducción de costos de operación y a la optimización de los tiempos de ejecución de los procesos. Dado lo anterior, el trabajo que se pretende realizar tiene un aporte valioso para el municipio de González, ya que, al implementar el modelo de gobierno de vigilancia tecnológica, se tendrán progresos en la realización de sus procesos misionales y de apoyo, el uso eficiente de sus recursos informáticos y la mejora continua en la atención y protección de datos, cumpliendo así con los mandatos constitucionales frente estos temas de especial cuidado y vigilancia.

Finalmente, se considera que el estudio propicio al estudiante la aplicación de los conocimientos adquiridos a lo largo de su Maestría en Gobierno de TI, poniendo a disposición de la comunidad sus habilidades investigativas y analíticas para proponer un modelo que puede ser de utilidad para los municipios de sexta categoría y que genera impacto en los demás grupos de interés.

4. Marco referencial

4.1 Estado del arte.

Desde la antigüedad, la información ha estado siempre presente. El ser humano ha llevado datos importantes como bienes y propiedades por medio de registros escritos, logrando así mantener de una u otra forma el control y poder así tomar decisiones, si se tiene en cuenta lo anterior con el mundo actual aún se mantiene mismo concepto, pero la cantidad de información que se genera en el mundo contemporáneo es extremadamente grande, en donde nace la necesidad de administrar de forma segura y eficiente la información. Desde el desarrollo de parámetros internacionales que constituyen bloque de constitucionalidad y que en nuestra legislación y en general en nuestro ordenamiento jurídico tienen exigibilidad de derechos, frente al tratamiento de datos personales y por la protección de la soberanía nacional en cada uno de los niveles de desarrollo de las diferentes ramas del poder público, es decir el orden nacional, departamental y en caso de nuestra investigación el orden municipal de sexta categoría, se viene aplicando lo concerniente y estipulado en la constitución, en las leyes concordantes, en los, resoluciones, manuales, actos administrativos y en general en todos aquellos que emana la voluntad del estado para proteger los diferentes tipos de información y garantizar la privacidad, eficiencia en el trato y eficacia en el desarrollo de las estrategias de protección en el modelo de gobernanza de TI.

4.1.1 Antecedente Internacional.

Título: "Proyecto amparo (fortalecimiento de la capacidad regional de atención de incidentes de seguridad en américa latina y el caribe).
Autor (es): LACNIC con el apoyo de IDRC (centro de investigaciones para el desarrollo internacional) de Canadá.
Institución: LACNIC (Registros de direcciones de internet para américa latina y caribe).
Fecha: 2009 – 2010

Resumen: este manual ha sido desarrollado en el marco de las actividades del Proyecto

AMPARO, una iniciativa de LACNIC con el apoyo de IDRC de Canadá. El proceso de creación del mismo ha implicado un gran esfuerzo por parte de un equipo de expertos en el manejo de incidentes de seguridad, académicos de diversos países de la región, de alto reconocimiento nacional e internacional y personal de LACNIC, e IDRC. (AMPARO). Este es un proyecto donde se analizan todos los incidentes que ocurren en cuanto a seguridad de la información se refiere, el estudio está realizado a América latina la cual tiene un gran índice de incidentes en cuanto a violación de la seguridad de la información se refiere. Este proyecto trata todos estos factores que inciden a que la información se vea expuesta a una serie de amenazas y como tomar acciones preventivas para mitigar estos riesgos.

Título: "Tendencias en la seguridad cibernética en américa latina y el caribe y respuestas de los gobiernos."
Autor (es): Organización de los estados americanos
Institución: Organización de los estados americanos
Fecha: 07/04/2013

Resumen. En un mundo interconectado, es necesario buscar un equilibrio entre disfrutar la comodidad que ofrecen las tecnologías de la información y minimizar las oportunidades que su uso les ofrece a los delincuentes cibernéticos, quienes pueden, por ejemplo, difundir amenazas complejas explotando los populares dispositivos móviles y las aplicaciones en la nube para infiltrarse en blancos de alto valor y han convertido el espacio cibernético en un medio para victimizar al público (Americanos, 2013).

4.1.2 Antecedente Nacional.

Título: "Guía de buenas prácticas de seguridad de la información en contextos de micro, pequeñas y medianas empresas de la región."
Autor (es): Gerardo Ayala González, Julián Alberto Gómez Isaza.
Año: 2011
Institución: Universidad Tecnológica de Pereira.

Resumen: Este documento se centra en la aplicación de la norma ISO/IEC 27001 en atención a los numerales 4.2.2 Implementación y Operación de un Sistema de Gestión de la Seguridad de la Información (por sus siglas, SGSI), identificando las acciones de: la gestión apropiada, prioridades y responsabilidades de la gerencia en la creación de políticas que garanticen el cumplimiento de los objetivos del SGSI, además se hace referencia a la creación 4 de planes de acción para el tratamiento, análisis y gestión de los riesgos implementando procedimientos que brindan una atención oportuna a los incidentes de seguridad de la información, acompañados de estrategias de capacitación y formación para los integrantes de la organización. (SEGURIDAD) En el trabajo anterior se basa en establecer un sistema de gestión de seguridad de la información el cual está basado en el estándar ISO 27001 con el objetivo de establecer políticas de seguridad aplicando controles que permitan cumplir los objetivos de la misma.

Título: "Definición de un modelo de seguridad de la información para computación en nubes privadas y comunitarias."
Autor (es): Andrés Felipe Chacón Hurtado- Juan Federico Maya Sudupe
Año: 2012.
Institución: Universidad Icesi (Santiago de Cali - Colombia)

Resumen: En los últimos años, la computación en la nube ha tenido un incremento en su utilización. Se espera que dentro de los próximos 5 a 10 años este modelo de despliegue de servicios esté en una fase de producción, y que no sea de uso exclusivo de expertos en tecnologías de información y comunicaciones, sino también de académicos, empresarios y personas comunes que se vean atraídos por las ventajas ofrecidas por este modelo. La seguridad de la información es uno de los aspectos que más preocupan a los directivos de TI para migrar sus aplicaciones e información a la nube, debido a que están confiando sus datos privados a un tercero. Por este motivo, las organizaciones toman medidas que garanticen el control de su información y que minimicen los riesgos que la pueden impactar, basándose en estándares de seguridad pensados para la computación tradicional. Existen iniciativas y marcos de trabajo, tales como PCI o CSA, que pueden aportar información, pero al no haber un modelo completo de seguridad para la computación en la nube, existe la posibilidad de no hacer consciencia de los diferentes riesgos, o tratarlos de forma

inadecuada. (Chacón Hurtado Andrés Felipe, 2012). Esta investigación busca darle un tratamiento diferente a la información en cual está basado en que la información este alojado en la nube, es decir, que estén situada o almacenadas en servidores distintos, pero con accesos comunitarios.

4.2 Marco teórico

Al abarcar contenidos teóricos a la investigación cabe resaltar las teorías en las cuales se ha enfocado a través de los años para realizar un sistema de gestión de seguridad de la información, que sea apropiado para alcanzar el éxito deseado y se adapte a las necesidades presentes en la organización que desee implementarlo.

4.2.1 Teoría de la información.

La Teoría de la Información nos muestra, entre otras cosas, el camino a seguir para determinar la cantidad de información útil a partir de unos datos. Y para comprimir la información de manera que los datos se representen de una manera eficiente. Nace de la necesidad de optimizar los contenidos de las informaciones, en una época histórica en la que la comunicación alcanzaba un destacado papel (Shannon, 1948), esto después del nacimiento del código binario (Hartley, 1927) y los primeros pasos de encriptación (Turing, 1936). En consecuencia, se debía encontrar una forma en la cual determinar "la cantidad de información" que entregaba un mensaje.

El mayor investigador de este tema fue Claude Shannon quién aportó el concepto de que la información debe dejar de verse como inmaterial y subjetiva, sino que como perfectamente material y cuantificable. Así pasó a considerarse de una manera independiente un dispositivo de representación y se dio la posibilidad de hablar de procesos de representación y manipulación de la información sin hacer énfasis si era el cerebro o un ordenador quien realizaba dichos procesos. Esto permitió, dar el primer paso para la cibernética: el control de las máquinas para realizar tareas humanas. (TOMAS, 2014)

Seguridad de la información desde la Teoría de las Limitaciones el eslabón más débil de la cadena. A cualquier profesional le suena: "La seguridad es como una cadena, es tan fuerte como el

eslabón más débil". Esto se dice por varios motivos: Para enfatizar la naturaleza de seguridad como proceso, como sistema, pero también

Para entender que se trata de una posición de defensa débil, es decir, el defensor tiene que defender todos los puntos, mientras que al atacante le basta con encontrar un punto vulnerable para tener éxito en su ataque.

Sin embargo, aunque se está convencido de que esto es así, muy pocos (por no decir, ninguno) realiza la gestión de este proceso conforme a esta máxima. Porque si se gestionará la seguridad teniendo este paradigma en mente, lo mejor sería emplear la misma estrategia que cualquier otro sistema cuya producción esté gobernada por su factor limitante. Me explico, después de identificarlo, habría que hacer que este factor limitante produjese al máximo nivel. Esta forma de gestionar la seguridad cambiaría sobremanera el enfoque actual del proceso de gestión. Si se sigue lo establecido en los estándares, por ejemplo, el estándar ISO/IEC 27001 que establece las pautas para montar un Sistema de Gestión de la Seguridad de la Información (SGSI) "certificable", tenemos que (como ya hemos comentado aquí anteriormente) llevar a cabo un análisis de riesgos que nos permita identificar el nivel de riesgo por cada área o dominio del alcance establecido y pasar a gestionar el riesgo en función de la estrategia definida.

Si se plantea la seguridad como un sistema en el que el output fuera el nivel de seguridad de la organización (parece obvio, ¿no?), el máximo nivel estaría marcado por el máximo caudal que pudiera gestionar el cuello de botella del sistema, es decir, el nivel de seguridad de la organización sería el del eslabón más débil de la cadena.

¿Cuál es la diferencia entre estas dos maneras de gestionar la seguridad? la diferencia es que no tendría tanto interés realizar un análisis de riesgos como el hecho de encontrar cuál es el factor limitante, cuál es el eslabón más débil, puesto que sería el que marcaría el nivel de seguridad de nuestra organización. A partir de ahí, si se quiere elevar el nivel de seguridad de nuestra organización, se debería gestionar esa limitación y eso, ya se sabe, hay que preguntarle a Goldratt el cómo. (RAMOS, 2011)

Teoría de la seguridad por oscuridad Gaming. Shannon buscó la seguridad contra el atacante con poderes computacionales ilimitados: si la información transmite cierta información, a continuación, el atacante de Shannon seguramente va a extraer esa información. Diffie y Hellman refinaron el modelo atacante de Shannon al tener en cuenta el hecho de que los atacantes reales son computacionalmente limitados. Esta idea se convirtió en uno de los grandes nuevos paradigmas en ciencias de la computación, y condujo a la criptografía moderna. Shannon también buscó la seguridad contra el atacante con poderes lógicos y observacionales ilimitadas, expresada a través de la máxima de que "el enemigo conoce el sistema". Este punto de vista todavía es refrendado de la criptografía. La formulación popular, que se remonta a Kerckhoffs, es que "no hay seguridad por oscuridad", lo que significa que los algoritmos no se pueden mantener ocultos al atacante, y que las seguridades sólo deben confiar en las claves secretas. De hecho, la criptografía moderna va más allá de Shannon o Kerckhoffs en asumir tácitamente que si hay un algoritmo que puede romper el sistema, entonces el atacante seguramente encontrará ese algoritmo. El atacante no es visto como un equipo omnipotente más, pero él todavía se interpreta como un programador omnipotente (Cano, 2013).

Así que el paso de Diffie-Hellman de ilimitado a potencias computacionales limitados no se ha extendido a un paso de la ilimitada a los limitados poderes lógicos o de programación. Es la hipótesis de que todos los algoritmos factibles finalmente serán descubiertos y aplican realmente diferente de la suposición de que todo lo que es computable el tiempo se puede calcular. Aquí se exploran algunas maneras para refinar los modelos actuales del atacante y del defensor, teniendo en cuenta lo limitado de sus facultades lógicas y programación. Si el atacante adaptativo consulta activo el sistema para buscar a sus vulnerabilidades, el sistema puede ganar un poco de seguridad al aprender activamente los métodos del atacante, y la adaptación a ellos. (Pavlovic,2013).

4.3 Marco conceptual

En este apartado realizo una vigilancia conceptual, con el fin que sustente la investigación del presente proyecto. Se tomarán como conceptos principales: Gestión de la Seguridad de la Información, GRISK (Gestión de riesgos), COBIT, Normas ISO y el proyecto Gobierno en Línea (GEL) e IT4+ emanados por el Gobierno Nacional.

Información:

Es el conjunto de datos o mensajes inteligibles creados con un lenguaje de representación y que debemos proteger ante las amenazas del entorno, durante su transmisión o almacenamiento, usando técnicas criptográficas entre otras herramientas. – La teoría de la información (Jorge, 2006) mide la cantidad de información que contiene un mensaje a través del número medio de bits necesario para codificar todos los posibles mensajes con un codificador óptimo.

Riesgos y Seguridad**:**

Los análisis de riesgos y de la seguridad se desarrollan con el objetivo de minimizar los diferentes riesgos debido a la de amenazas y vulnerabilidades tales como: las personas, organizaciones, gobiernos, tecnología o el medio ambiente. En la actualidad es muy común que las empresas del sector privado, gobiernos y la sociedad estén de cara a los retos ambientales, económicos y sociales lo que implica que los responsables, estén con la mejor disposición en temas de visión, liderazgo y herramientas adecuadas para ello.

Gobierno corporativo de TIC (corporate governance of IT):

El sistema mediante el cual se dirige y controla el uso actual y futuro de las tecnologías de la información

Gestión (management):

El sistema de controles y procesos requeridos para lograr los objetivos estratégicos establecidos por la dirección de la organización. Está sujeta a la guía y monitorización establecida mediante el gobierno corporativo.

Interesado (stakeholder):

Individuo, grupo u organización que puede afectar, ser afectado, o percibir que va a ser

afectado, por una decisión o una actividad.

Uso de TIC (use of IT):

Planificación, diseño, desarrollo, despliegue, operación, gestión y aplicación de TI para cumplir con las necesidades del negocio. Incluye tanto la demanda como la oferta de servicios de TIC por unidades de negocio internas, unidades especializadas de TI, proveedores externos y "utility services" (como los que se proveen de software como servicio).

Factor humano (human behavior):

La comprensión de las interacciones entre personas y otros elementos de un sistema con la intención de asegurar el bienestar de las personas y el buen rendimiento del sistema. Incluye la cultura, necesidades y aspiraciones de las personas como individuos y como grupo.

4.4 Marco geoFigura

El proyecto de investigación se realizará para las alcaldías de sexta categoría del Departamento del Cesar que está situado en el norte del país, en la llanura del Caribe; localizado entre los 07º41'16" y 10º52'14" de latitud norte y los 72º53'27" y 74º08'28" de longitud oeste Cuenta con una superficie de 22.925 km2 lo que representa el 2.0 % del territorio nacional. Limita por el Norte con los departamentos de Magdalena y La Guajira, por el Este con la República de Venezuela y el departamento de Norte de Santander, por el Sur con los departamentos de Norte de Santander y Santander, y por el Oeste con los departamentos de Bolívar y Magdalena (Cesar., 2016).

Figura 1. Departamento del Cesar

Fuente: Google maps (2021)

4.5 Marco Temporal

Para el desarrollo del proyecto de investigación se propone un plazo de 12 meses a partir de la aprobación de la propuesta para abarcar los elementos de Gobierno de TI planteados en los objetivos.

4.6 Marco legal

Acerca de la Tecnologías de la información y la seguridad digital

Constitución Política de Colombia

Las entidades públicas, ministerios, gobernaciones, alcaldías, poseen bases de datos e información de sus usuarios que puede ser vulnerada en caso que sus TI sean vulneradas, sin embargo, estas deben garantizar que esta información que sea de carácter reservada no vaya a ser publicada sin previa autorización o parte de su información pueda prestarse para exponerla a calumnias o difamaciones. Es en este sentido que el artículo 15 de la Constitución Política de

Colombia, determina como derecho de todos los colombianos a su intimidad personal y familiar y a su buen nombre, exigiendo además que el Estado los respete y haga respetar. Además de poder conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en los bancos de datos y en archivos de entidades públicas y privadas (Secretaría Senado, 2021).

En igual sentido se observa que el artículo 12 de la Declaración Universal de los derechos humanos y el artículo 11 de la Convención Americana de Derechos Humanos de 1969 protege la honra y la reputación de todos los seres humanos, estipulando el derecho de la protección de la ley contra injerencia o ataques.

- El artículo 20 de la Constitución política ampara los derechos de libertad de expresión y difusión de pensamiento y opiniones, además del derecho a la rectificación en condiciones de equidad. La TI se han convertido en un medio de difusión rápido, oportuno y universal para abrir la oportunidad a muchas personas que puedan participar y enterarse de la información que procesa el sector público (Secretaría Senado, 2021).

- Desde el año 1991, cuando se expidió la Constitución Política a través del artículo 71, se dieron lineamientos para la promoción y desarrollo de la ciencia y tecnología, reconociendo estos sectores como fundamentales para el desarrollo económico y social de los pueblos; su forma me motivar este ejercicio es la generación de estímulos especiales a personas e instituciones que realicen este tipo de actividades.

- La constitución política de Colombia ha definido en su artículo 75 el espectro electromagnético como un bien público inajenable imprescriptible, además garantiza el pluralismo informativo y la competencia, por tanto, las TI no son exclusivas del sector público, esto exige un mejor desempeño por parte de las entidades para que la información que producen sea de interés y atractiva para la comunidad.

- Las leyes 23 de 1982 y 44 de 1993 han establecido directrices en cuento al manejo de los derechos de autor, entendiéndose estos como los derechos de los creadores de obras literarias o artísticas, entre las cuales se encuentran las bases de datos, por este motivo las entidades públicas

deben tener claridad cuando van a publicar información si ésta contiene derechos de autor o si en caso contrario la entidad ha declarado derechos sobre información de reserva (Secretaría Senado, 2020).

- Las entidades públicas, incluyendo las alcaldías han incorporado a sus medios de comunicación los correos electrónicos, es por ello que se deben guardar los cuidados en el manejo de información a través de estos medios; en este sentido la Ley 527 de 1999 ha reglamentado el acceso y uso de los mensajes de datos, del comercio electrónico y de las firmas digitales (Mintic, 2020).

- Las Tecnologías de la Información han facilitado el mejoramiento en la prestación de los servicios que el presta el estado a la ciudadanía, la racionalización, entendiéndose esta como los mecanismos que se implementan para facilitar el acceso a los servicios por parte de los usuarios, como son el pago electrónico, las solicitudes por mecanismos digitales, el uso de plataformas para registros, entre otros que favorecen el ahorro de tiempo y dinero por cuestiones de desplazamiento; es allí donde la Ley 962 de 2005 y en especial su artículo 6 hace un llamado a las entidades públicas a utilizar medios tecnológicos para informar y atender los tramites y procedimientos de la entidad. Además, promueve la implementación de condiciones y requisitos de seguridad que sean procedentes.

- Cuando la constitución establece orientaciones sobre el derecho a la honra, la intimidad y el buen nombre, hace referencia a todas las situaciones que en la vida cotidiana puedan pasar, sin embargo las reglamentaciones desagregan y aterrizas estas condiciones, así como la Ley Estatutaria 1266 Del 31 De Diciembre De 2008 y la Ley 1581 de 2012 definen de manera detallada las formas de actuar frente a los escenarios relacionadas con la recolección, tratamiento y circulación de datos personales a que se refiere el artículo 15 de la constitución política (Función Pública , 2020).

- El estado colombiano ha avanzado en la implementación de estrategias que permitan mejorar los servicios a los ciudadanos y a las empresas, la Ley 1151 de 2008 ha dispuesto las Tecnologías de la Información y la Comunicación, como uno de los mecanismos más relevantes

para fortalecer el gobierno nacional, departamental y local; estableciendo como principios aplicables a la estrategia denomina Gobierno en Línea: a) Gobierno centrado en el ciudadano, b) Visión unificada del Estado, c) Acceso equitativo y multicanal d) Protección de la información del individuo, e)Credibilidad y confianza en el Gobierno en Línea (Función Pública , 2020).

- En el año 2017 el departamento administrativo de la función pública emitió el Decreto 1499, a través del cual se reglamentó la integración del sistema de desarrollo administrativo y la gestión de la calidad en las entidades del estado, para que con la implementación de las políticas, normas, procedimientos, formatos se obtenga un mejor desempeño institucional y por ende la satisfacción de la ciudadanía que demanda los servicios del estado. Adicionalmente en su artículo 2.2.22.2.1, definió las políticas de gestión institucional que las entidades deben desarrollas entre las cuales se encuentra la política de gobierno en línea y de seguridad digital (Presidencia, 2020).

- Recientemente el Ministerio de Tecnología y la Información estableció los lineamientos generales para la implementación del Modelo de Seguridad y Privacidad de la Información - MSPI, la guía de gestión de riesgos de seguridad de la Información y el procedimiento para la gestión de los incidentes de seguridad digital, y, establecer los lineamientos y estándares para la estrategia de seguridad digital, a través de la Resolución 500 de 2021. Esta reglamentación trae a los municipios a través de sus Alcaldías a mejorar los procesos que involucran la TI puesto que deben adoptar la estrategia de seguridad digital en la que se integren los principios, políticas, procedimientos, guías, manuales, formatos y lineamientos para la gestión de la seguridad de la información digital (Mintic , 2020).

5. Diseño metodológico

5.1 Tipo de investigación

Para el desarrollo de la investigación se acudirá a la investigación Descriptiva-explicativa, porque esta busca especificar las propiedades, características y los perfiles de, procesos, procedimientos o cualquier otro fenómeno que se someta a un análisis. Describe tendencias de un grupo o población. Es decir, únicamente pretenden medir o recoger información de manera independiente o conjunta sobre los conceptos o las variables a las que se refieren, esto es, su objetivo no es indicar como se relacionan éstas. (Hernández Sampieri, 2010).

De igual forma, es una investigación cualitativa, toda vez que pretende caracterizar los procesos de TI en un lugar determinado, Teniendo en cuenta que el objeto del estudio inicialmente es establecer Diseño del Modelo de Gobierno de TI, dirigido a las alcaldías de sexta categoría del sur del departamento del Cesar, Para la Gestión de Riesgos de la Seguridad de la Información, para lograr este fin se necesita caracterizar el objeto de estudio, identificar los objetos que tienen dicha característica, describir el contexto en el cual se está desarrollando el objeto de estudio, cuantificar que tan grande es la problemática.

5.2 Población y muestra

La población está definida las Alcaldías del Sur del Departamento del Cesar, Considerando que la población objeto de la investigación, cuantitativamente es reducida, se trabajará con el total de la población.

5.3 Técnicas e instrumentos de recolección de datos

Para el cumplimiento de la recolección de la información será recopilada por medio de observación directa, listas de verificación y Petición de información a las alcaldías de sexta categoría del sur del departamento del Cesar.

Según (PUENTE, 2009) la observación directa es una técnica que consiste en observar atentamente el fenómeno, hecho o caso, sin intervención, con el fin de tomar información y registrarla para su posterior análisis. La observación es un elemento fundamental de todo proceso investigativo; en ella se apoya el investigador para obtener el mayor número de datos. Gran parte del acervo de conocimientos que constituye la ciencia ha sido lograda mediante la observación. Observar científicamente significa observar con un objetivo claro, definido y preciso: el investigador sabe qué es lo que desea observar y para qué quiere hacerlo, lo cual implica que debe preparar cuidadosamente la observación.

5.4 Fases de Desarrollo

Este trabajo se desarrollará en 4 fases

Fase 1: Análisis del contexto y definición del problema, este se desarrolla en un término de 15 días contados a partir del 1 de octubre de 2020 y termina el 15 de octubre de 2020. Del resultado de esta fase se extrae un conocimiento general de la problemática

Fase 2: Recolección de información, esta fase comienza el 16 de octubre 2020 y se extiende hasta el 28 de febrero de 2021, del resultado de esta fase, se estructura los diferentes marcos que constituyen la investigación, es decir, Marco Histórico, conceptual, teórico, legal y de referencia.

Fase 3: Procesamiento de los datos, obtención de resultados y estructuración de resultados para desarrollo de propuesta investigativa, en esta fase se analiza los datos obtenidos en las diferentes fuentes de información, con el fin de estructurar las mismas para dar solución al problema inicial. Esta fase comienza desde el primero (1) de marzo de 2021 hasta 30 de abril de 2021.

Fase 4: Estructuración del modelo de Gestión de TI, propuesta de mejora continua de los servicios de TI y Conclusiones finales de la investigación. Esta fase se desarrolla desde el primero (1°) de Mayo hasta el 30 de octubre de 2021

Tiempo total del desarrollo de la investigación: primero de octubre de 2020 hasta 30 de octubre de 2021 **total meses 12**

5.5 Metodología.

Fase 1: Recopilación deInformación

Está fase tiene como propósito el recolectar la información de los diferentes tipos de fuentes, permitiendo la construcción del objetivo de este proyecto y su respectiva sustentación.

El alcance de esta fase es revisar la información primaria y secundaria acerca de los diseños de un modelo de gestión de riesgos de tecnologías de la información y seguridad de la información en las alcaldías del departamento del atlántico.

Fase 2: Caracterización de Requerimiento

Está fase tiene como propósito en definir un alcance, organizar y estructurar la información cosechada en la fase de recopilación, permitiendo la determinación de los requerimientos de un modelo de gestión de riesgos de tecnologías de la información y seguridad de la información en las alcaldías del departamento del Cesar.

Fase 3: Diseño del Modelo de Gobierno

Está fase tiene como propósito en definir y diseñar modelo de gestión de riesgos de tecnologías de la información y seguridad de la información en las alcaldías del departamento del atlántico, que permita integrar los modelos de Gobierno de TI ISO 27005 y de innovación para generar valor, ventajas competitivas en los procesos y generar confianza de los habitantes de los diferentes habitantes del departamento.

Fase 4: Diseño de la Estructura de Proceso de Gobierno de TI

Está fase tiene como propósito en definir la estructura organizacional, los procesos, las métricas y agenda informática para desplegar modelo de gestión de riesgos de tecnologías de la información y seguridad de la información en las alcaldías del departamento del atlántico.

6. Resultados

6.1 Análisis de la situación actual de los municipios de sexta categoría del sur del Departamento del Cesar.

La Alcaldía es una Entidad del Estado al servicio del ciudadano, conformada por varias dependencia e Institutos Descentralizados que tienen como principal objetivo cumplir variadas funciones enfocadas al beneficio de la comunidad brindando servicios de manera oportuna, eficaz, con calidad y honestidad para el mejoramiento de la ciudad y el bienestar de los habitantes.

6.1.1 Categorización.

La ley 1551 de 2012, por la cual se dictan normas para modernizar la organización y el funcionamiento de los municipios, establece que los distritos y municipios se clasificarán atendiendo su población, ingresos corrientes de libre destinación, importancia económica y situación geográfica. Para efectos de lo previsto en la ley y las demás normas que expresamente lo dispongan, las categorías serán las siguientes:

Primer grupo (Grandes municipios):

a) Categoría Especial

Tabla 2. Características municipios categoría especial

Aspecto	Característica
Población	Superior o igual a los quinientos mil unos (500.001) habitantes
Ingresos	Ingresos corrientes de libre destinación anuales: que superen cuatrocientos mil (400.000) salarios mínimos legales mensuales vigentes
Importancia económica	Grado Uno

Fuente: Ley 1551 de 2012

b) Primera Categoría

Tabla 3. Características Municipios Primera Categoría

Aspecto	Característica
Población	Comprendida entre cien mil unos (100.001) y quinientos mil (500.000) habitantes
Ingresos	Ingresos corrientes de libre destinación anuales: Superiores a cien mil (100.000) y hasta de cuatrocientos mil (400.000) salarios mínimos legales mensuales vigentes
Importancia económica	Grado dos

Fuente: Ley 1551 de 2012

Segundo grupo (Municipios intermedios):

Tabla 4. Características Municipios Segunda Categoría

Aspecto	Característica
Población	Comprendida entre cincuenta mil uno (50.001) y cien mil (100.000) habitantes
Ingresos	Ingresos corrientes de libre destinación anuales: Superiores a cincuenta mil (50.000) y hasta de cien mil (100.000) salarios mínimos legales mensuales vigentes
Importancia económica	Grado tres

Fuente: Ley 1551 de 2012

d) Tercera categoría

Tabla 5. Características Municipios Tercera Categoría

Aspecto	Característica
Población	Comprendida entre treinta mil uno (30.001) y cincuenta mil (50.000) habitantes
Ingresos	Ingresos corrientes de libre destinación anuales: Superiores a treinta mil (30.000) y hasta de cincuenta mil (50.000) salarios mínimos legales mensuales
Importancia económica	Grado cuatro

Fuente: Ley 1551 de 2012

e) Cuarta categoría

Tabla 6. Características Municipios Cuarta Categoría

Aspecto	Característica
Población	Comprendida entre veinte mil unos (20.001) y treinta mil (30.000) habitantes
Ingresos	Ingresos corrientes de libre destinación anuales: Superiores a veinticinco mil (25.000) y de hasta de treinta mil (30.000) salarios mínimos legales mensuales
Importancia económica	Grado cinco

Fuente: Ley 1551 de 2012

Tercer grupo (Municipios básicos):

f) Quinta Categoría

Tabla 7. Características Municipios Quinta Categoría

Aspecto	Característica
Población	Comprendida entre diez mil unos (10.001) y veinte mil (20.000) habitantes
Ingresos	Ingresos corrientes de libre destinación anuales: Superiores a quince mil (15.000) y hasta veinticinco mil (25.000) salarios mínimos legales mensuales
Importancia económica	Grado seis

Fuente: Ley 1551 de 2012

g) Sexta Categoría

Tabla 8. Características Municipios Sexta Categoría

Aspecto	Característica
Población	Igual o inferior a diez mil (10.000).
Ingresos	Ingresos corrientes de libre destinación anuales: No superiores a quince mil (15.000) salarios mínimos legales mensuales.
Importancia económica	Grado siete.

Fuente: Ley 1551 de 2012

6.1.2 Diagnóstico de la situación actual de las alcaldías.

Con el fin de establecer el nivel de cumplimiento frente al sistema de seguridad de la información, se aplicó una lista de verificación basada en la estrategia Gobierno Digital en las alcaldías de Aguachica, Gamarra, Gonzales, La Gloria, Pelaya, Río de Oro, San Alberto, San

Martín, obteniendo los resultados que se muestran a continuación.

6.1.2.1 *Diagnóstico Aguachica.*

Tabla 9. Diagnóstico Aguachica

No.	**Evaluación de Efectividad de controles**			
	Dominio	**Calificación Actual**	**Calificación Objetivo**	**Evaluación de efectividad de control**
A.5	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	0	100	Inexistente
A.6	Organización de la seguridad de la información	0	100	Inexistente
A.7	Seguridad de los recursos humanos	0	100	Inexistente
A.8	Gestión de activos	0	100	Inexistente
A.9	Control de acceso	0	100	Inexistente
A.10	Criptografía	0	100	Inexistente
A.11	Seguridad física y del entorno	0	100	Inexistente
A.12	Seguridad de las operaciones	0	100	Inexistente
A.13	Seguridad de las comunicaciones	0	100	Inexistente
A.14	Adquisición, desarrollo y mantenimiento de sistemas	0	100	Inexistente
A.15	Relaciones con los proveedores	0	100	Inexistente
A.16	Gestión de incidentes de seguridad de la información	0	100	Inexistente

A.17	Aspectos de seguridad de la información de la gestión de la continuidad del negocio	0	100	Inexistente
A.18	Cumplimiento	0	100	Inexistente
Promedio evaluación de controles		**0**	**100**	Inexistente

Fuente: Elaboración propia

Figura 1. Brecha ISO 2701:2013 Alcaldía Aguachica

Fuente: Elaboración propia

Una vez aplicada la lista de chequeo a la Alcaldía de Aguachica, puede evidenciarse que su nivel de cumplimiento frente a la norma es cero, lo que significa que es inexistente el sistema de seguridad de la información y no cuentan con controles definidos para garantizar la confiabilidad y seguridad de la información.

6.1.2.2 *Diagnóstico Alcaldía de Gamarra.*

Tabla 10. Diagnóstico Alcaldía de Gamarra

No.	**Evaluación de Efectividad de controles**			
	Dominio	**Calificación Actual**	**Calificación Objetivo**	**Evaluación de efectividad de control**
A.5	Políticas de seguridad de la información	20	100	Inicial
A.6	Organización de la seguridad de la información	2	100	Inicial
A.7	Seguridad de los recursos humanos	0	100	Inexistente
A.8	Gestión de activos	0	100	Inexistente
A.9	Control de acceso	5	100	Inicial
A.10	Criptografía	0	100	Inexistente
A.11	Seguridad física y del entorno	0	100	Inexistente
A.12	Seguridad de las operaciones	0	100	Inexistente
A.13	Seguridad de las comunicaciones	0	100	Inexistente
A.14	Adquisición, desarrollo y mantenimiento de sistemas	0	100	Inexistente
A.15	Relaciones con los proveedores	0	100	Inexistente
A.16	Gestión de incidentes de seguridad de la información	0	100	Inexistente
A.17	Aspectos de seguridad de la información de la gestión de la continuidad del negocio	0	100	Inexistente
A.18	Cumplimiento	0	100	Inexistente
Promedio evaluación de controles		**2**	**100**	**Inicial**

Fuente: Elaboración propia

Figura 2. Brecha ISO 2701:2013 Alcaldía Gamarra

Fuente: Elaboración propia

Al aplicar la lista de verificación, puede concluirse que la Alcaldía de Gamarra se encuentra en la fase inicial de implementación, queriendo decir esto que hay una evidencia de que la organización ha reconocido que existe un problema y que hay que tratarlo. Sin embargo, aún no cuenta con procesos estandarizados, asimismo, la implementación de un control depende de cada individuo y es principalmente reactiva.

6.1.2.3 *Diagnóstico Alcaldía de Gonzales.*

Tabla 11. Diagnóstico Alcaldía de Gonzales

No.	**Evaluación de Efectividad de controles**			
	Dominio	**Calificación Actual**	**Calificación Objetivo**	**Evaluación de efectividad de control**
A.5	Políticas de seguridad de la información	0	100	Inexistente
A.6	Organización de la seguridad de la información	10	100	Inicial
A.7	Seguridad de los recursos humanos	10	100	Inicial
A.8	Gestión de activos	0	100	Inexistente
A.9	Control de acceso	16	100	inicial
A.10	Criptografía	0	100	Inexistente
A.11	Seguridad física y del entorno	9	100	Inicial
A.12	Seguridad de las operaciones	0	100	Inexistente
A.13	Seguridad de las comunicaciones	0	100	Inexistente
A.14	Adquisición, desarrollo y mantenimiento de sistemas	0	100	Inexistente
A.15	Relaciones con los proveedores	0	100	Inexistente

A.16	Gestión de incidentes de seguridad de la información	0	100	Inexistente
A.17	Aspectos de seguridad de la información de la gestión de la continuidad del negocio	0	100	Inexistente
A.18	Cumplimiento	0	100	Inexistente
Promedio evaluación de controles		**3**	**100**	**Inicial**

Fuente: Elaboración propia

Figura 3. Brecha ISO 2701:2013 Alcaldía Gonzales

Fuente: Elaboración propia

Al aplicar la lista de verificación, puede concluirse que la Alcaldía de Gonzales se

encuentra en la fase inicial de implementación, queriendo decir esto que hay una evidencia de que la organización ha reconocido que existe un problema y que hay que tratarlo. Sin embargo, aún no cuenta con procesos estandarizados, asimismo, la implementación de un control depende de cada individuo y es principalmente reactiva.

6.1.2.4 *Diagnóstico Alcaldía de La Gloria.*

Tabla 12. Diagnóstico Alcaldía La Gloria

No.	**Evaluación de Efectividad de controles**			
	Dominio	**Calificación Actual**	**Calificación Objetivo**	**Evaluación de efectividad de control**
A.5	Políticas de seguridad de la información	10	100	Inicial
A.6	Organización de la seguridad de la información	11	100	Inicial
A.7	Seguridad de los recursos humanos	11	100	Inicial
A.8	Gestión de activos	6	100	Inicial
A.9	Control de acceso	0	100	Inexistente
A.10	Criptografía	0	100	Inexistente
A.11	Seguridad física y del entorno	0	100	Inexistente
A.12	Seguridad de las operaciones	0	100	Inexistente
A.13	Seguridad de las comunicaciones	0	100	Inexistente
A.14	Adquisición, desarrollo y mantenimiento de sistemas	0	100	Inexistente
A.15	Relaciones con los proveedores	0	100	Inexistente

A.16	Gestión de incidentes de seguridad de la información	0	100	Inexistente
A.17	Aspectos de seguridad de la información de la gestión de la continuidad del negocio	17	100	Inicial
A.18	Cumplimiento	0	100	Inexistente
Promedio evaluación de controles		**4**	**100**	**Inicial**

Fuente: Elaboración propia

Figura 4. Brecha ISO 2701:2013 Alcaldía La Gloria

Fuente: Elaboración propia.

Al aplicar la lista de verificación, puede concluirse que la Alcaldía de La Gloria se encuentra en la fase inicial de implementación, queriendo decir esto que hay una evidencia de que la organización ha reconocido que existe un problema y que hay que tratarlo. Sin embargo, aún no cuenta con procesos estandarizados, asimismo, la implementación de un control depende de cada individuo y es principalmente reactiva.

6.1.2.5 *Diagnóstico Alcaldía Pelaya.*

Tabla 13. Diagnóstico Alcaldía Pelaya

No.	**Evaluación de Efectividad de controles**			
	Dominio	**Calificación Actual**	**Calificación Objetivo**	**Evaluación de efectividad de control**
A.5	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	20	100	Inicial
A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	28	100	Repetible
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	6	100	Inicial
A.8	GESTIÓN DE ACTIVOS	18	100	Inicial
A.9	CONTROL DE ACCESO	25	100	Repetible
A.10	CRIPTOGRAFÍA	10	100	Inicial
A.11	SEGURIDAD FÍSICA Y DEL ENTORNO	0	100	Inexistente
A.12	SEGURIDAD DE LAS OPERACIONES	0	100	Inexistente
A.13	SEGURIDAD DE LAS COMUNICACIONES	0	100	Inexistente
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	0	100	Inexistente
A.15	RELACIONES CON LOS PROVEEDORES	20	100	Inicial
A.16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	0	100	Inexistente
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA	10	100	Inicial

	GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO			
A.18	CUMPLIMIENTO	25	100	Repetible
PROMEDIO EVALUACIÓN DE CONTROLES		**12**	**100**	**Inicial**

Fuente: Elaboración propia

Figura 5. Brecha ISO 2701:2013 Alcaldía Pelaya

Fuente: Elaboración propia

Al aplicar la lista de verificación, puede concluirse que la Alcaldía de Pelaya se encuentra en la fase inicial de implementación, queriendo decir esto que hay una evidencia de que la organización ha reconocido que existe un problema y que hay que tratarlo. Sin embargo, aún no cuenta con procesos estandarizados, asimismo, la implementación de un control depende de cada individuo y es principalmente reactiva.

6.1.2.6 *Diagnóstico Alcaldía Río de Oro.*

Tabla 14. Diagnóstico Alcaldía Río de Oro

No.	Evaluación de Efectividad de controles			
	Dominio	**Calificación Actual**	**Calificación Objetivo**	**Evaluación de efectividad de control**
A.5	POLITICAS DE SEGURIDAD DE LA INFORMACIÓN	30	100	Repetible
A.6	ORGANIZACIÓN DE LA SEGURIDAD DE LA INFORMACIÓN	18	100	Inicial
A.7	SEGURIDAD DE LOS RECURSOS HUMANOS	9	100	Inicial
A.8	GESTIÓN DE ACTIVOS	0	100	Inexistente
A.9	CONTROL DE ACCESO	14	100	Inicial
A.10	CRIPTOGRAFÍA	0	100	Inexistente
A.11	SEGURIDAD FÍSICA Y DEL ENTORNO	0	100	Inexistente
A.12	SEGURIDAD DE LAS OPERACIONES	0	100	Inexistente
A.13	SEGURIDAD DE LAS COMUNICACIONES	0	100	Inexistente
A.14	ADQUISICIÓN, DESARROLLO Y MANTENIMIENTO DE SISTEMAS	0	100	Inexistente
A.15	RELACIONES CON LOS PROVEEDORES	0	100	Inexistente

A.16	GESTIÓN DE INCIDENTES DE SEGURIDAD DE LA INFORMACIÓN	0	100	Inexistente
A.17	ASPECTOS DE SEGURIDAD DE LA INFORMACIÓN DE LA GESTIÓN DE LA CONTINUIDAD DEL NEGOCIO	0	100	Inexistente
A.18	CUMPLIMIENTO	0	100	Inexistente
PROMEDIO EVALUACIÓN DE CONTROLES		**5**	**100**	**Inicial**

Fuente: Elaboración propia

Figura 6. Brecha ISO 2701:2013 Alcaldía Río de Oro

Fuente: Elaboración propia

Al aplicar la lista de verificación, puede concluirse que la Alcaldía Río de Oro se encuentra en la fase inicial de implementación, queriendo decir esto que hay una evidencia de que la organización ha reconocido que existe un problema y que hay que tratarlo. Sin embargo, aún no cuenta con procesos estandarizados, asimismo, la implementación de un control depende de cada individuo y es principalmente reactiva.

6.1.2.7 *Diagnóstico Alcaldía San Alberto.*

Tabla 15. Diagnóstico Alcaldía San Alberto.

No.	**Evaluación de Efectividad de controles**			
	Dominio	**Calificación Actual**	**Calificación Objetivo**	**Evaluación de efectividad de control**
A.5	Políticas de seguridad de la información	20	100	Inicial
A.6	Organización de la seguridad de la información	16	100	Inicial
A.7	Seguridad de los recursos humanos	0	100	Inexistente
A.8	Gestión de activos	0	100	Inexistente
A.9	Control de acceso	8	100	Inicial
A.10	Criptografía	0	100	Inexistente
A.11	Seguridad física y del entorno	4	100	Inicial
A.12	Seguridad de las operaciones	3	100	Inicial
A.13	Seguridad de las comunicaciones	0	100	Inexistente
A.14	Adquisición, desarrollo y mantenimiento de sistemas	0	100	Inexistente
A.15	Relaciones con los proveedores	0	100	Inexistente

A.16	Gestión de incidentes de seguridad de la información	0	100	Inexistente
A.17	Aspectos de seguridad de la información de la gestión de la continuidad del negocio	0	100	Inexistente
A.18	Cumplimiento	0	100	Inexistente
Promedio evaluación de controles		**4**	**100**	**Inicial**

Fuente: Elaboración propia

Figura 7. Brecha ISO 2701:2013 Alcaldía San Alberto

Fuente: Elaboración propia

Al aplicar la lista de verificación, puede concluirse que la Alcaldía de San Alberto se encuentra en la fase inicial de implementación, queriendo decir esto que hay una evidencia de que la organización ha reconocido que existe un problema y que hay que tratarlo. Sin embargo, aún no cuenta con procesos estandarizados, asimismo, la implementación de un control depende de cada individuo y es principalmente reactiva.

6.1.2.8 *Diagnóstico Alcaldía San Martín.*

Tabla 16. Diagnóstico Alcaldía San Martín

No.	**Evaluación de Efectividad de controles**			
	Dominio	**Calificación Actual**	**Calificación Objetivo**	**Evaluación de efectividad de control**
A.5	Políticas de seguridad de la información	20	100	Inicial
A.6	Organización de la seguridad de la información	16	100	Inicial
A.7	Seguridad de los recursos humanos	20	100	Inicial
A.8	Gestión de activos	16	100	Inicial
A.9	Control de acceso	6	100	Inicial
A.10	Criptografía	0	100	Inexistente
A.11	Seguridad física y del entorno	0	100	Inexistente
A.12	Seguridad de las operaciones	0	100	Inexistente
A.13	Seguridad de las comunicaciones	0	100	Inexistente
A.14	Adquisición, desarrollo y mantenimiento de sistemas	0	100	Inexistente
A.15	Relaciones con los proveedores	20	100	Inicial
A.16	Gestión de incidentes de seguridad de la información	0	100	Inexistente
A.17	Aspectos de seguridad de la información de la gestión de la continuidad del negocio	7	100	Inicial
A.18	Cumplimiento	20	100	Inicial

PROMEDIO EVALUACIÓN DE CONTROLES	**9**	**100**	**Inicial**

Fuente: Elaboración propia

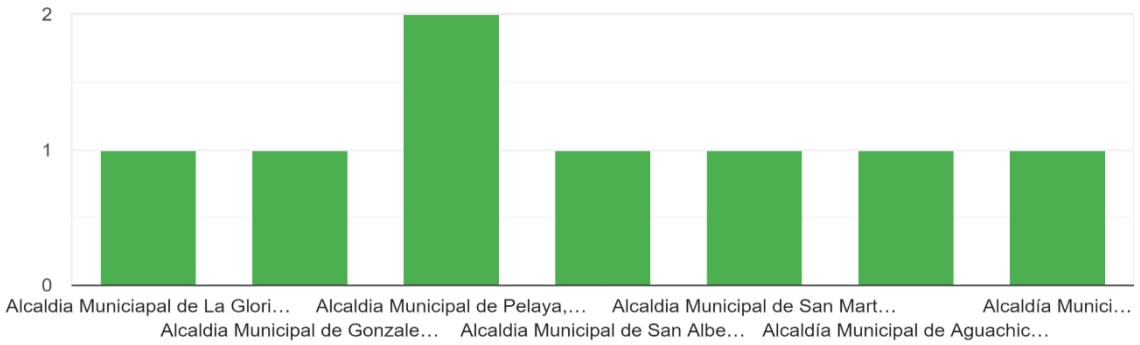
Figura 8. Brecha ISO 2701:2013 Alcaldía San Martín

Fuente: Elaboración propia.

Al aplicar la lista de verificación, puede concluirse que la Alcaldía de San Martín se encuentra en la fase inicial de implementación, queriendo decir esto que hay una evidencia de que la organización ha reconocido que existe un problema y que hay que tratarlo. Sin embargo, aún no cuenta con procesos estandarizados, asimismo, la implementación de un control depende de cada individuo y es principalmente reactiva.

Dentro de las encuestas aplicadaas a las administraciones municipales, se puede obervar el diligenciamiewnto del respectivo intrumento de recoleccion de informacion.

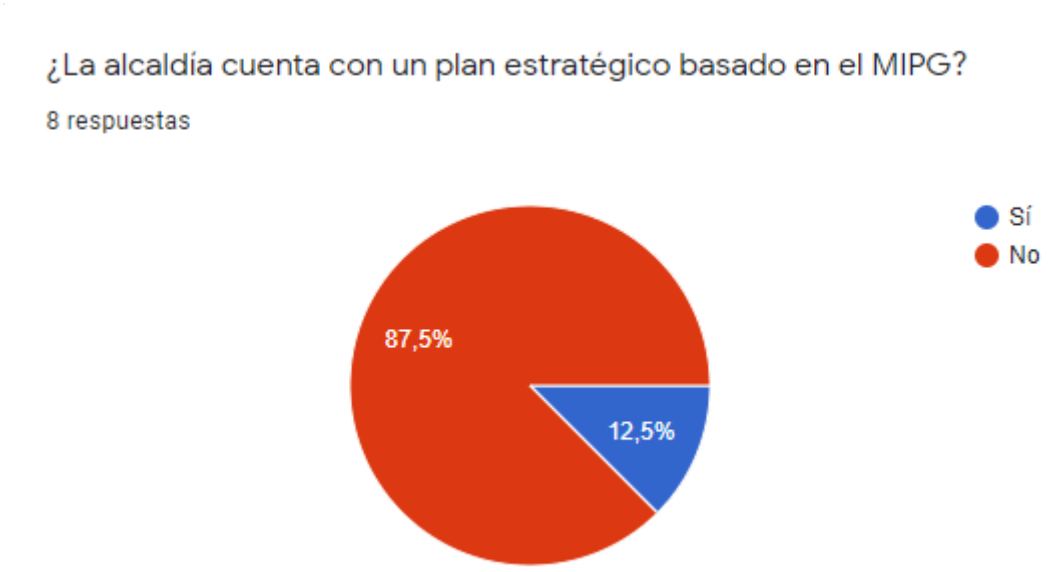
Figura 9. Consolidado Municipios de Sexta categoría.



Fuente: Elaboración propia.

Se observo que dentro de las administraciones municipales del sur del departamento del cesar, el 87,5% de dichas alcaldias en la actualidad no cuenta con un plan estrategico basado en el modelo integrado de planeacion y gestion; y tan solo el 12,5% han alineado la administracion el modelo antes mencioado.

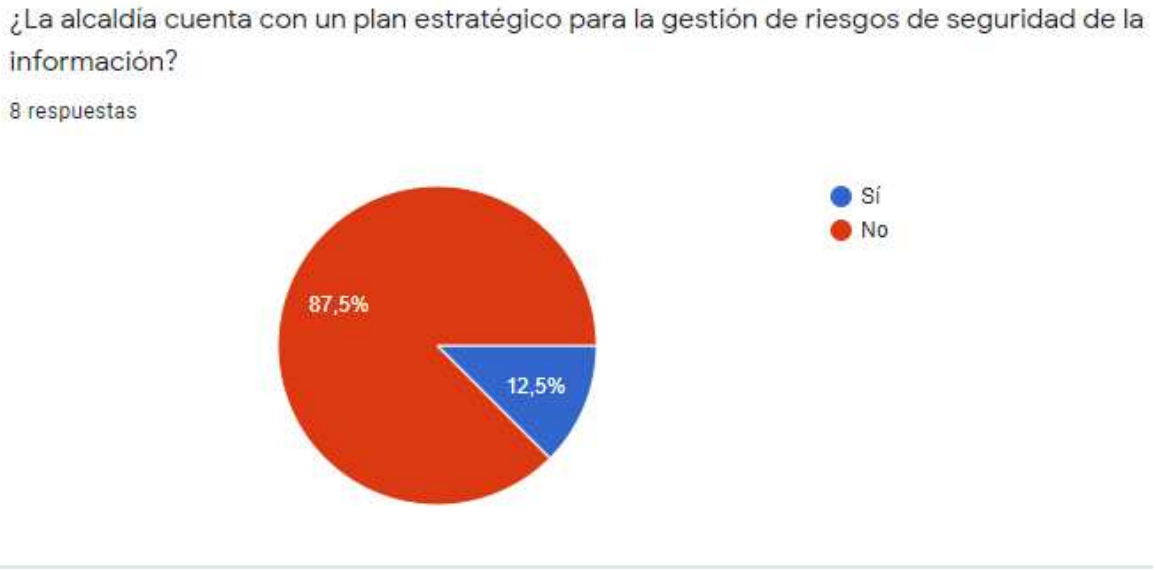
Figura 9. Plan estratégico.



Fuente: Elaboración propia

Se observo que dentro de las administraciones municipales del sur del departamento del cesar, el 87,5% de dichas alcaldias en la actualidad no cuenta con un plan estrategico para la gestion de riesgos de seguridad de la informacion; y tan solo el 12,5% han alineado la administracion el modelo antes mencioado.

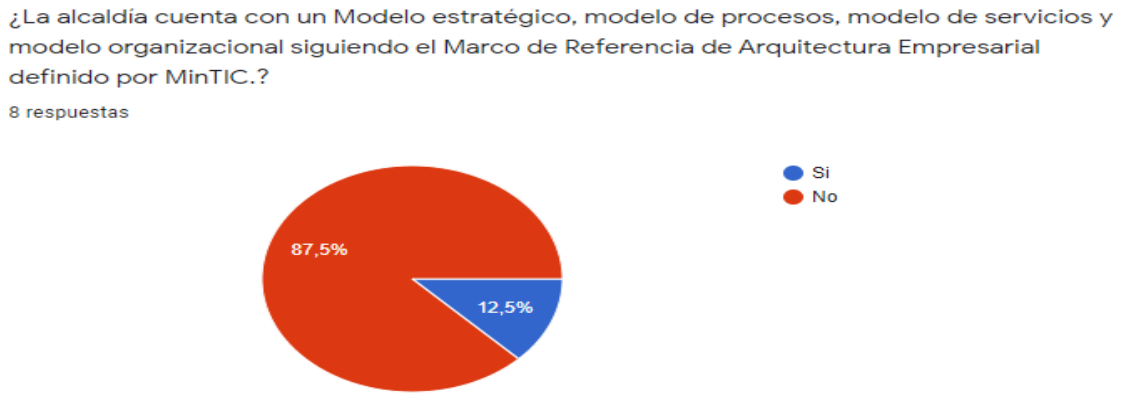
Figura 10. Plan estratégico de gestión de riesgos.



Fuente: Elaboración propia.

Se observo que dentro de las administraciones municipales del sur del departamento del cesar, el 87,5% de dichas alcaldias en la actualidad no se encuentran alineados a ningun marco de referecia de la politica de gobierno digital; y tan solo el 12,5% han alineado la administracion el modelo antes mencioado.

Figura 11. Plan estratégico.



Fuente: Elaboración propia.

Se observo que dentro de las administraciones municipales del sur del departamento del cesar, el 50% de dichas alcaldias en la actualidad no conocen la estrategia IT4+ del Gobierno Nacional tan solo el 37,5% lo ha conoce y el 12,5% tal vez conozca la estrategia que esta dirigida a la institucones del orden publico.

Figura 12. Modelo IT4+.

Estrategia IT4+

Fuente: Elaboración propia.

Se observo que dentro de las administraciones municipales del sur del departamento del cesar, que dentro de las alcaldias ninguna ha implmenentado el modelo de seguridad y privacidad de la informacion.

Figura 13. MSPI.

Fuente: Elaboración propia.

Se observo que dentro de las administraciones municipales del sur del departamento del cesar, tan solo el 12,5% tiene definido un rubro para la aplicación de la politica de gobierno digital y el 87,5% de las administraciones no cuentan con un presupuesto asignado para dicha politica.

Figura 14. Presupuesto para la implementación de gobierno digital.

Fuente: Elaboración propia.

Se observo que dentro de las administraciones municipales del sur del departamento del cesar, el tan solo el 12,5 cuentan con el plan estrategico de tecnologias de la informacion PETI y el 87,5% no han ni siquiera diseñado el plan de adquisicion de Tecnologia.

Figura 15. PETI.

Fuente: Elaboración propia.

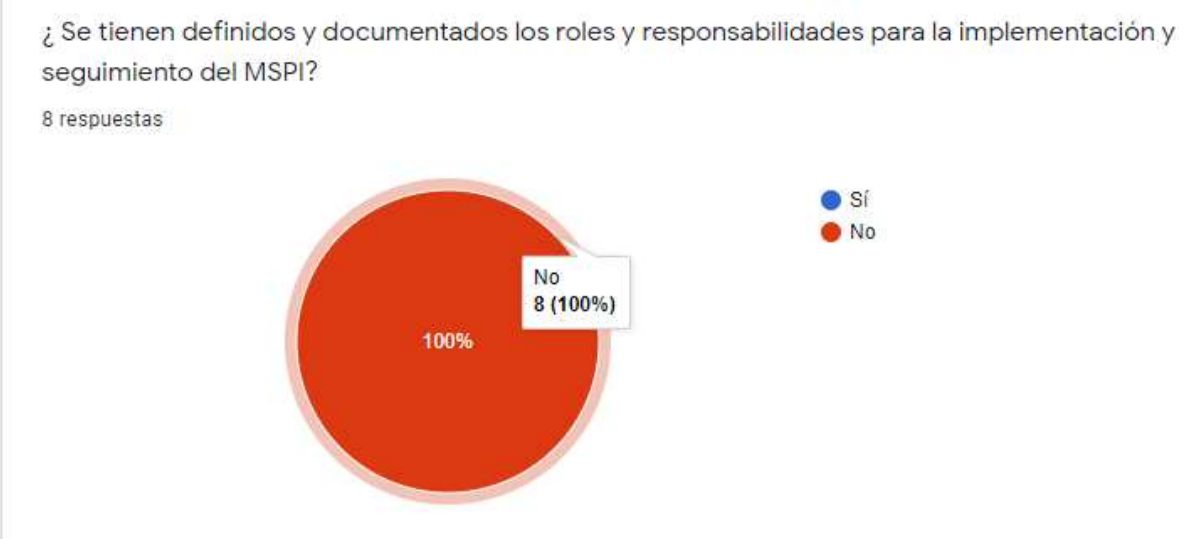
Se observó que en 75% de las administraciones municipales del sur del departamento del cesar no cuentan con un acto administrativo en donde se soporte la creación del comité de gestión de desempeño, tan solo el 25% de los municipios cuentan con dicho comité.

Figura 16. Actos administrativos de gobierno digital.

Fuente: Elaboración propia

Se observo que el 100% de las administraciones municipales del sur del departamento del Cesar, aun no tienen definidos ni documentados los roles y responsabilidades para la implementación del modelo.

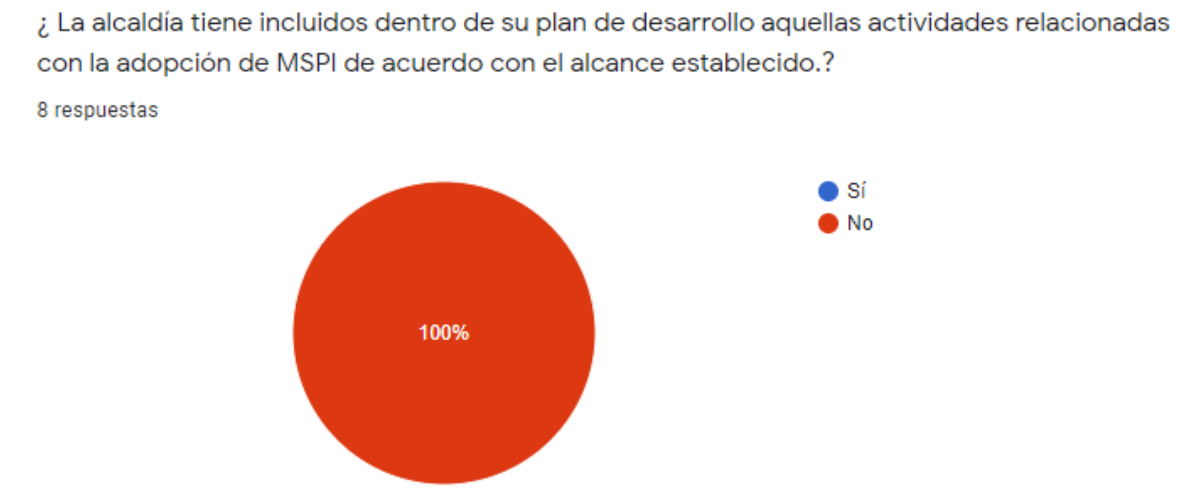
Figura 17. Roles y responzabilidades.



Fuente: Elaboración propia

Se observó que dentro del 100% de los planes de desarrollo 2020-2023 dentro de sus líneas estratégicas no contemplaron acciones encaminadas a la adopción del MSPI y política de Gobierno en Línea.

Figura 17Adopcion del MSPI



Fuente: Elaboración propia

Se observo que dentro de las administraciones municipales actualmente el 100% no cuentan con plan de capacitaciones en lo relacionado políticas de seguridad de la información.

Figura 18. Campañas de sensibilización

Fuente: Elaboración propia

Una vez evaluada cada una de las alcaldías, se presenta un resumen del estado actual del sistema para cada una:

Tabla 17. Resumen diagnóstico

Alcaldía	Etapa en la que se encuentra el sistema de seguridad de la información	Puntaje
Aguachica	Inexistente	0/100
Gamarra	Inicial	2/100
Gonzales	Inicial	3/100
La Gloria	Inicial	4/100
Pelaya	Inicial	12/100
Río de Oro	Inicial	5/100

San Alberto	Inicial	4/100
San Martín	Inicial	9/100

Fuente: Elaboración propia

Puede apreciarse que en general, las alcaldías no cuentan con un sistema de seguridad de la información maduro, una de las alcaldías se encuentra en la etapa donde el sistema se diagnostica como inexistente y las demás se encuentran en la etapa inicial con una puntuación baja. Dado lo anterior, estas entidades requieren definir planes de trabajo que contribuyan a cerrar las brechas para dar cumplimiento a los requerimientos normativos frente a la seguridad de la información.

6.2 Análisis de los componentes del modelo gobierno TI con base en los requerimientos normativos.

De acuerdo al proyecto de grado denominado "Modelo de Integración entre MECI y un marco de referencia para Gobierno de TI aplicado a entidades territoriales municipales en Colombia", de la Universidad ICESI de Cali, las entidades territoriales requieren desarrollar su misión social y para esto se requiere el apoyo de TI, pero es necesario contar con objetivos de TI asociados y alineados con el objetivo de las entidades. Es por eso que las ventajas que tienen las Entidades Públicas al implementar un buen Gobierno de TI son las siguientes:

- Ayuda a la gestión de los programas de TI en el trabajo hacia una estructura y un proceso como medio para demostrar la rendición de cuentas y el cumplimiento de la legislación, políticas, procedimientos y estrategias y requerimientos del sector público.
- Fortalece las Actividades de Control y los Controles asociados a TI.
- Proporciona oportunidades para ofrecer un Mejor servicio a la Ciudadanía.
- Integra los planes de TI y los Proyectos a la Estrategia Pública.
- Ofrece información más oportuna y de mayor calidad.
- Entrega proyectos de mejor calidad y más exitosos.
- Los costos totales del ciclo de vida de TI serán más transparentes y predecibles.
- Los requisitos de seguridad y privacidad serán más claros y la implementación será monitoreada con mayor facilidad.

- Los riesgos de TI serán gestionados con mayor eficacia.
- Las auditorías serán más eficientes y exitosas.
- El cumplimiento de TI con los requisitos regulatorios serán una práctica normal de gestión.

6.2.1 MECI.

El Manual de Implementación Modelo Estándar de Control Interno para el Estado Colombiano - MECI 1000:2005 - del DAFP, indica que la Constitución Política de 1991 incorporó el concepto del Control Interno como un instrumento orientado a garantizar el logro de los objetivos de cada entidad del Estado y el cumplimiento de los principios que rigen la función pública. Por su parte, la Ley 87 de 1993 establece normas para el ejercicio del Control Interno en las entidades y organismo del Estado, y la Ley 489 de 1998 dispuso la creación del Sistema Nacional de Control Interno.

Con el fin de buscar mayor eficacia e impacto del Control Interno en las entidades del Estado, la Contraloría General de la República y el Departamento Administrativo de la Función Pública (DAFP), firmaron un convenio con el propósito de obtener la unificación, adopción e implementación de un modelo de control interno, iniciativa que fue acogida por el Consejo Asesor del Gobierno Nacional en materia de Control Interno, que condujo a la expedición del Decreto 1599 de 2005 “por el cual se adopta el Modelo Estándar de Control Interno MECI 1000:2005”.

Además, en este manual se realiza una definición de MECI y los subsistemas que lo integran entre otros aspectos.

6.2.1.1 Definición.

El Modelo Estándar de Control Interno para el Estado Colombiano – MECI 1000:2005 proporciona la estructura básica para evaluar la estrategia, la gestión y los propios mecanismos de evaluación del proceso administrativo, y aunque promueve una estructura uniforme, se adapta a las necesidades específicas de cada entidad, a sus objetivos, estructura, tamaño, procesos y servicios que

suministran.

6.2.1.2 *Subsistemas.*

El propósito esencial del MECI es orientar a las entidades hacia el cumplimiento de sus objetivos y la contribución de éstos a los fines esenciales del Estado, para lo cual se estructura en tres grandes subsistemas, desagregados en sus respectivos componentes y elementos de control:

Subsistema de Control Estratégico: agrupa y correlaciona los parámetros de control que orientan la entidad hacia el cumplimiento de su visión, misión, objetivos, principios, metas y políticas. Es decir, es el conjunto de Componentes de Control que, al interrelacionarse entre sí, permiten el cumplimiento de la orientación estratégica y organizacional de la entidad pública.

El Subsistema de Control Estratégico tiene como objetivo la creación de una cultura organizacional fundamentada en el control a los procesos de direccionamiento estratégico, administrativos y operativos de la entidad pública.

Alrededor de este objetivo, el Subsistema de Control Estratégico se estructura en tres Componentes: Ambiente de Control, Direccionamiento Estratégico y Administración de Riesgos, orientados a generar los estándares que auto-controlan la entidad en cuanto a la cultura de control, direccionamiento estratégico y organizacional. Estos elementos o estándares de control se relacionan entre sí, lo cual garantiza su operación en forma sistémica.

De allí que, a partir de la función institucional y legal de la entidad, del entendimiento de la misión para la cual fue creada, de su contribución al cumplimiento de los fines del Estado y, con la claridad de las necesidades y expectativas de la ciudadanía y de las partes interesadas a las que debe servir, la entidad debe establecer en forma participativa y consensuada con sus servidores, el estándar de control a la conducta de la organización, de tal forma que se garantice la transparencia, la ética institucional y el buen servicio público que se espera de las entidades del Estado.

Así mismo, permite el diseño de los lineamientos estratégicos que contribuyen a crear un

ambiente favorable al control, la forma de operación con base en una gestión orientada a procesos, administrando el riesgo del no cumplimiento de sus objetivos y fines constitucionales y legales.

Los componentes y elementos de este Subsistema intervienen toda la entidad y la preparan para una gestión eficiente, eficaz, efectiva y transparente en la prestación de los servicios y/o producción de los bienes que le son inherentes.

Subsistema de Control de Gestión: reúne e interrelaciona los parámetros de control de los aspectos que permiten el desarrollo de la gestión: planes, programas, procesos, actividades, procedimientos, recursos, información y medios de comunicación. Es decir, es el conjunto de Componentes de Control, que al interrelacionarse bajo la acción de los niveles de autoridad y/o responsabilidades correspondientes, aseguran el control a la ejecución de los procesos de la entidad pública, orientándola a la consecución de los resultados y productos necesarios para el cumplimiento de su Misión.

Es el segundo Subsistema que se debe implementar para contar con el Modelo Estándar de Control Interno, dado que permite a la entidad construir los elementos o estándares de control necesarios para auto-controlar el desarrollo de las operaciones, tomando como base los estándares de carácter estratégico definidos con base en los lineamientos del Subsistema de Control Estratégico.

Este Subsistema está compuesto por elementos o estándares de control que deben ser diseñados, adoptados e integrados a la operatividad del Modelo de Operación, buscando garantizar el cumplimiento de los resultados esperados, fijados mediante el proceso de direccionamiento estratégico de la entidad.

Una vez la entidad cuente con un ambiente organizacional favorable al control, establezca la orientación estratégica de su accionar y los mecanismos básicos de protección de sus recursos es preciso definir, diseñar y correlacionar las acciones, funciones, flujos de información y de comunicación, tendientes a garantizar la alineación de la operación de la entidad con sus propósitos institucionales, permitiendo su contribución a los fines esenciales del Estado.

De allí que sea necesario establecer las reglas, acciones, métodos, procedimientos e instrumentos necesarios en la entidad que le aseguren el cumplimiento de las metas y objetivos previstos, a través de tres Componentes, a saber: Actividades de Control, Información y Comunicación Pública.

Subsistema de Control de Evaluación: agrupa los parámetros que garantizan la valoración permanente de los resultados de la entidad, a través de sus diferentes mecanismos de verificación y evaluación. Este enfoque concibe el Control Interno como un conjunto de elementos interrelacionados, donde intervienen todos los servidores de la entidad y le permite estar siempre atenta a las condiciones de satisfacción de los compromisos contraídos con la ciudadanía, garantiza la coordinación de las acciones y la fluidez de la información y comunicación, y anticipa y corrige, de manera oportuna, las debilidades que se presentan en el quehacer institucional. Es decir, conjunto de Componentes de Control que al actuar inter-relacionadamente, permiten valorar en forma permanente la efectividad del Control Interno de la entidad pública; la eficiencia, eficacia y efectividad de los procesos; el nivel de ejecución de los planes y programas, los resultados de la gestión, detectar desviaciones, establecer tendencias y generar recomendaciones para orientar las acciones de mejoramiento de la Organización Pública.

El Subsistema de Control de Evaluación desarrolla mecanismos de medición, evaluación y verificación, necesarios para determinar la eficiencia y eficacia del Sistema de Control Interno en la realización de su propósito de contribuir al cumplimiento de los objetivos de la entidad; si todas las operaciones se realizan de conformidad con los principios de la función pública establecidos en la Constitución Política, la ley y las políticas trazadas por la dirección en atención a las metas u objetivos previstos.

A partir de los resultados de la evaluación a la efectividad del Sistema de Control Interno, al conjunto de planes, programas, proyectos, objetivos y metas previstas por la entidad, se deben incorporar en la planificación corporativa, acciones de mejoramiento continuo de la organización, así como las recomendaciones producto de la vigilancia que realiza el órgano de control fiscal.

La Constitución Política establece que la función del control fiscal la ejerce la Contraloría General de la República, la cual vigila la gestión fiscal de la Administración Pública y de los

particulares o entidades que manejen fondos de la Nación.

Las deficiencias encontradas y las recomendaciones sugeridas en las diferentes instancias de evaluación, incluyendo las emitidas por los órganos de control del Estado, deben ser acogidas por el servidor responsable y/o por el nivel de administración o dirección correspondiente. El Subsistema se estructura bajo tres Componentes: *Autoevaluación, Evaluación Independiente*, *Planes de Mejoramiento*.

En términos generales, los Subsistemas de MECI, sus componentes y sus elementos se pueden resumir en la siguiente figura:

Figura 2. Modelo estándar de control interno

6.2.2 Gobierno en línea.

En el mundo se están produciendo una serie de cambios en la manera en que operan los Estados y en su responsabilidad frente a la sociedad, lo cual ha exigido que la búsqueda de la eficiencia, eficacia, visibilidad y publicidad, sigan siendo un gran imperativo, no solo en temas asociados con la gestión interna de las entidades, sino en la solución de problemas relacionados con el desempleo, la pobreza, la salud, el medio ambiente, y en general, todos aquellos asociados con la actividad estatal y la satisfacción de necesidades y mejora en la calidad de vida.

Del mismo modo, el rol de los ciudadanos también ha venido transformándose, las formas de expresión son diversas y se basan en mecanismos más directos y más poderosos, la mayoría apoyados en el uso de las Tecnologías de la Información y las Comunicaciones-TIC. La ciudadanía tiene un conocimiento importante que puede ser aprovechado en beneficio de las sociedades y el Estado puede servir de plataforma para canalizar y potenciar dicho conocimiento. Asimismo, son los ciudadanos los beneficiarios directos de las políticas públicas y de la toma de decisiones, lo que hace cada vez más imperante involucrarlos activamente en su construcción y validación.

En cuanto a la industria de la tecnología, los avances también son vertiginosos, no solo en lo que respecta al desarrollo de aplicaciones o servicios, también en lo relacionado con la gestión de la tecnología al interior de las organizaciones, hecho que ha transformado los procesos y actividades del mismo Estado.

En este contexto, la Estrategia de Gobierno en línea permite potenciar los cambios que se han presentado en la forma de operar de las naciones, aprovechando los avances de la tecnología para garantizar una mejor comunicación e interacción con la ciudadanía, que permita además la prestación de más y mejores servicios por parte del Estado, dando respuesta satisfactoria a los siguientes interrogantes:

Figura 3. Interrogantes de la estrategia de Gobierno en Línea

Fuente: http://programa.gobiernoenlinea.gov.co/apc-aa-

El desarrollo del Gobierno En Línea debe asumirse como un proceso evolutivo, que comprende cinco fases: Información, Interacción, Transacción, Transformación y Democracia en Línea oe-Democracia.

6.2.2.1 La Estrategia Gobierno en línea en Colombia y su evolución.

Conscientes de que la administración pública colombiana NO puede quedarse atrás de los avances tecnológicos, especialmente cuando contribuyen a mejorar la transparencia y eficiencia en la gestión estatal, desde finales del siglo XX el Gobierno Nacional ha promulgado diversas directrices que han impulsado y guiado a las instituciones del Estado en la incorporación efectiva de las TIC en su operación.

La política pública de Gobierno en línea en Colombia que inició en el año 2000 con la directiva presidencial 02 de dicho año y continuó de manera decidida desde el 2008 con la expedición del Decreto 1151 que definió los lineamientos generales de la Estrategia de Gobierno en línea, ha evolucionado de forma permanente en el país, tanto en su alcance hacia un mayor número de entidades, como en su implementación por parte de las mismas, pues cada vez más las Tecnologías de la Información y las Comunicaciones se han convertido en una herramienta por excelencia para mejorar la gestión de lo público y la relación Estado-ciudadano. Es así como la Estrategia de Gobierno en línea es considerada un eje estratégico del Buen Gobierno, porque

procura un Estado más eficiente, más transparente y participativo que preste mejores servicios con la colaboración de toda la sociedad.

La implementación de esta Estrategia en Colombia por el conjunto de entidades públicas ha generado logros muy importantes tales como el incremento en la provisión de trámites y servicios por medios electrónicos, la mejora en la calidad de la información de las entidades públicas en sus sitios web y la apertura de espacios de participación, entre otros. Gracias al Gobierno en línea, los colombianos tienen acceso a la información pública en los sitios web del Estado, lo cual incluye a entidades de todas las ramas del poder público del orden nacional y al 100% de los municipios y departamentos de Colombia. Asimismo, el país ha mejorado en las mediciones internacionales, relacionadas con la implementación de servicios en línea y en participación electrónica13.

Considerando estos avances y también los nuevos retos que impone la evolución de la misma sociedad en temas tales como el gobierno abierto, la multicanalidad, la conciencia del ambiente, la seguridad, cambios normativos subyacentes, el ciudadano como centro de la gestión pública, entre otros. La Estrategia de Gobierno en línea liderada por el Ministerio de Tecnologías de la Información y las Comunicaciones- Ministerio TIC, en coordinación con el Departamento Administrativo de la Función Pública, el Departamento Nacional de Planeación y la Alta Consejería para el Buen Gobierno y la Eficiencia Administrativa, inició un proceso de evolución hacia un nuevo modelo que exige a las entidades esfuerzos cada vez mayores que permitan, no solo aumentar el número y uso de servicios en línea, sino también mejorar la calidad y el acceso a los mismos, así como el acceso a mayor información y datos, y que permita el involucramiento de forma directa de los demás actores de la sociedad en su construcción. Todo lo anterior a través del uso eficiente de las TIC para el cumplimiento de los objetivos del Gobierno Nacional de: disminuir pobreza, aumentar seguridad y aumentar empleo.

De igual manera la implementación del nuevo modelo de Gobierno en línea implica para las entidades la alineación de actividades con otros temas esenciales de la gestión pública en Colombia, como lo son: la Política Anti trámites, la Política Nacional del Servicio al Ciudadano,

la Política de Rendición de Cuentas a la Ciudadanía, la Política Nacional Anticorrupción, la Política Nacional de Archivo y Gestión Documental, entre otras.

6.2.2.2 *El nuevo modelo de Gobierno en línea: la Estrategia se renueva de cara al futuro.*

De conformidad con los nuevos retos que se deben abordar, la Estrategia Gobierno en línea se renueva y proyecta la siguiente visión a 2015 para las entidades de nivel nacional, y para el 2016 y 2017 para las entidades de nivel territorial:

En el año 2015 la ciudadanía en general tendrá acceso de forma oportuna a más y mejor información bajo un esquema de comunicación en doble vía y de rendición de cuentas permanente y en tiempo real, lo cual permitirá una mejor participación en el proceso de toma de decisiones y un mejor ejercicio del control social. De igual forma, la ciudadanía no tendrá la necesidad de hacer filas ni asistir personalmente a las entidades para llevar a cabo sus trámites y recibir los servicios del Estado, generando una relación más fácil, con menores costos y que genere mayor confianza y satisfacción.

Lo anterior será logrado gracias a que las entidades se habrán transformado en entidades digitales abiertas, pues habrán incorporado las TIC de forma transversal en su operación tradicional, transformando su funcionamiento interno y la relación con sus usuarios.

Para esto las entidades contarán con sedes electrónicas, en donde se dispondrá de acceso multicanal a toda la información, así como a la gestión en línea de trámites y servicios, observando permanentemente las condiciones de accesibilidad, usabilidad, calidad, seguridad, reserva y privacidad.

Igualmente, se habrá creado una cultura de colaboración y participación, en donde se intercambiará activamente información por medios electrónicos entre entidades, se construirán políticas y estrategias con la participación electrónica de actores clave, y existirán las condiciones para que terceros creen nuevos servicios que generan valor a la ciudadanía. Asimismo, la entidad habrá reducido al menos el 30% de su consumo de papel a la vez que aumentará su eficiencia debido a la optimización y uso de medios electrónicos en sus procesos y procedimientos.

Lo anterior estará sustentado en el conocimiento de las necesidades de los usuarios, la adopción de nuevas tendencias tecnológicas y la implementación de buenas prácticas, generando así un esquema de innovación y mejoramiento permanente.

Para el logro de la visión y de los objetivos del Gobierno en línea, el Ministerio TIC desde la expedición del Decreto 1151 de 2008 ha venido publicando los Manuales para la Implementación de la Estrategia de Gobierno en línea, los cuales son concebidos como herramientas de autoayuda, que buscan proporcionar a las entidades públicas de las diferentes ramas y niveles, y a los privados que ejercen funciones administrativas, el enfoque, lineamientos y herramientas de apoyo que faciliten sus avances y mejoras, ya sea a través de las directrices incluidas en el mismo o mediante documentos complementarios a los que se hace referencia en el Manual.

En el año 2018, con el objeto de impulsar el Gobierno en línea, se ha definido un nuevo método a seguir por parte de las entidades, el cual está compuesto por 6 componentes que agrupan definidos en el Decreto 2693 de 2012 que se derivan de la evolución. Actividades que deben ser implementadas por las entidades para avanzar en la implementación de la Estrategia. Dichos componentes están enfocados en los ciudadanos y/o usuarios, quienes determinan la calidad de la información y servicios que el Estado presta y habilita.

6.2.2.3 *Componentes.*

Los componentes de la Estrategia de Gobierno en línea definidos en el Decreto 2693 de 2012 que se derivan de la evolución de las "Fases de Gobierno en línea" contempladas en el Decreto 1151 de 2008, se adiciona un nuevo componente que contempla temas y actividades transversales, así:

Elementos Transversales:

Comprende las actividades que deben implementar las entidades para conocer sus diferentes

grupos de usuarios, identificar sus necesidades e investigar permanentemente sobre los cambios en las tendencias de comportamiento, para aplicar este conocimiento a sus diferentes momentos de interacción. De igual forma, se promueve que las entidades cuenten con una caracterización actualizada de la infraestructura tecnológica y establezcan un plan de ajuste permanente.

En este componente también se describen actividades orientadas a que cada entidad cuente con una política de seguridad que es aplicada de forma transversal y mejorada constantemente; y que se garantice la incorporación del Gobierno en línea como parte de la cultura organizacional y elemento de soporte en sus actividades misionales. Para alcanzar los objetivos de este componente, las entidades deberán desarrollar las siguientes actividades: 1. Institucionalizar la Estrategia de Gobierno en línea; 2. Centrar la atención en el usuario; 3. Implementar un sistema de gestión de Tecnologías de Información; 4. Implementar un sistema de gestión de seguridad de la información (SGSI).

Información en línea:

Comprende todas las actividades a desarrollar para que las entidades dispongan para los diferentes tipos de usuarios de un acceso electrónico a toda la información relativa a su misión, planeación estratégica, trámites y servicios, espacios de interacción, ejecución presupuestal, funcionamiento, inversión, estructura organizacional, datos de contacto, normatividad relacionada, novedades y contratación, observando las reservas constitucionales y de Ley, cumpliendo todos los requisitos de calidad, disponibilidad, accesibilidad, estándares de seguridad y dispuesta de forma tal que sea fácil de ubicar, utilizar y reutilizar. Las actividades de este componente están concentradas principalmente en dos aspectos: 1. Publicación de información y 2. Publicación de datos abiertos.

Interacción en línea:

Comprende todas las actividades para que las entidades habiliten herramientas de comunicación de doble vía entre los servidores públicos, organizaciones, ciudadanos y empresas. Igualmente, este componente promueve la habilitación de servicios de consulta en línea y de otros mecanismos que acerquen a los usuarios a la administración pública, que les posibiliten contactarla y hacer uso de la

información que proveen las entidades por medios electrónicos. Las actividades están concentradas en dos aspectos: 1. Habilitar espacios electrónicos para interponer peticiones y 2. Habilitar espacios de interacción.

Transacción en línea:

Comprende todas las actividades para que las entidades dispongan sus trámites y servicios para los diferentes tipos de usuarios, los cuales podrán gestionarse por diversos canales electrónicos, permitiéndoles realizar desde la solicitud hasta la obtención del producto sin la necesidad de aportar documentos que reposen en cualquier otra entidad pública o privada que cumpla funciones públicas. Lo anterior haciendo uso de autenticación electrónica, firmas electrónicas y digitales, estampado cronológico, notificación electrónica, pago por medios electrónicos y actos administrativos electrónicos.

La actividad a adelantar por parte de las entidades para dar cumplimiento al Componente de Transacción en línea está relacionada principalmente con la posibilidad del ciudadano de realizar trámites y servicios en línea, lo cual implica: 1. Formularios para descarga y/o diligenciamiento en línea, 2. Expedición en línea de certificaciones y constancias, 3. Automatización de trámites y servicios, 4. Ventanillas Únicas Virtuales, 5. Pagos en línea, 6. Uso de firmas electrónicas y digitales, entre otros.

Democracia en línea:

Comprende todas las actividades para que las entidades creen un ambiente para empoderar a los ciudadanos e involucrarlos en el proceso de toma de decisiones. Con estas actividades se propicia que el ciudadano participe activa y colectivamente en la toma de decisiones de un Estado totalmente integrado en línea. Igualmente, se promueve que las entidades públicas incentiven a la ciudadanía a contribuir en la construcción y seguimiento de políticas, planes, programas, proyectos, la toma de decisiones, el control social y la solución de problemas que involucren a la sociedad en un diálogo abierto de doble vía.

Este componente establece las indicaciones para que las entidades lleven a cabo sus ejercicios de participación en línea a través de un proceso ordenado y de realimentación permanente tanto al interior, como hacia sus ciudadanos y/o usuarios. Son 4 los grupos de actividades de democracia en línea

que se desarrollan en este componente: 1. Definir la estrategia de participación; 2. Construir de forma participativa las políticas y planeación estratégica; 3. Abrir espacios para el control social; 4. Abrir espacios de innovación abierta.

6.2.3 Cómo implementar el nuevo modelo de Gobierno en línea.

Planeación y plazos:

La Estrategia de Gobierno en Línea debe ser incorporada por parte de las entidades de forma transversal dentro de sus planes estratégicos sectoriales e institucionales, y anualmente dentro de los planes de acción, en donde se deben definir las actividades, responsables, metas y recursos presupuestales que les permitan dar cumplimiento a los lineamientos que se establecen en el Decreto de Gobierno en línea, en los Manuales para la implementación de la Estrategia y en el presente documento. En este sentido, el Gobierno en línea se encuentra incluido en Modelo Integrado de Planeación y Gestión como una herramienta dinamizadora para el cumplimiento de las metas de las Políticas de Desarrollo Administrativo, las cuales permiten enmarcar el quehacer misional y el de apoyo, tomando como referentes las metas de Gobierno establecidas en el Plan Nacional de Desarrollo y las competencias normativas asignadas a cada entidad.

Para orientar la planeación de la Estrategia de Gobierno en línea en cada sector, departamento y entidad, el Ministerio de Tecnologías de la Información y las Comunicaciones ha definido pesos ponderados para cada una de las actividades contenidas en los Componentes de la Estrategia antes enunciados, según la importancia o complejidad para su desarrollo. Igualmente ha establecido unos plazos para la implementación de la Estrategia y unos porcentajes mínimos de avance para los diferentes grupos de entidades que conforman la administración pública, desde el año 2013 hasta el año 2015 para entidades del orden nacional y desde el año 2013 hasta el año 2017 para entidades del orden territorial. Estas actividades y respectivos pesos están plasmadas en la versión 3.1 del Manual para la Implementación de la Estrategia de Gobierno en línea.

Los plazos para la implementación de la Estrategia establecidos en el Decreto 2693 de 2012 de Gobierno en línea son los siguientes:

a) Para entidades del orden nacional:

	Información en línea	Interacción en línea	Transacción en línea	Transformación	Democracia en línea	Transversales
2013	80%	80%	70%	70%	80%	75%
2014	95%	95%	95%	95%	95%	95%
2015	100%	100%	100%	100%	100%	100%

Fuente: http://programa.gobiernoenlinea.gov.co/apc-aa-

b) Para gobernaciones de categoría especial y primera; alcaldías de categoría especial, la administración pública y demás sujetos obligados en el mismo orden.

	Información en línea	Interacción en línea	Transacción en línea	Transformación	Democracia en línea	Transversales
2013	50%	60%	30%	20%	55%	50%
2014	80%	70%	70%	45%	80%	75%
2015	95%	95%	95%	90%	95%	95%
2016	100%	100%	100%	100%	100%	100%

Fuente: http://programa.gobiernoenlinea.gov.co/apc-aa-

c) Para gobernaciones de categoría segunda, tercera y cuarta; alcaldías de categoría primera, segunda y tercera, la administración pública y demás sujetos obligados en el mismo orden.

	Información en línea	Interacción en línea	Transacción en línea	Transformación	Democracia en línea	Transversales
2013	40%	25%	15%	15%	40%	35%
2014	55%	60%	35%	40%	65%	60%
2015	80%	75%	70%	70%	85%	85%
2016	100%	100%	100%	100%	100%	100%

Fuente: http://programa.gobiernoenlinea.gov.co/apc-aa-

d) Para alcaldías de categoría cuarta, quinta y sexta, la administración pública y demás sujetos obligados en el mismo orden.

	Información en línea	Interacción en línea	Transacción en línea	Transformación	Democracia en línea	Transversales
2013	40%	25%	15%	15%	40%	35%
2014	55%	50%	35%	35%	65%	60%
2016	80%	75%	70%	60%	95%	85%
2017	100%	100%	100%	100%	100%	100%

Fuente: http://programa.gobiernoenlinea.gov.co/apc-aa-

6.2.4 Monitoreo y Evaluación.

Las entidades públicas deben adelantar las acciones pertinentes para realizar el monitoreo y evaluación del cumplimiento de la Estrategia de Gobierno en línea, igualmente deberán adelantar las mediciones de impacto del uso y beneficio del Gobierno en línea en sus usuarios y/o ciudadanos, lo anterior de acuerdo con las metodologías y lineamientos respectivos definidos por el Ministerio TIC. Asimismo, y como complemento a la tarea de autoevaluación realizada por cada entidad, el Ministerio TIC adelantará acciones que permitan medir el avance en la implementación de la

Estrategia de Gobierno en línea, así como el uso, calidad e impacto de la prestación de los más importantes trámites y servicios en línea del Estado colombiano.

Como resultado de este proceso de monitoreo y evaluación adelantado por cada entidad y por el Ministerio TIC, el Ministerio publicará periódicamente el Índice de Gobierno en línea, instrumento cuantitativo que mide el estado de avance de las entidades en la implementación de la Estrategia Gobierno en línea, teniendo como referencia los criterios definidos en el Manual para la Implementación de la Estrategia de Gobierno en línea.

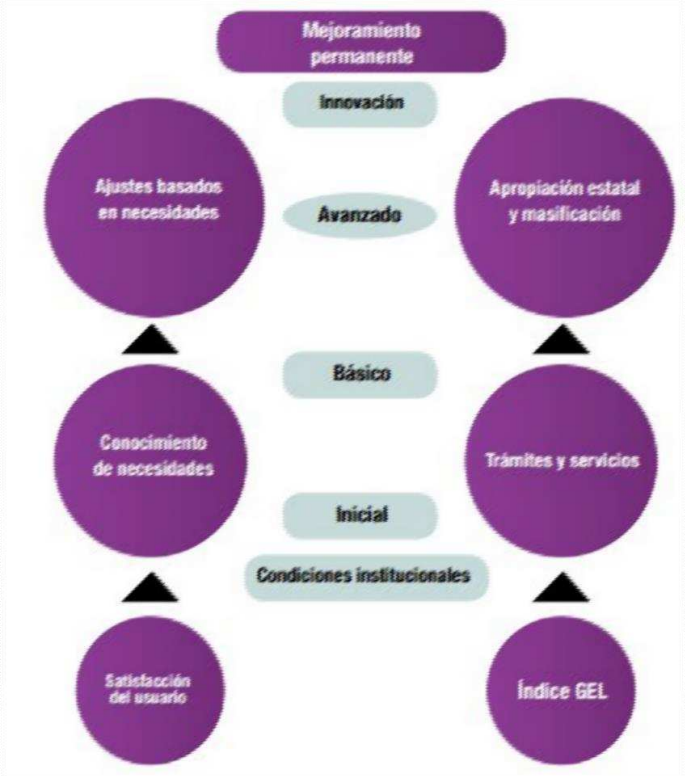
El Índice de Gobierno en línea se calcula de la sumatoria de los pesos ponderados de cada uno de los diferentes criterios definidos en el Manual, los cuales están agrupados en los 6 componentes del nuevo modelo de Gobierno en línea y contemplan elementos de insumos, procesos y resultados que al sumarse completan 100 puntos por componente. Los resultados de cada componente, a su vez, se ponderan para obtener un resultado agregado total sobre 100 puntos, puntaje que se denomina Índice de Gobierno en línea.

Adicional a este Índice, el Ministerio TIC y las entidades podrán identificar el grado de madurez en la implementación de lo establecido en los Manuales de Gobierno en línea, los cuales están determinados por el cumplimiento de la implementación de la Estrategia, así como por la obtención de resultados, y la generación de impacto y beneficios para los ciudadanos y usuarios. Los niveles de madurez que se enuncian a continuación se definen como un estado de evolución de la implementación de la Estrategia y sirven como referente para establecer el avance en términos generales en cada uno de los componentes:

Figura 4. Descripción de los niveles de madurez de la estrategia de Gobierno en Línea

Fuente: http://programa.gobiernoenlinea.gov.co/apc-aa-

Figura 5. Niveles de madurez de la Estrategia Gobierno en ***línea***

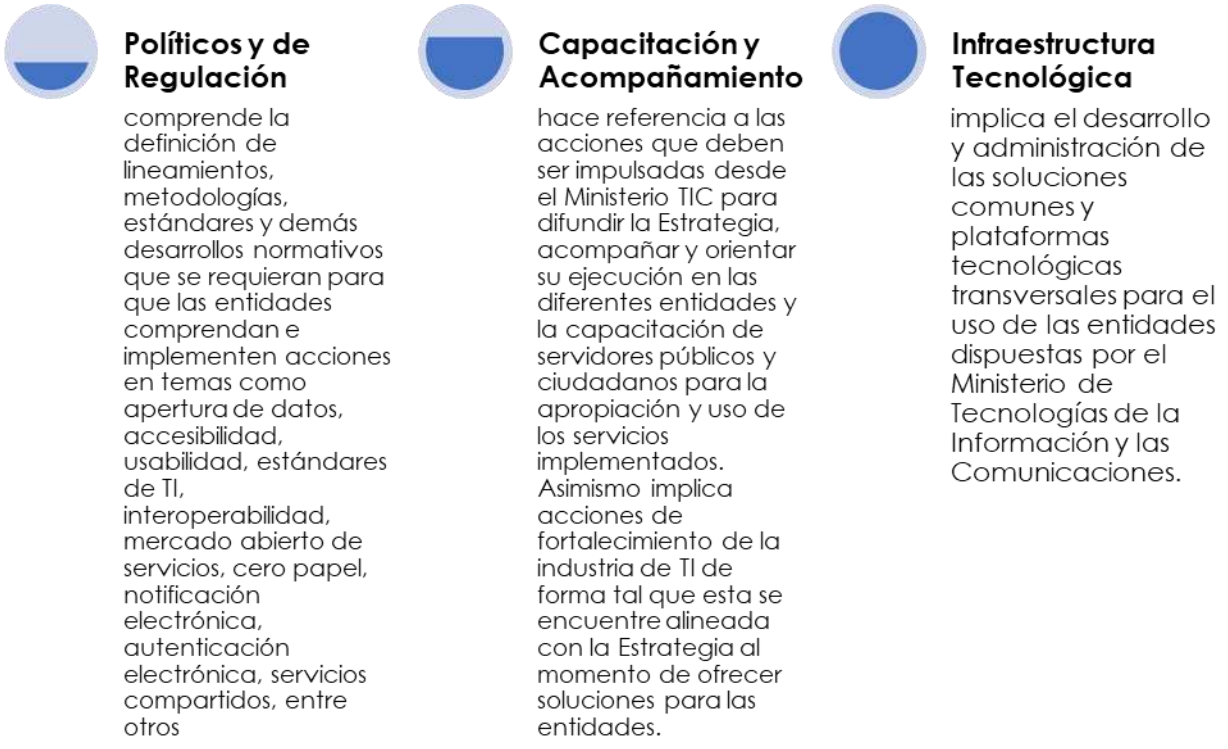


Fuente: http://programa.gobiernoenlinea.gov.co/apc-aa-

6.2.5 Herramientas de apoyo para implementar Gobierno en línea.

El Ministerio TIC liderará e impulsará ciertos elementos habilitantes de la Estrategia, que deberán ser adaptados y posteriormente implementados por las entidades. Dentro de estos elementos habilitantes se encuentran los siguientes:

Figura 6. Regulación del modelo de Gobierno en línea



Fuente: http://programa.gobiernoenlinea.gov.co/apc-aa-

6.3 Modelo de TI orientada a los municipios de sexta categoría del sur del Departamento del Cesar.

6.3.1 Aspectos del Modelo de TI

El modelo que se plante en el presente documento, parte de la interiorización de la naturaleza de las entidades a que va dirigido, puesto que el Gobierno TI, se viene aplicando en muchos países en diferentes sectores de la economía, principalmente en el sector privado que utiliza la Tecnologías de la Información como un mecanismo para aumentar sus utilidades; sin embargo los municipios de sexta categoría del Sur del Departamento del Cesar tienen una particularidad y es que pertenecen al sector público del territorio Colombiano y que por ende estas entidades deben dar cumplimiento a los lineamientos que así definan las autoridades sectoriales, en este caso El Ministerio de Tecnologías de la Información y Comunicación de Colombia MINTIC; quien ha establecido que un modelo de Gobierno para TI debe contener los siguientes aspectos:

- Marco legal y normativo
- Estructura de TI y procesos

6.3.1.1 *Marco legal y normativo.*

Aunque ya se ha revisado este componente anteriormente, con el fin de esclarecer y desarrollar las directrices del MINTIC se considera de gran importancia hacer énfasis en las siguientes normativas que orientan el accionar de las entidades públicas en Colombia, respecto a la Tecnologías de la Información:

- 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 –TIC–. Tiene como uno de sus principios orientadores la masificación del Gobierno en Línea y establece que las entidades públicas deberán adoptar todas las medidas necesarias para garantizar el máximo aprovechamiento de las TIC en el desarrollo de sus funciones.

- Decreto 1078 de 2015, Por medio del cual se expide el Decreto Único

Reglamentario del Sector de Tecnologías de la Información y las Comunicaciones, define en su artículo 2.2.9.1.4.2. sobre la segmentación de entidades en el Manual de Gobierno Digital, la cual deberá realizarse de acuerdo a los criterios diferenciales de los territorios y de las entidades, para adelantar la orientación, implementación, seguimiento y evaluación de la política de gobierno digital.

- Decreto 1414 de 2017**:** por el cual se modifica la estructura del Ministerio de Tecnologías de la Información y las Comunicaciones. Define la estructura que conforma el Ministerio, así como las diferentes funciones que deben realizar para dar cumplimiento a los objetivos propuestos en materia de las TIC.

- Decreto 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. Dicho Decreto define los principios bajo los cuales debe operar el Gobierno en línea, siendo estos: innovación, proactividad, competitividad y seguridad de la información. Asimismo, establece que la Política de Gobierno Digital debe ser evaluada mediante indicadores de cumplimiento y de resultado.

- Ley 1978 de 2019**:** Por la cual se moderniza el Sector de las Tecnologías de la Información y las Comunicaciones -TIC, se distribuyen competencias, se crea un Regulador Único. Uno de los propósitos de esta ley es focalizar las inversiones para el cierre efectivo de la brecha digital y potenciar la vinculación del sector privado en el desarrollo de los proyectos asociados.

- Decreto 1064 de 2020: Por el cual se modifica la estructura del Ministerio de Tecnologías de la Información y las Comunicaciones. Establece los objetivos que tiene el ministerio, entre los que se encuentra diseñar, formular, adoptar y promover las políticas, planes, programas y proyectos del sector de Tecnologías de la Información; y Promover el uso y apropiación de las Tecnologías de la Información y las Comunicaciones entre los ciudadanos, las empresas, el Gobierno.

- Resolución 500 de 2021, cuyo objetivo es establecer los lineamientos generales para la implementación del Modelo de Seguridad y Privacidad de la Información - MSPI, además de la guía de gestión de riesgos de seguridad de la Información y el procedimiento para la gestión de los incidentes de seguridad digital.

6.3.1.2 *Estructura de TI y procesos.*

El Gobierno TI consiste en una estructura de relaciones y procesos orientados a dirigir y controlar la entidad, con la finalidad de alcanzar sus objetivos.

Aunque el MINTIC ha definido algunos lineamientos a través de su política de gobierno digital, se hace necesario realizar un análisis comparativo con otros modelos como es el establecido por la norma internacional ISO 38500, con el fin de identificar puntos de encuentro y diferenciadores que permiten entender con mayor claridad los tipos de desarrollos y exigencias que puede tener el sector empresarial, el sector privado con el sector público (Morales, 2016).

Podría inferirse que el modelo de Gobierno de TI puede ser universal para todas las organizaciones y si bien algunos principios generales pueden converger y determinar acciones compatibles, sus especificidades, sus características únicas obligan a las entidades a adaptar los modelos y sus estructuras de acuerdo a las expectativos, objetivos y metas que se plantea cada una.

6.3.2 Similitudes entre Principios MITIC y principios ISO 38500.

El Modelo de gobierno planteado en la ISO 38500:2015, orienta a las organizaciones públicas o privadas hacía uno uso eficaz de las TI, se basa en tres componentes: a) La Dirección b) La Evaluación y c) el Monitoreo, tal como se muestra en la figura 1 (Mazo Cuenca, 2016):

Figura 19. Modelo de gobierno de la ISO 38500

Fuente: Maza Cuenca (2016)

Por otro lado, la estructura que se ha definido para las entidades del estado en relación con las TI, es una estructura empresarial que busca el fortalecimiento de sus capacidades institucionales y de gestión de TI; a diferencia del modelo de Gobierno planteado por la ISO 38500:2015, este no contempla tácitamente la etapa de monitoreo, pero comparten las etapas de direccionamiento y acción.

Figura *20*. Estructura del Modelo de Gestión y Gobierno de TI

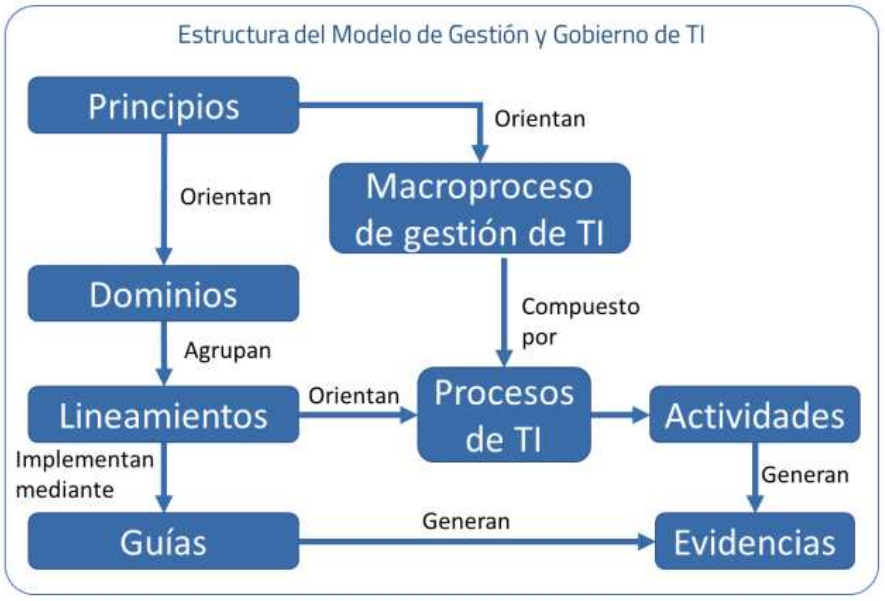


Ilustración 2 Estructura del Modelo de Gestión y Gobierno de TI

Fuente: (MGGTI.G.GEN.01 – Documento Maestro del Modelo de Gestión y Gobierno de TI, 2021)

En cuanto a los principios, se han extraído de ambos documentos algunas definiciones y se realiza un paralelo entre algunos de ellos que comparten similitudes, inicialmente se identifican seis principios más en el modelo de MINTIC (Mintic, 2019).

Tabla 18. Principios de TI ISO 38500 Vs Mintic

ISO 38500	**MINTIC**	**Similitudes**
Responsabilidad: Los individuos y grupos dentro de la organización entienden y aceptan sus responsabilidades en relación con la oferta y la demanda de las tecnologías de la información. Aquellos con responsabilidad también tienen la autoridad para llevar a cabo	Foco en las necesidades: Las decisiones sobre el ecosistema tecnológico deben enfocarse en responder y dar solución las necesidades de la Entidad.	El centro de estos principios es el entendimiento de las entradas y las salidas del sistema de las TI, y la objetividad de quienes tomas las decisiones.

esas acciones		
Estrategia: Toma en cuenta la presente y futuras capacidades de las tics. Los planes necesarios de TIC compensan las necesidades existentes y pronosticadas derivadas de la estrategia de negocio	Co-Creación: Componer soluciones y generar servicios sobre lo ya construido y definido, con la participación de todos los interesados (internos y externos) para garantizar su máximo valor	La estrategia y la co-creación están orientadas a definir soluciones a los problemas o necesidades identificados.
Adquisición: Las adquisiciones de las tecnologías de la información se realizan por razones legales, en base a un análisis apropiado y continuo que involucre decisiones claras. Hay un equilibrio apropiado entre beneficios, conformidades, costes y riesgos ya sea a corto como a largo plazo	Costo / Beneficio: El criterio de selección de un proyecto de TI debe priorizar el valor público por encima de su costo, de tal forma que se garantice que las inversiones en TI tengan un retorno definido por el beneficio. Estandarización: Definir un ecosistema tecnológico estandarizado para controlar la diversidad tecnológica, la complejidad técnica y reducir los costos asociados al mantenimiento de la operación	Estos principios establecen las reglas para el proceso de selección de las tecnologías a utilizar, enfatizando el análisis de costos y riesgos.
Rendimiento: La TI está dimensionada para brindar soporte a la empresa, suministrando los servicios con la aptitud adecuada para poder realizar y satisfacer las	Racionalización: Optimizar el uso de los recursos de TI teniendo en cuenta criterios de pertinencia y reutilización, sin perjuicio de la calidad el servicio y de la	La optimización de los recursos que involucran la implementación de TI en las organizaciones son un punto de

necesidades presentes y futuras	operación de la entidad.	encuentro de estos principios
Cumplimiento: La función de TI desempeña todos los regímenes y normas aplicables. Las políticas y prácticas están visiblemente definidas, efectuadas y requeridas	Calidad: Cumplir con los criterios y atributos de calidad definidos para los procesos y soluciones de TI construidas para la entidad.	Estos principios se enfocan en la satisfacción de las necesidades y demandas de los usuarios y beneficiarios de las TI.
Factor Humano: Las políticas de TIC, prácticas y decisiones indican respecto al factor humano, encerrando las necesidades actuales y procedentes de todas las personas involucradas	Excelencia del servicio al ciudadano: Fortalecer de forma digital la relación de los ciudadanos con el Estado enfocándose en la generación de valor público sobre cada una de las interacciones entre ciudadano y Estado	Estos principios identifican al ser humano como un factor determinante en el proceso de implementación de las TI, pues son quienes aplican la demanda sobre los servicios y posteriormente la califican
	Interoperabilidad: Utilizar los estándares que fortalezcan la plena interoperabilidad entre los sistemas de información e infraestructura tecnológica y que faciliten el intercambio de información entre las entidades y los sectores	
	Seguridad Digital: Establecer la seguridad y	

	privacidad de la información teniendo en cuenta los lineamientos definidos en la Política de Gobierno Digital.	
	Sostenibilidad: Definir las acciones que propendan por el cumplimiento de los objetivos de desarrollo sostenible de las Naciones Unidas	
	Neutralidad tecnológica: Garantizar la libre adopción de tecnologías, teniendo en cuenta recomendaciones, conceptos y normativas de los organismos internacionales competentes en la materia, fomentando la eficiente prestación de servicios, el empleo de contenidos y aplicaciones, la garantía de la libre y leal competencia mediante criterios de selección objetivos	
	Vigilancia Tecnológica: Realizar vigilancia tecnológica sobre las tendencias de la industria TI para evaluar su oportunidad en la solución a necesidades de la	

Entidad.

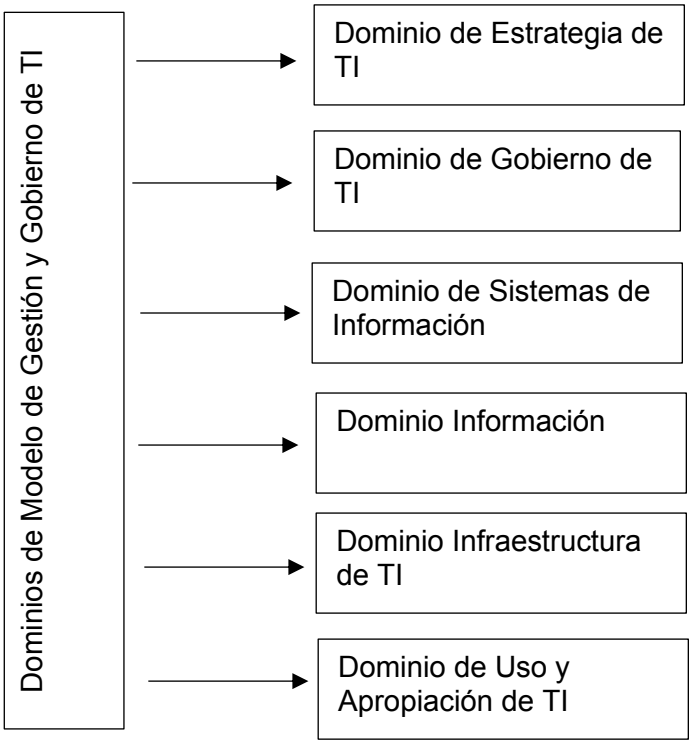
Fuente: Elaboración propia

Son cinco los principios que ha establecido el MINTIC para el gobierno de TI, que no guardan relación o similitudes con los principios establecidos por la norma NTC 38500, y es que la complejidad del sector público puede llevar a requerir otros instrumentos que promuevan la mitigación de riesgos que son más difíciles de controlar que en el sector privado. Es así como la interoperabilidad se hace necesaria en los entes territoriales puesto que la diversidad de servicios que se presta a la sociedad civil es alta y el uso de diferentes plataformas para atender la demanda de servicios intersectoriales como salud, educación, seguridad, equidad, infraestructura, entre otros requiere por ejemplo que bases de datos puedan homologarse entre sí para garantizar la transparencia en los procesos; otros principios como La Vigilancia Tecnológica, la Neutralidad Tecnológica, Sostenibilidad y Seguridad Digital han sido adaptados por el estado Colombiano para orientar las gestiones en TI de las entidades territoriales y otras que por definición de ley deben acogerse a éstos lineamientos.

6.3.3 Dominio de Gobierno de TI.

De acuerdo a las directrices definidas en el Documento Maestro del Modelo de Gestión y Gobierno de TI, esté se encuentra compuesto por seis dominios que aterrizan las necesidades de la entidad mediante el uso adecuado y consciente de las TIC.

Figura *21*. Dominios del Modelo de Gestión y Gobierno de TI



Fuente: Elaboración propia

En el presente documento se desarrollará el Dominio de Gobierno tomando en cuenta que es el objeto de estudio, para ello se ha tomado como marco de referencia la guía del gobierno de TI, expedido por MINTIC, el cual se desarrolla en cuatro ámbitos:

- Cumplimiento y Planeación
- Esquema de Gobierno de TI
- Gestión Integral de Proyectos
- Gestión de la Operación de TI

Figura *22*. Esquema Gobierno TI

Fuente: Elaboración propia

6.3.3.1 Alineación de Gobierno TI.

Las acciones planteadas para fortalecer los procesos de TI, deben estar incorporada en los Planes de Desarrollo Territoriales, a través del comité institucional de gestión y desempeño se debe aprobar al menos un procedimiento que permita a la entidad, tener la disponibilidad de directrices claras sobre que hacen para articular sus actividades a las metas del Gobierno Digital y específicamente a las TI. Se deben tener claros los responsables de estos procesos, debe identificarse un líder de las TI y contar con algún apoyo técnico – operativo.

En este sentido, los municipios del sur del departamento del Cesar de sexta categoría presentan estructuras orgánicas muy básicas, dificultando su capacidad de liderar y operar este tipo de sistemas; sin embargo, los apoyos para la elaboración del procedimiento, operación

básica de las TI y seguimiento, pueden gestionarse para avanzar de manera paulatina.

En el caso del municipio de Gamarra, a pesar que solo cuenta con dos dependencias de nivel directivo, tiene una oficina de las TIC que asume el liderazgo del tema (Alcaldía de Gamarra, 2020).

El municipio de Gonzales, presenta una estructura más básica, con cuatro dependencias de nivel directivo, sin embargo, a simple vista no se observa quien lidera el tema de TI (Alcaldía González, 2020).

Por último, para la alineación de Gobierno TI, se hace necesarios consolidar los comités, para generar espacios de discusión y toma de decisiones.

6.3.3.2 Apoyo de TI a los procesos.

Identificar los procesos de la entidad desde el Modelo Integrado de Planeación y Gestión para definir y especificar las necesidades de sistematización y apoyo tecnológico a los procesos, de manera tal que se puedan generar planes de mejora de acuerdo a las priorizaciones realizadas conforme a la disponibilidad de recursos que el municipio haya definido para el cuatrienio que se haya establecido en el Plan de Desarrollo Territorial. En este punto se debe elaborar o actualizar el Plan Estratégico de las Tecnologías e Información.

6.3.3.3 Conformidad.

El sistema de TI debe ser evaluado internamente por la oficina de Control Interno, adicionalmente la evaluación que realiza la función pública a través del FURAG de manera anual, permite identificar los elementos no conformes del sistema sobre los cuales se deben plantear acciones correctivas.

6.3.3.4 Cadena de valor TI.

El Sistema de TI para los municipios de sexta categoría puede presentar dificultades en su ejecución detallada, por ello se debe identificar el macro procesos de TI, y de esta manera ir bajando de nivel, conforme a los avances que se puedan obtener. Sin excepción se debe trabajar el proceso de Seguridad y privacidad de la información.

La seguridad y privacidad de la información, como componente transversal a la Estrategia de Gobierno en línea, permite alinearse al componente de TIC para la Gestión al aportar en el uso estratégico de las tecnologías de la información con la formulación e implementación del modelo de seguridad enfocado a preservar la confidencialidad, integridad y disponibilidad de la información, lo que contribuye al cumplimiento de la misión y los objetivos estratégicos de la entidad.

6.3.3.5 Capacidades y Recursos.

Es fundamental que la entidad pueda identificar con claridad cuáles son sus fortalezas, capacidades y recursos disponibles para alcanzar una implementación eficiente de TI, una vez identificadas se podrán establecer cuáles son las falencias y como se puede superar de forma programática.

6.3.3.6 Optimización de las Compras de TI.

Establecer la arquitectura de TI, es una de las principales metas de los entes territoriales, ya que con ésta se avanza de manera contundentes en lograr eficacia de la gestión de Tecnologías de la Información. Garantizando la adquisición de equipos físicos que no caduquen al corto plazo y que por el contrario se pueda avanzar en la mejora de la infraestructura de TI y con ende la mejora en la prestación de servicios a la sociedad.

6.3.3.7 Indicadores de Gestión de los proyectos.

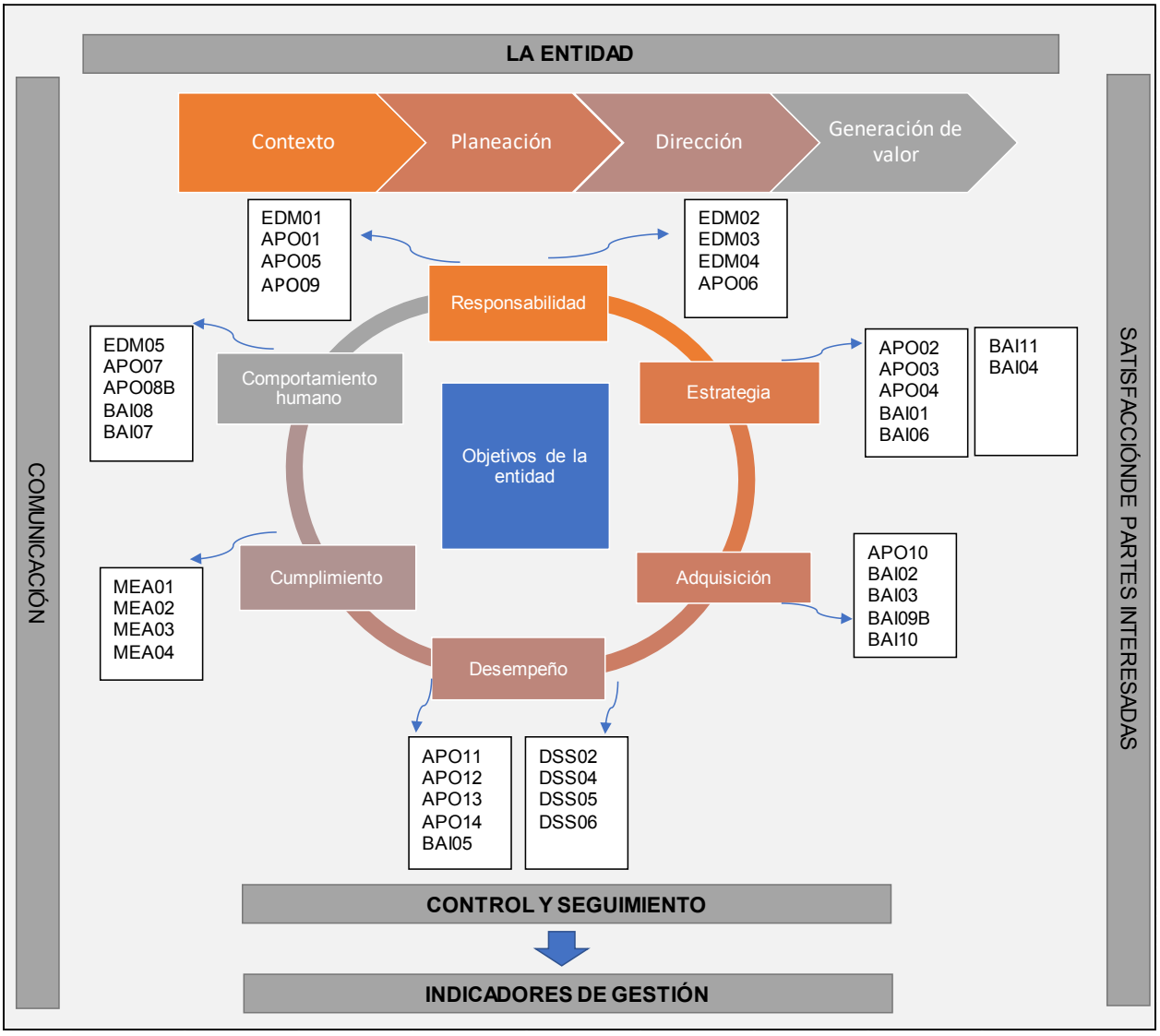
Los entes territoriales deben garantizar el monitoreo periódico de los planes establecidos, por tanto, al formulación e indicadores de gestión que permita medir el avance de los resultados de las ejecuciones en un periodo corto de tiempo, es vital. Los indicadores deben incorporarse a los cuadros de control de indicadores de la entidad.

6.3.4 Propuesta de guía para la implementación del modelo de Gobierno TI

Para la implementación del Gobierno TI en las alcaldías, se toma en cuenta el modelo planteado en COBIT 19, el cual está conformado por 40 objetivos, de los cuales 5 son de gobierno y 35 son de gestión. Asimismo, se divide en 5 dominios, tal como se describe a continuación:

Dominio Evaluar, Dirigir y Monitorear (EDM): Primer dominio (Objetivos de gobierno)
Dominio Alinear, Planificar y Organizar (APO): Segundo dominio (Objetivos de gestión)
Dominio Construir, Adquirir e Implementar (BAI): Tercer dominio (Objetivos de gestión)
Dominio Entregar, Dar servicio y Soporte (DSS): Cuarto dominio (Objetivos de gestión)
Dominio Monitorear, Evaluar y Valorar (MEA): Quinto dominio (Objetivos de gestión)

Figura 22. Modelo propuesto para el proceso de Gestión de Riesgos de TI

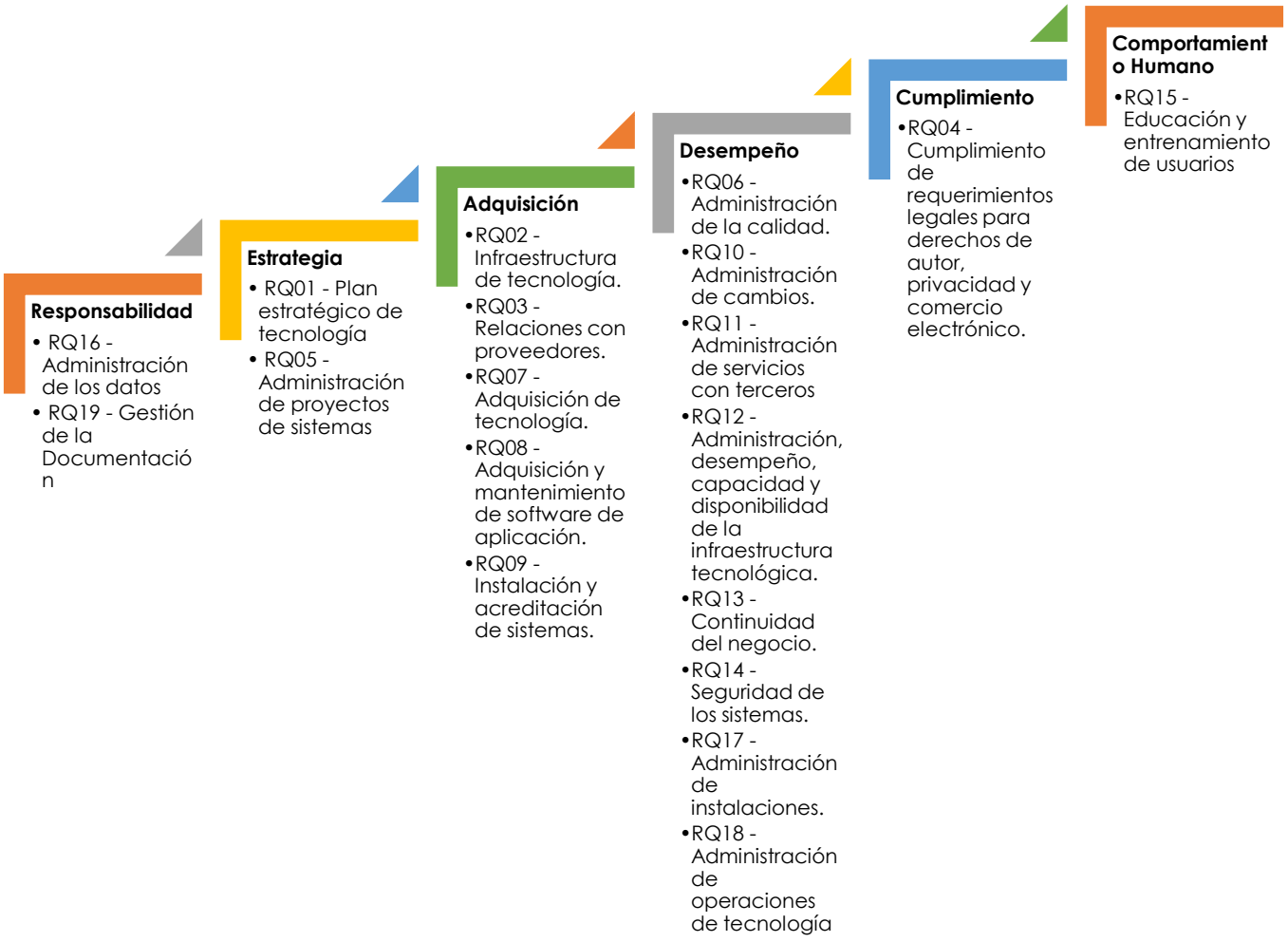


Fuente: Elaboración propia

6.3.4.1 Estructura del Modelo.

El modelo de Gobierno de TI para las administraciones municipales se encuentra soportado en 6 principios y 19 requerimientos de TI, tal como puede apreciarse en la siguiente figura:

Figura 23. Estructura del Modelo de Gobierno Propuesto – Elaboración propia

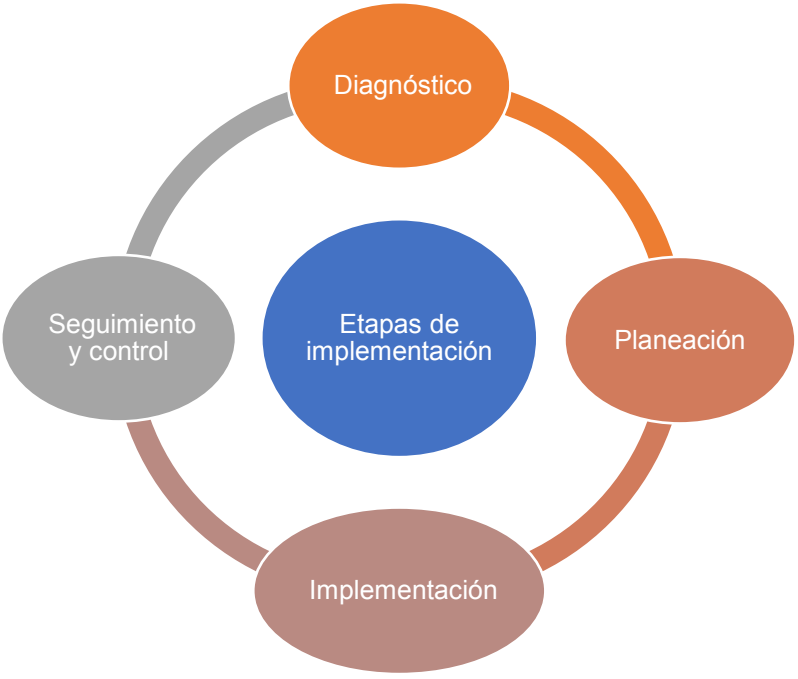


Fuente: Elaboración propia

6.3.4.2 Plan de implementación.

El plan de implementación debe obedecer a una secuencia lógica de pasos que permita adaptarse a los requerimientos de los objetivos de gobierno y gestión, por tanto se considera que el ciclo PHVA puede resultar efectivo para la puesta en marcha del modelo de gobierno TI, tal como puede apreciarse en la siguiente figura:

Figura 24. Plan de Implementación del Modelo de Gobierno



Fuente: Elaboración Propia

6.3.4.3 *Descripción de las fases de implementación.*

Fase 1: Diagnóstico

La etapa de diagnóstico permite que establecer el nivel de cumplimiento de las alcaldías frente a los requisitos definidos para el Gobierno TI, y a partir de allí poder establecer un plan de trabajo que contribuya a cerrar las brechas existentes. No obstante, es necesario contar con el compromiso de todos los involucrados en el proceso para que se logren los objetivos propuestos, por tanto, como antesala al diagnóstico se considera relevante realizar una capacitación en la cual se explique de manera breve y concisa los elementos que constituyen el modelo y la manera en que cada funcionario desde su quehacer impacta en los procesos. Es importante en esta etapa de capacitación y/o sensibilización dejar registros a través de fotografías y listado de asistencia.

Posterior a la capacitación se tiene entonces la realización del diagnóstico, para lo cual debe presentarse una programación de la auditoría interna donde se indique a los involucrados la fecha y hora, así como los procesos que se revisarán. Durante este proceso, las partes interesadas

deberán poner a disposición toda la información, documentos, entre otros, que puedan servir como soporte para establecer el nivel de cumplimiento de la entidad frente al Modelo de Gobierno de Gestión de Riesgos de TI.

Una vez finalizada la recopilación y comparación de información se determinarán los hallazgos y se elaborará un informe con los resultados, el cual será socializado a todo el equipo directivo.

Fase 2: Planeación

En esta fase, se define un plan de trabajo con base en los resultados obtenidos en la etapa de diagnóstico, con el fin de subsanar las falencias que se tengan frente al Modelo de Gobierno de TI. El plan de trabajo debe contener las actividades a realizar, el requisito que se subsanará, el responsable, el tiempo estimado de ejecución y el presupuesto. Es vital que el equipo de trabajo que se involucre en esta etapa sea pleno conocedor de los procesos y procedimientos que se desarrollan en la alcaldía y que haya asistido a la capacitación inicial en la que se explica sobre los componentes del modelo y sus requisitos. De igual manera, en esta etapa se establece la metodología que se deberá aplicar para alcanzar las metas propuestas, definiendo por ejemplo un proceso de retroalimentación en el cual el equipo de trabajo pueda socializar sobre los avances y dificultades que se presenten.

Otro aspecto que debe tenerse en cuenta en la etapa de planeación, es que es toda la estructura del Gobierno de TI debe incorporarse dentro el plan de desarrollo de las alcaldías, esto con el fin de que quede alineado e integrado a la estrategia institucional.

Fase 3: Implementación:

En esta etapa se da desarrollo al plan de trabajo definido en la fase anterior, garantizando que cada responsable ejecute las diferentes actividades que le fueron asignadas y que contribuirán a la implementación del Modelo de Gobierno de TI.

6.3.4.4 *Monitoreo y Mejora Continua.*

Fase 4: Seguimiento y control:

Esta etapa tiene como objetivo garantizar que el Modelo de Gobierno TI haya sido implementado tal como se estableció en el plan de trabajo, asimismo, permite que puedan realizarse modificaciones y/o cambios provenientes de situaciones externas que afecten el desarrollo del modelo. Es de mencionar que esta fase es la que contribuye a que exista un mejoramiento continuo del sistema, dado que se detectan falencias y vuelve a iniciarse el proceso para definir acciones correctivas y de mejora.

6.3.5 Modelo Organizacional

Para el efectivo funcionamiento del modelo, deben establecerse roles y responsabilidades en el equipo de trabajo, tal como se menciona a continuación:

- Concejo municipal: se trata del órgano coadministrador del municipio y se homologa al cargo del consejo de administración (board). Las funciones que debe desempeñar este órgano directivo se encuentran estipuladas en el artículo 313 de la Constitución Política Colombiana.

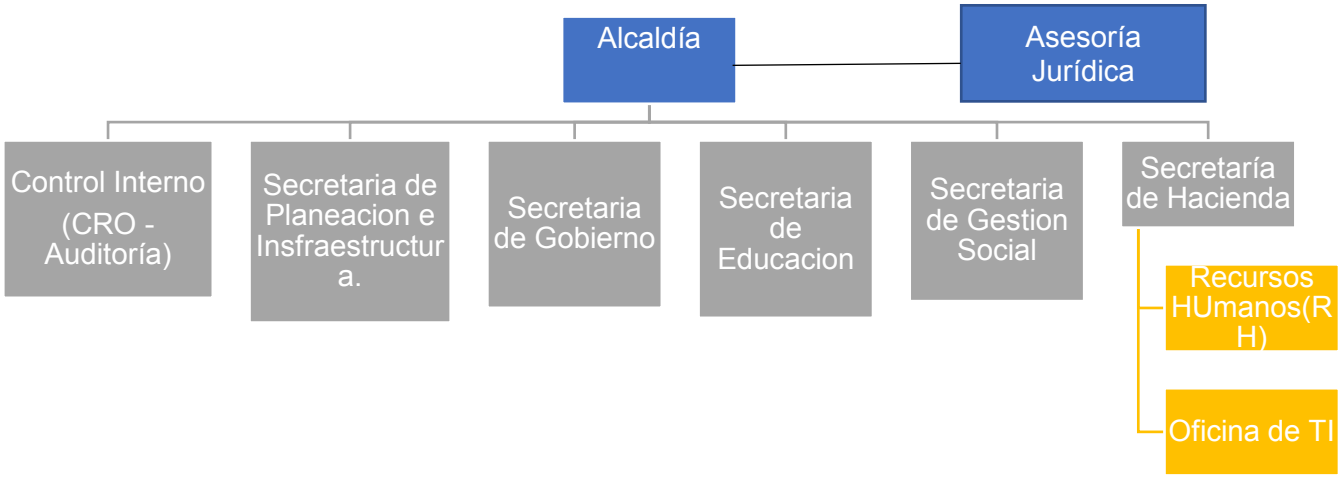
- Alcalde: cumplirá administrador, y es la máxima autoridad del municipio. Sus funciones se encuentran detalladas principalmente en el artículo 315 de la Constitución Política Colombiana.

- Secretaría de Hacienda: su objetivo es atender la gestión de los ingresos y los gastos públicos, la política de financiación y la consolidación y buen manejo de la hacienda pública del municipio.

- Secretaria de Planeación: encargada de realizar la planificación

- Secretaria de Gestión Social: integrado por las secretarias de salud, educación cultura recreación y deporte.
- Control Interno: el sistema integrado por el esquema de organización y el conjunto de planes y métodos, principios, normas, procedimientos y mecanismos de verificación y evaluación adoptados por el Municipio.
- Oficina Asesora Jurídico: asesora al alcalde y secretarios, en lo relacionado de la juridicidad de sus actuaciones y absolución de las consultas jurídicas; velar por el cumplimiento de las normas legales que regulan la Alcaldía.
- Oficina de Recursos Humanos: se encarga principalmente de responder por los procesos de contratación y vinculación laboral de funcionarios administrativos; así como por la información de sus hojas de vida y demás documentos laborales.
- Auditoria: corresponde a la función realizada por la Oficina de Control Interno. Sirve para garantizar que cada uno de los procesos, políticas, metas y actividades se cumplan de acuerdo a lo preestablecido, dando el máximo de rendimiento en cumplimiento de su misión.
- Profesional del área de sistemas: responsable de TI.

Figura 25. Modelo Organizacional (Estructura Esperada)



Fuente: Elaboración Propia

6.3.6 Modelo Gobierno Corporativo

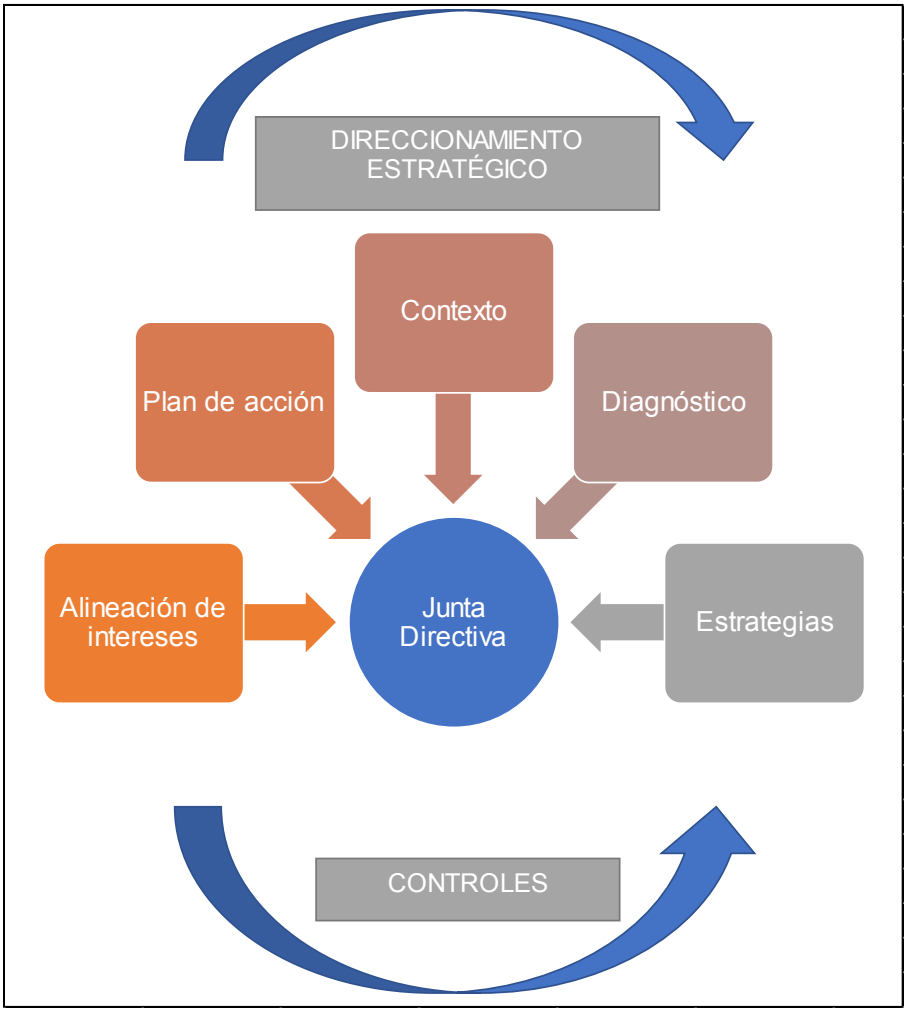
La implementación del Gobierno Corporativo (EDM) obedece al primer dominio del COBIT 19, y del cual parte el Modelo de Gobierno TI, por tanto, se requiere la implementación de un proyecto de Gobierno Corporativo que tenga como finalidad unificar criterios que contribuyan al fortalecimiento de la administración pública desde los principios de transparencia y efectividad de las estrategias definidas con el ánimo de beneficiar a los grupos de interés.

Un gobierno corporativo trae beneficios tales como la unión de esfuerzos para el cumplimiento de planes y programas propuestos, asimismo, define claramente cuáles son los objetivos tanto de la administración pública como de los organismos que interactúan con este. De igual manera, puede mencionarse como beneficio la articulación de los procesos de modo tal que facilite la toma de decisiones, el fortalecimiento de los controles para mitigar los riesgos existentes.

Dado lo anterior, la propuesta del modelo, tiene como finalidad proporcionar elementos que contribuyan a la adecuada gestión de los municipios, teniendo en cuenta los EDM's, siendo estos:

- EDM01: Asegurar el establecimiento y el mantenimiento del marco de gobierno.
- EDM02: Asegurar la entrega de beneficios.
- EDM03: Asegurar la optimización del riesgo.
- EDM04: Asegurar la optimización de recursos.
- EDM05: Asegurar la participación de las partes interesadas.

Figura 26. Modelo de Gobierno Corporativo



Fuente: Elaboración propia.

6.3.8 Articulación Estratégica

Debido a que el proyecto va enfocado al sector público, y cuyo core principal del negocio es la atención a la ciudadanía, por medio de trámites y servicios. Observando que modelos tradicionales afectan típicamente la automatización de trámites, se puede decir que sufren principalmente de responder de manera ágil a las condiciones cambiantes del entorno en el que se desarrolla una iniciativa de este tipo.

Figura 27. Marco de Referencia

Fuente: Mintic (2021)

Los Dominios o dimensiones del marco de Referencia de Articulación Estratégica para las entidades del Estado colombiano incorporan los siguientes dominios:

Dominio de Información: define estándares y lineamientos para la gestión de información como principal generador de valor estratégico para la alcaldía. Comprende la definición de los siguientes aspectos: diseño de los servicios de información, la gestión de la calidad de la misma, la gestión del ciclo de vida del dato y de información, el análisis de información y el desarrollo de capacidades para el uso estratégico de ésta.

Dominio de Sistemas de Información: define estándares y lineamientos para la gestión de los sistemas de información, incluyendo su arquitectura, ciclo de vida, las aplicaciones que los conforman y los procesos de implementación y soporte.

Dominio de Servicios Tecnológicos: define estándares y lineamientos para la gestión de la infraestructura tecnológica que soporta los sistemas y los servicios de información, así como los servicios requeridos para su operación. Comprende la definición de la infraestructura tecnológica, la gestión de la capacidad de los servicios de TI, la gestión de la operación y la gestión de los servicios de soporte.

Dominio de Estrategia de TI: define estándares y lineamientos, para diseñar la estrategia de TI y lograr su alineación con las estrategias del Estado y el sector a la que pertenece.

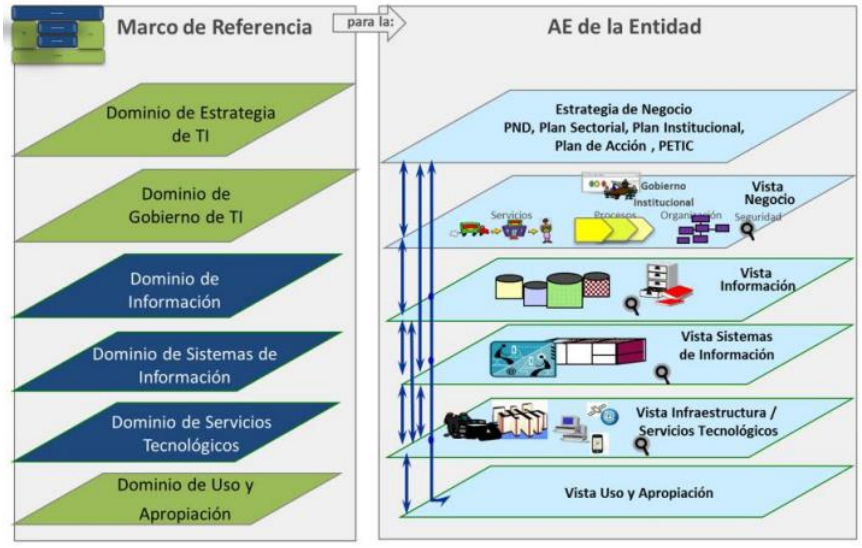
Dominio de Gobierno de TI: define estándares y lineamientos para diseñar e implementar esquemas de gobernabilidad de TI, alinear los procesos de la entidad con los del sector e incorporar políticas de TI en las entidades y procesos para la gestión de TI, gestión por procesos de TI, estructura organizacional de TI, gestión de proveedores y gestión de proyectos.

Dominio de Uso y Apropiación: define estándares y lineamientos para el Uso y Apropiación de TI, el cual incluye la gestión del cambio y gestión de grupos de interés.

Diseño detallado del modelo marco de referencia de Articulación Estratégica: Los dominios del Marco de Referencia de Articulación Estratégica, en las entidades estatales están alineados con las definiciones hechas en el Diseño Contextual del Marco de Referencia de

Articulación Estratégica y son similares a los niveles que se presentan en los conceptos tradicionales de Arquitectura Empresarial, como se puede ver a continuación:

Figura 28. Marco de Regencia y Articulación Estratégica



Fuente: Mintic (2021)

De lo anterior y conociendo que es un proceso aplicado a entidades del estado se puede decir de manera generalizada que existen necesidades internas y externas, tal como se representan en la siguiente tabla de relación de necesidades y metas del negocio.

Tabla 19. Relación de Necesidades y Metas del Negocio

		Metas de la entidad			
Tipo de Stakeholder	Necesidad del Stakeholder	Financiero	Servicios de la entidad	Productividad operativa	**Funcionarios capacitados y motivados**

Control Interno	¿La entidad vela porque se desarrolle una labor efectiva desde la oficina de control interno, garantizando la realización del seguimiento y control a través de auditorías a los procesos?	
OFICINA DE TI	¿Se tienen definidos y estandarizados los procesos de TI?	
	¿De qué manera estructurar el área de TI con el fin de dar cumplimiento a los objetivo y funciones planteadas?	
	¿Cuáles estrategias debo implementar para garantizar que todos los funcionarios cuentas con las competencias requeridas en TI?	

	¿Cómo definir un plan para proveer a los funcionarios con todos los elementos de TI requeridos en su puesto de trabajo?	

Fuente: Elaboración Propia

Tal como puede apreciarse en la figura anterior, las necesidades de los stakeholders están soportadas en las metas del negocio, tal como puede apreciarse en la siguiente tabla:

Tabla 20. Relación negocio con objetivos del negocio

Perspectivas del BSC	Metas de la entidad	Objetivos de Gobierno		
		Beneficios	Optimización de	
			Riesgos	Recursos
Financiera	Transparencia financiera	P	S	S
Clientes	Servicios de la entidad	P	P	
Procesos	Productividad operativa	P		P
Aprendizaje	Funcionarios capacitados y motivados	P		P

Fuente: Elaboración Propia

Con las metas de TI claramente identificadas y que se deben alcanzar, se obtendrá el siguiente mapeo, con el cual se conocerán los procesos relacionados, los cuales se clasifican de forma primaria **(P)** o secundaria (S), tal como lo muestra la siguiente tabla:

Tabla 21. Alineamiento de Dominios COBIT con Metas de TI

Dominios COBIT.	Procesos De TI	Objetivos/Metas de TI					
		Alineación de TI y la estrategia en el negocio	**Cumplimiento y soporte de la TI al cumplimiento del negocio de las leyes y regulaciones externas**	**Compromiso de la dirección ejecutiva para tomar decisiones relacionadas con TI.**	**Entrega de servicios de TI de acuerdo a los requisitos del negocio.**	**Seguridad de la información, infraestructuras de procesamiento y aplicaciones.**	**Entrega de Programas que proporcionen beneficios a tiempo, dentro del presupuesto y satisfaciendo**
Evaluar, Dirigir y Monitorear	EDM01. Asegurar el Establecimiento y Mantenimiento del Marco de Gobierno	P		P	P		
	EDM02. Asegurar la Entrega de Beneficios	P			P	P	
	EDM03. Asegurar la Optimización del Riesgo					S	
	EDM05. Asegurar la Transparencia hacia las partes interesadas			S	P		

	APO01. Gestionar el Marco de Gestión de TI	P	P		S	
	APO02. Gestionar la Estrategia	P		P		
	APO03. Gestionar la Arquitectura Empresarial	S	S			
Alinear, Planear, Organizar	APO05. Gestionar el Portafolio	S				P
	APO06. Gestionar el Presupuesto y los Costes	S	S			
	APO07. Gestionar los Recursos Humanos	S				P
	APO08. Gestionar las Relaciones	P		P		

	APO09. Gestionar los Acuerdos de Servicio			S	
	APO10. Gestionar los Proveedores			S	
	APO11. Gestionar la Calidad			S	
	APO12. Gestionar el Riesgo		P		P
	APO13. Gestionar la Seguridad		P		P
Construir, Adquirir, Implementar	BAI01. Gestionar los Programas y Proyectos	S			P
	BAI02. Gestionar la Definición de Requisitos	S		S	

	BAI03. Gestionar la Identificación y Construcción de soluciones		S		
	BAI04. Gestionar la Disponibilidad y la Capacidad		S		
	BAI05 Gestionar la introducción de Cambios Organizativos				S
	BAI06. Gestionar los Cambios		S	S	
	BAI10. Gestionar la Configuración	S			
Brindar Servicios y Soporte	DSS01. Gestionar las Operaciones		S		

	DSS02. Gestionar las Peticiones y los Incidentes del Servicio		S
	DSS03. Gestionar los Problemas		S
	DSS04. Gestionar la Continuidad		S
	DSS05. Gestionar los Servicios de Seguridad	P	P
	DSS06. Gestionar los Controles de los Procesos del Negocio		S
Monitorear y Evaluar	MEA01. Supervisar, Evaluar y Valorar Rendimiento y Conformidad		S

	MEA02. Supervisar, Evaluar y Valorar el Sistema de Control Interno	P
	MEA03. Supervisar, Evaluar y Valorarla Conformidad con los Requerimientos Externos	S

Fuente: Elaboración Propia

6.3.9 Métricas

Teniendo en cuenta que todo sistema requiere ser monitoreado, es necesario contar con un conjunto de indicadores que permitan realizar seguimiento y evaluación a los servicios de TI, por tanto, se considera necesario definir un cuadro de mando integral que establezca las responsabilidades y periodicidad de la medición.

6.3.9.1 Tipos de indicadores.

A continuación, se describen los tipos de indicadores que se tomarán en cuenta para el proceso se seguimiento y evaluación:

- ✓ Indicadores de implementación: Permiten medir la implementación de la Continuidad del Servicio TI. Esta es la primera métrica que se debería implementar en

una organización. Es importante destacar que para poder llegar a implementar esta métrica la organización ha debido previamente disponer de una política de Continuidad del Servicio TI dirigida y apoyada por la alta gerencia de la organización que marque la estrategia corporativa. Además, deberá tener desarrollados los procedimientos (o en fase de construcción) y se estará planteando 'medir' el grado de implantación de dichos controles.

- ✓ Indicadores de efectividad/eficiencia: Permiten medir los resultados obtenidos por el desarrollo de servicios de continuidad. Una vez implantado los controles y las métricas de implementación, se puede plantear medir el grado de implantación de los procedimientos.

- ✓ Indicadores de impacto: Permiten medir el impacto operativo o de negocio de los eventos de la Continuidad del Servicio TI. La organización debe medir cómo están impactando todos aquellos controles que están ya implementados, y son efectivos y eficientes.

6.3.10 Matriz RACI

La Matriz RACI hace énfasis en la gestión de proyectos o sistemas con el fin de asignar responsabilidades a las tareas definidas para que sean ejecutadas en los tiempos establecidos.

Tabla 22. Roles y Responsabilidades de la matriz RACI

Rol	Descripción
Responsable (R)	Debe responder por la entrega de la tarea
Aprobador (A)	Delega las tareas que deben ser ejecutadas en pro de realizar la tarea asignada a la persona responsable.
Consultado (C)	Son aquellos que brindan opiniones de valor, generalmente son expertos en el tema con quienes hay comunicación en ambas direcciones.

Informado (I)	Los informados son actualizados sobre el progreso del proyecto, que generalmente ocurre al momento de la finalización y la entrega de la tarea.

Fuente: Elaboración Propia

En la siguiente tabla se puede apreciar la participación de las áreas de las alcaldías de sexta categoría en los diferentes procesos definidos en el mapa:

Tabla 23. Matriz RACI

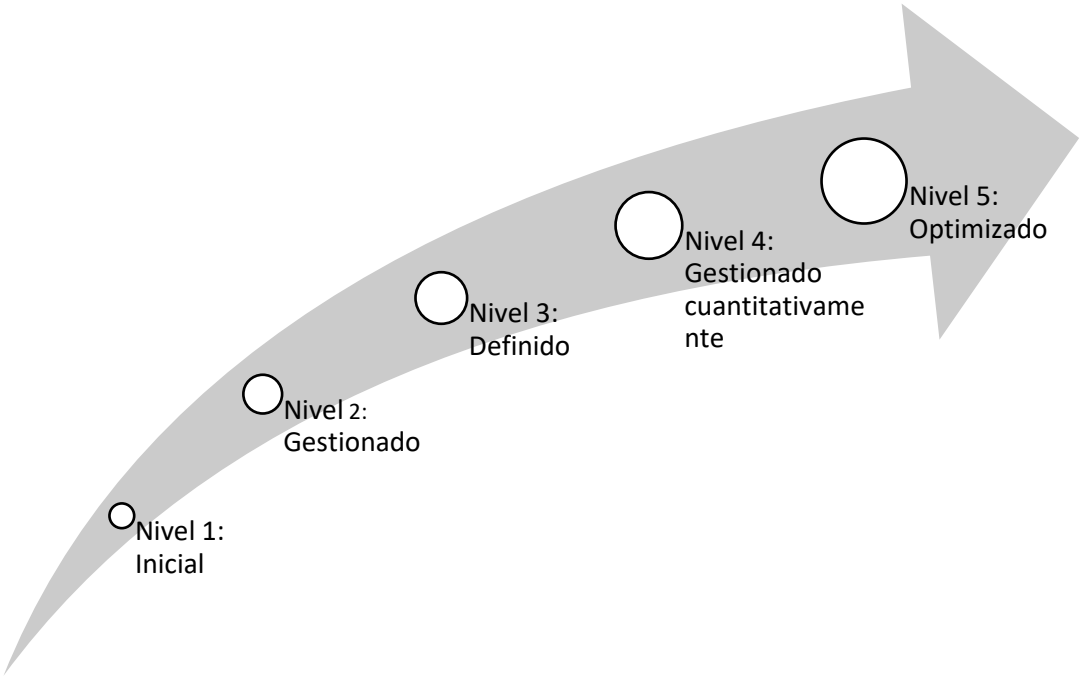
	ESTRATEGICO			MISIONAL				APOYO				EVALUACIÓN	
	Direccionamiento Estratégico	Tecnologías de la Información y las	Comunicación Estratégica	Participación Ciudadana y Control Social	Estudios de Economía y Política Pública	Vigilancia y Control a la Gestión Fiscal	Responsabilidad Fiscal y Jurisdicción	Gestión Jurídica	Gestión Del Talento Humano	Gestión Contractual	Gestión De Recursos Físicos	Gestión Documental	Gestión Financiera Evaluación y Control	
ALCALDE	R	A	A		A	A			A	A				A
SECRETARÍA DE HACIENDA		I												
OFICINA DE TIC		R	I	I	I		I		C	I	R	C		I
OFICINA DE RRHH									R	C				
CONTROL INTERNO						R			C	C				R
SECRETARÍA DE GOBIERNO	C			R			R					C		

Fuente: Elaboración Propia

6.3.11 Modelo de madurez

En la siguiente figura se definen los criterios de valoración que definen el estado de la seguridad de la información en las alcaldías municipales de sexta categoría:

Figura 7. Modelo de Madurez



Fuente: González (2016)

A continuación, se presentan los requerimientos de cada uno de los niveles de madurez con sus respectivas metas.

Nivel	Descripción
Inicial	A este nivel pertenecen las alcaldías, que aún han realizado el debido proceso de identificación de activos y gestión de riesgos, que les permita determinar el grado de criticidad de la información, respecto a la seguridad y privacidad de la misma, por lo tanto, los controles no están alineados con la preservación de la confidencialidad, integridad,

	disponibilidad y privacidad de la información.
Gestionado	Es el segundo nivel y en él se clasifican aquellas alcaldías en las que se tienen definidos procesos básicos de gestión de la seguridad y privacidad de la información, asimismo, se establecen controles que permiten detectar posibles incidentes de seguridad, pero no se encuentran gestionados dentro del componente de planificación del Modelo seguridad y privacidad de la información.
Definido	En este nivel se encuentran las alcaldías que tienen documentado, estandarizado y aprobado por la dirección, el modelo seguridad y privacidad de la información. Todos los controles se encuentran debidamente documentados, aprobados, implementados, probados y actualizados.
Gestionado cuantitativamente	A este nivel pertenecen las alcaldías que cuenten con indicadores y realizan auditorías al modelo de seguridad y privacidad de la información, recolectando información para establecer la efectividad de los controles.
Optimizado	En este nivel se encuentran las alcaldías, en donde existe un mejoramiento continuo del modelo de seguridad y privacidad de la información, retroalimentación cualitativa del modelo.

Fuente: Elaboración Propia

Tabla 24. Requerimientos y Metas por niveles de Madurez

Nivel	Requerimiento	Metas
INICIAL	• Se identifican en forma general los activos de información de la Entidad. • Se clasifican los activos de información lógicos y físicos de la Entidad.	• Establecer y documentar el alcance, limites, política, procedimientos, roles y responsabilidades y del Modelo de Seguridad y

	• Los funcionarios de la Entidad no tienen conciencia de la seguridad y privacidad de la información. • Existe la necesidad de implementar el Modelo de Seguridad y Privacidad de la Información, para definir políticas, procesos y procedimientos claros para dar una respuesta proactiva a las amenazas que se presenten en la Entidad. • Se tratan temas de seguridad y privacidad de la información en los comités del modelo integrado de gestión. • Se empiezan a definir las políticas de seguridad y privacidad de la información basada en el Modelo de Seguridad y Privacidad de la Información.	Privacidad de la Información. • Determinar el impacto que generan los eventos que atenten contra la integridad, disponibilidad y confidencialidad de la información de la Entidad. • Diseñar programas para los funcionarios, de toma de conciencia y comunicación, de las políticas de seguridad y privacidad de la información.
GESTIONADO	• Los temas de seguridad de la información se tratan en los comités directivos interdisciplinarios de la Entidad, con regularidad. • Con base en el inventario de activos de información clasificado, se establece la caracterización de cada uno de los sistemas de información. • Identificar los riesgos asicados con la información, físicos, lógicos, identificando sus vulnerabilidades y amenazas. • Elaborar un informe de los incidentes de seguridad de la información, estos deben	• Aprobación de la alta dirección, documentada y firmada, para la Implementación del Modelo de Seguridad y Privacidad de la Información. • Tener un inventario de activos de información física y lógica de toda la entidad, documentado y firmada, por la alta Dirección. • Documentar todos los incidentes de seguridad y

	ser documentados e incluidos en el plan de mejoramiento continuo. • Se cuentan con procedimientos que indican a los funcionarios como manejar la información y los activos de información en forma segura. • Existen planes de continuidad del negocio que contemplen los procesos críticos de la Entidad que garanticen la continuidad de los mismos. • Los roles de seguridad y privacidad de la información están bien definidos y se lleva un registro de las actividades de cada uno. • Se observa en los funcionarios una conciencia de seguridad y privacidad de la información. • Se revisan y se aprueban las políticas de seguridad y privacidad de la información. • Se definen los controles y medidas necesarias para disminuir los incidentes y prevenir su ocurrencia en el futuro.	privacidad de la información. • Documentar y proteger adecuadamente los planes de continuidad del negocio de la Entidad, este de estar documentado y firmado, por la alta Dirección. • Los planes de toma de conciencia y comunicación, de las políticas de seguridad y privacidad de la información, deben estar aprobados y documentados, por la alta Dirección. • Documentar los controles físicos y lógicos que se han definido en la Entidad, con los cuales se busca preservar la seguridad y privacidad de la información, aprobado por la alta Dirección.
DEFINIDO	• Se Divulgan las políticas de seguridad y privacidad de la información. • El comité directivo divulga, las medidas de seguridad y privacidad de la información que deberán ser tomadas para la conservación de la información.	• Ejecutar los planes de toma de conciencia, comunicación y divulgación, de las políticas de seguridad y privacidad de la información, aprobados por la alta Dirección.

	• Se observa el compromiso de los funcionarios con la seguridad y privacidad de la información. • Se reconoce la importancia de ampliar los planes de continuidad del negocio a otros procesos, pero aún no se pueden incluir ni trabajar con ellos. • Se implementan los controles y medidas necesarias para disminuir los incidentes y prevenir su ocurrencia en el futuro. • Se implementa el plan de tratamiento de riesgos y las medidas necesarias para mitigar la materialización de las amenazas.	• Implementar los controles físicos y lógicos que se han definido en la Entidad, con los cuales se busca preservar la seguridad y privacidad de la información.
GESTIONADO CUANTITATIVAMENTE	• Se revisa y monitorea periódicamente los activos de información de la Entidad. • Se utilizan indicadores de cumplimiento para establecer si las políticas de seguridad y privacidad de la información y las cláusulas establecidas por la organización en los contratos de trabajo, son acatadas correctamente. • Se realizan pruebas de manera sistemática a los controles, para determinar si están funcionando de manera adecuada. • Se realizan pruebas y ventanas de mantenimiento (simulacro), para determinar la efectividad de los planes de respuesta de incidentes. • Se realizan pruebas a las aplicaciones o software desarrollado “in house” para determinar	• Informe del desempeño de la operación del modelo de seguridad y privacidad de la información, el cual debe contener como mínimo: - La revisión y verificación continúa de los controles implementados. - Revisión y elaboración de riesgos. - Medición de los indicadores de gestión. - Informes de auditorías de acuerdo con lo establecido en el plan de auditorías de la entidad.

	que cumplen con los requisitos de seguridad y privacidad de la información, definidos en la metodología de desarrollo de software de la Entidad. • Se evalúa la efectividad los controles y medidas necesarias para disminuir los incidentes y prevenir su ocurrencia en el futuro. • Se realizan pruebas de efectividad en la Entidad, para detectar vulnerabilidades (físicas, lógicas y humanas) y accesos no autorizados a activos de información críticos.	- Registro de actividades en seguridad (bitácora operativa) - Elaboración de planes de mejora.
OPTIMIZADO	• Los funcionarios apoyan y contribuyen al mejoramiento de la seguridad y privacidad de la información en la Entidad. • La Entidad aprende continuamente sobre los incidentes de seguridad presentados. • Se analizan los datos arrojados por el informe de desempeño en seguridad y privacidad de la información para definir acciones correctivas más claras. • Se implementan las acciones correctivas y planes de mejora. • Se incluyen todas las áreas de la Entidad, en los planes de respuesta de incidentes.	• Lograr que la seguridad y privacidad de la información este en toda la Entidad de manera implícita, para que ningún funcionario o Directivo sean ajenos, sino que por el contrario, que ellos apoyen y contribuyan a la conservación de la seguridad y privacidad de la información en toda la organización.

Fuente: Elaboración Propia

6.3.12 Procesos más relevantes de ISO 27005

Por medio del siguiente diagrama se pueden relacionar las actividades más relevantes del

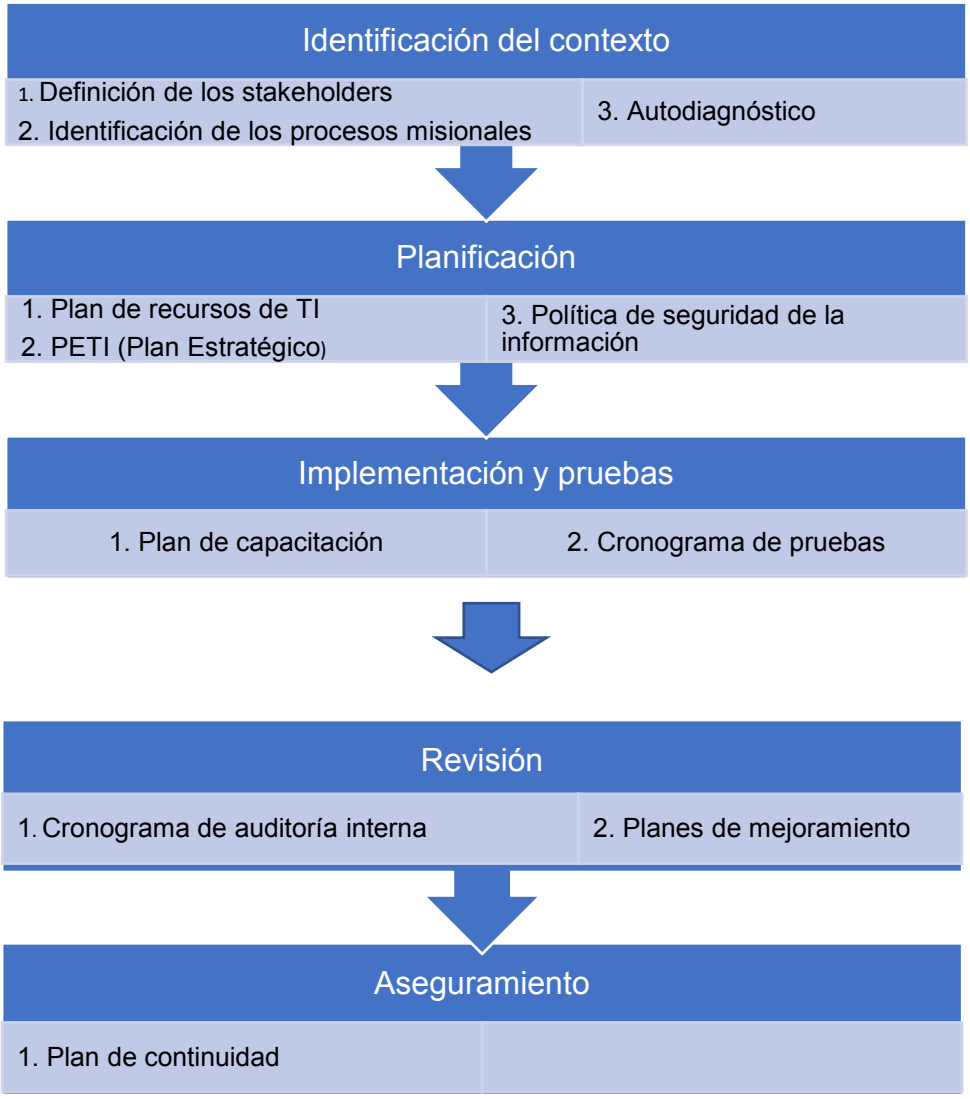
proceso de ISO 27005 que van de la mano con los procesos de gestión de una entidad estatal, son los siguientes:

- Implicación de la Dirección.
- Alcance del SGSI y política de seguridad.
- Inventario de todos los activos de información.
- Metodología de evaluación del riesgo.
- Identificación de amenazas, vulnerabilidades e impactos.
- Análisis y evaluación de riesgos.
- Selección de controles para el tratamiento de riesgos.
- Aprobación por parte de la dirección del riesgo residual.
- Declaración de aplicabilidad.
- Plan de tratamiento de riesgos.
- Implementación de controles, documentación de políticas, procedimientos e instrucciones de trabajo.
- Definición de un método de medida de la eficacia de los controles y puesta en marcha del mismo.
- Formación y concienciación en lo relativo a seguridad de la información a todo el personal.
- Monitorización constante y registro de todas las incidencias.
- Realización de auditorías internas.
- Evaluación de riesgos periódica, revisión del nivel de riesgo residual, del propio SGSI y de su alcance.
- Mejora continua del SGSI.

Una forma de representarlos gráficamente sería la siguiente:

El Plan de Implementación diseñado consta de seis fases que permiten que este sea aplicable y sostenible, brindando una hoja de ruta que identifica detalladamente desde sus necesidades iniciales hasta una completa implementación:

Figura 8. Fases de implementación del modelo de Gobierno de TI



Fuente: Elaboración propia

6.4 Definición de un mecanismo de seguimiento y control al modelo de gobierno TI para los municipios de sexta del sur del Departamento del Cesar.

6.4.1 Evaluación del nivel de madurez: Riesgos y Seguridad.

Los sistemas para gestionar los riesgos y la seguridad se desarrollan con la finalidad de minimizar los distintos riesgos referentes a multitud de amenazas originadas por las personas,

organizaciones, gobiernos, tecnología o el medio ambiente. Para llevar a cabo una correcta gestión del riesgo y seguridad, es necesario invertir todos los recursos humanos y materiales con los que cuente la organización. Actualmente es muy común que las organizaciones, gobiernos y la sociedad en general hagan frente a retos ambientales, económicos y sociales que implican que los responsables, cuenten con el liderazgo, visión y herramientas adecuadas para ello. La normativa vinculada con los sistemas de gestión de riesgos y seguridad colabora con las organizaciones y permiten conseguir los objetivos establecidos.

6.4.1.1 *Marco de administración de riesgos.*

Es importante definir claramente el marco de trabajo que será utilizado para la gestión de los riesgos en la Oficina de TIC de las Alcaldías del Departamento del Cesar; los objetivos son los siguientes:

a. Contar con un marco de referencia para la gestión de los riesgos; este marco de referencia debe ser conocido y comprendido por todos los miembros de la Oficina.
b. Preparar a la organización para eventos de riesgo que pueda atentar contra los servicios prestados por la Oficina de TIC.
c. Orientar la gestión de la Unidad para tomar medidas que ayuden, dentro de las posibilidades de la Alcaldía, a mantener la continuidad de las operaciones.
d. Fortalecer la imagen institucional por medio de una operación tecnológica más estable y confiable.

La estrategia para la administración de los riesgos está basada en los siguientes aspectos:

- Utilizar los sub procesos de COBIT por guía y referencia para la identificación de riesgos de gestión.
- Complementar la identificación de riesgos basándose en los procesos de la Unidad, esto para identificar riesgos operativos.
- Utilizar escalas de calificación de los riesgos (impacto, probabilidad, exposición) de acuerdo con modelos internaciones.

El alcance de este ejercicio de análisis de riesgos comprende lo siguiente:

- Actividades de gestión de la Oficina de TIC las cuales están a cargo de la jefatura y de los coordinadores.
- Procesos de la Oficina de TIC que incluyen las operaciones continuas y el desarrollo de proyectos
- Proyectos tecnológicos de trascendencia institucional lo cuales influyen en la imagen que se proyecta a la ciudadanía.
- Riesgos relacionados con el recurso más importante de la organización: el recurso humano.

6.4.1.2 Criterios de evaluación de riesgos.

Para la evaluación de riesgos se utilizarán, como valores primarios, la calificación de impacto y probabilidad de cada riesgo. Para ambos casos se utilizarán tablas de 5 valores con las equivalencias que se señalan a continuación. A partir de esos valores se calculará el nivel de exposición y la severidad de los riesgos representándolos en el mapa térmico. Para clasificar los riesgos se utilizarán 5 categorías asociadas con el origen del riesgo. Se utilizarán criterios de referencia específicos para cada categoría con el propósito de facilitar la evaluación de impacto para cada riesgo.

Calificación de laprobabilidad:

Para la calificar la probabilidad de los riesgos se utilizará una tabla de 5 valores:

Probabilidad	
P	Significado

5	Casi seguro
4	Muy probable
3	Probable
2	Poco probable
1	Raro

Calificación del impacto:

Para calificar el impacto se utilizará una tabla general de referencia con 5 valores; adicionalmente se utilizarán tablas específicas donde se describirán los criterios para asignar la calificación de impacto según la categoría de cada riesgo:

Impacto	
I	Significado
5	Mayor
4	Importante
3	Significativo
2	Regular
1	Menor

Severidad del riesgo:

Para medir la severidad del riesgo se utilizarán 4 valores que se determina según la calificación del impacto y la probabilidad, es decir el nivel de exposición:

Severidad	
S	**Significado**
4	Extrema
3	Alta

2	Moderada
1	Baja

Mapa térmico:

En la siguiente tabla se presenta el modelo para el mapa térmico donde según la calificación de impacto y probabilidad el riesgo es calificado por corlo en su nivel de severidad. El corlo rojo representa severidad extrema, el color naranja severidad alta, el color amarillo claro severidad moderada y el color verde claro severidadbaja:

Probab.	**Impacto**			
	1	2	3	4
1	Bajo	Bajo	Medio	Medio
2	Bajo	Medio	Medio	Alto
3	Medio	Medio	Alto	Alto
4	Medio	Alto	Alto	Muy Alto

6.4.1.3 *Categorías de los riesgos.*

Las categorías utilizadas son las siguientes:

Categoría	Descripción
Gestión	Riesgos relacionados con la ausencia o aplicación incorrecta de métodos de gestión de las tecnologías de información y comunicaciones.
Operación	Incumplimiento de directrices, procedimientos y metodologías y estándares

	en los procesos operativos de la Oficina de TIC.
Infraestructura	Riesgos relacionados con las fallas potenciales de la infraestructura tecnológica utilizada en la Alcaldía.
Seguridad	Eventos que atentan contra la confidencialidad, integridad disponibilidad de la información.
Recursohumano	Relacionados con el desempeño y regularidad de los recursos humanos.

6.4.2 Inserción Tecnológica.

Es posible que un riesgo pertenezca o está relacionado con dos o más categorías; por ejemplo, el incumplimiento de un procedimiento operativo puede dar lugar a un evento de seguridad. En estos casos el riesgo será asociado a la categoría que se considere más relevante o donde el impacto sea mayor.

Impacto de los riesgos según su categoría:

I	Significado	Criterios de calificación
5	Mayor	Evento que impedirá el logro de los objetivos institucionales.
4	Importante	El logro de objetivos institucionales se ve afectado de manera importante.
3	Significativo	Evento que representará un retraso significativo en el logro de objetivos institucionales.
2	Regular	El evento afecta levemente el logro de objetivos de la Oficina de TIC y de la Alcaldía Municipal.
1	Menor	Evento que afecta la gestión de la Oficina de TIC sin llegar a impactar en el logro de los objetivos.

Operación

I	Significado	Criterios de Calificación
5	Mayor	Evento que paraliza la prestación de servicios por parte de la unidadafectando a laalcaldía de maneraconsiderable.
4	Importante	Eventoque provoca lainterrupción parcial de servicios.
3	Significativo	Evento que provoca interrupciones intermitentes.
2	Regular	Eventoque provoca la interrupción momentánea de los serviciosdelaunidad,estainterrupciónespercibidaporla alcaldía.
1	Menor	Evento que provoca una disminución en los tiempos de respuesta que experimentan los usuarios.

Infraestructura

I	Significado	Criterios de Calificación
5	Mayor	Falla severa en un componente vital de la infraestructura tecnológica que impide la operación normal de la alcaldía.
4	Importante	Falla en un componente de la infraestructura tecnológica que afecta parcialmente la prestación de servicios.
3	Significativo	Falla en un componente de la infraestructura tecnológica que afecta de manera intermitente la prestación de servicios.
2	Regular	Falla en un equipo que afecta la prestación de servicios sólo en la Oficina de TIC.
1	Menor	Falla en un componente que puede ser sustituido de inmediato por mantener equipo similar en inventario. Se afecta la

Infraestructura

I	Significado	Criterios de Calificación
5	Mayor	Falla severa en un componente vital de la infraestructura tecnológica que impide la operación normal de la alcaldía.
4	Importante	Falla en un componente de la infraestructura tecnológica que afecta parcialmente la prestación de servicios.
3	Significativo	Falla en un componente de la infraestructura tecnológica que afecta de manera intermitente la prestación de servicios.
2	Regular	Falla en un equipo que afecta la prestación de servicios sólo en la Oficina de TIC.
1	Menor	Falla en un componente que puede ser sustituido de inmediato por mantener equipo similar en inventario. Se afecta la

Seguridad

I	Significado	Criterios de Calificación
5	Mayor	La seguridad es vulnerada y se desconocen sus efectos. Un ente no autorizado tiene acceso a información confidencial. Información total en la disponibilidad de información. Los datos institucionales han sido alterados.
4	Importante	Un ente no autorizado tiene acceso a información sensitiva. Interrupción de más de 1 día hábil en la disponibilidad de la información.
3	Significativo	Se reciben ataques masivos sobre la plataforma. Un funcionario de la alcaldía tiene acceso a información a la cual no está autorizado. Interrupción de 1 día hábil en la disponibilidad de la información. Pérdida de datos que se pueden restaurar por medio de los procesos de

		recuperación.
2	Regular	Entes no autorizados tienen acceso a información parcial en modo consulta. Interrupción de 4 horas en la disponibilidad de la información.
1	Menor	Hay intentos de acceso a la información. Interrupción momentánea en la disponibilidad de la información. Un ente no autorizado tiene la oportunidad de observar datos que se están utilizando en la operación de la alcaldía.

Recurso Humano

I	**Significado**	**Criterios de Calificación**
5	Mayor	Se prescinde de un funcionario importante para el logro de los objetivos. El evento imposibilita a todo el personal de la Oficina de TIC para realizar sus funciones de manera indefinida. Evento que provoca que un funcionario exceda en más de un 40% el tiempo estimado para finalizar una actividad.
4	Importante	Los objetivos a lograr exceden las cargas de trabajo de los recursos asignados a la Oficina de TIC. Evento que imposibilita que el personal de la Oficina de TIC pueda laborar durante un día hábil.

		Evento que provoca que un funcionario exceda en un 40% el tiempo estimado para finalizar una actividad.
3	Significativo	No se tiene participación del patrocinador para el logro de los objetivos. Evento que imposibilita a un funcionario de la Oficina de TIC para laborar durante cinco días hábiles en el lapso de un mes. Situación que provoca que un funcionario exceda en un 20% el tiempo estimado para finalizar una actividad.
2	Regular	Evento que provoca que un funcionario exceda en un 10% el tiempo estimado para finalizar una actividad. Evento que afecta, de manera temporal y no mayor de 4 horas, que los funcionarios de la Oficina de TIC puedan realizar sus funciones.
1	Menor	Se asignan objetivos adicionales que afectan levemente la carga de trabajo. Evento que imposibilita a un funcionario de la Oficina de TIC para laborar durante un día hábil.

6.4.3 Metodología para el seguimiento y control.

Como mecanismo de seguimiento y control se define un cuadro de mando con indicadores que evalúan la eficacia del modelo de gobierno de TI. Se recomienda además que se establezca el comité TI quien será el responsable de realizar el seguimiento y evaluación periódica a los resultados de los indicadores con el fin de establecer acciones de mejora.

Tabla 25. Indicadores para seguimiento y control

Indicador	Fórmula	Nivel óptimo	Nivel aceptable	Nivel crítico	Periodicidad
Satisfacción de usuarios internos	Número de funcionarios satisfechos con la calidad de los servicios de TI/ Total funcionarios	>/85%	Entre el 75 y 84	<75%	Mensual
Nivel de desarrollo de proyectos	Número de proyectos de TI desarrollados con éxito/Total de proyectos planeados	>/85%	Entre el 75 y 84	<75%	Trimestral
Ejecución presupuestal de TI	Recursos ejecutados/Recursos asignados	>/95%	Entre el 85 y 94	<85%	Semestral
Resolución de incidentes	Número de incidentes resueltos en el tiempo estipulado/Total de incidentes	>/85%	Entre el 75 y 84	<75%	Mensual
Efectividad de los trámites en línea	Número de trámites resueltos/Total de solicitudes recibidas	>/95%	Entre el 85 y 94	<85%	Mensual
Ejecución del plan de capacitación de TI	Número de capacitaciones realizadas/Total capacitaciones programadas	>/85%	Entre el 75 y 84	<75%	Trimestral
Ejecución de mantenimientos a software y hardware	Número de mantenimientos realizados/Total mantenimientos programados	>/95%	Entre el 85 y 94	<85%	Trimestral
Análisis de vulnerabilidad	Número de amenazas detectadas	-	-	-	Mensual

Fuente: Elaboración propia

Conclusiones.

Tras evaluar el estado actual del Gobierno de TI en las Alcaldías de la región, reconociendo los elementos de mayor incidencia, es posible afirmar que existe una brecha altamente significativa en lo que respecta a implementación de buenas prácticas y uso de las TI; lo cual se evidenció en los resultados arrojados por los instrumentos de recolección de información aplicados. Dicha situación afecta directamente a las partes interesadas, disminuyendo a posteriori la eficacia en los servicios prestados.

A raíz de lo anteriormente expuesto, resulta procedente examinar los componentes que deben integrar el modelo sugerido, cuya pertinencia está sujeta a posterior validación en la Alcaldías Municipal del sur del cesar.

Al desarrollar la serie de objetivos formulados como contestación a la problemática que origino el estudio, se logró constituir el modelo de Gobierno de TI diseñado para las alcaldías del Sur del Departamento del Cesar, con el objetivo de viabilizar la alineación de las tecnologías de la información con los procesos de dichas Entidades.

El modelo planteado contempla elementos principales que permiten el fortalecimiento de los procesos y su trazabilidad, mientras reducen el nivel de riesgo implícito; aportando viabilidad a la puesta en marcha dentro de la Organización; en la medida en que dicho modelo se encuentre soportado por un plan de implementación correctamente estructurado y gestionado.

Recomendaciones

Con base en el análisis de Administración Basada en Riesgos, llevado a cabo en la Unidad de Tecnologías de Información, se derivan una serie de recomendaciones que se incorporan a continuación en el presente documento.

a. Mantener un mapa térmico actualizado con los riesgos controlados que están identificados con una severidad alta o extrema.

b. Desarrollar una reunión cada primer lunes de mes, para que la jefatura de la Oficina de TIC evalúe con los coordinadores de área los planes de tratamiento que se están aplicando a los riesgos del mapa térmico identificados como alto o extremo, con el objetivo de actualizarlos si se considera que es factible mejorarlos para mitigar el riesgo.

c. Fortalecer la administración basada en riesgos en los niveles de coordinación, mediante capacitación periódica y con base en los análisis que se realicen en las reuniones los días lunes primero de mes.

d. Centralizar la actualización preliminar de los riesgos identificados, controlados, y planes de tratamiento, en un asistente de la jefatura de la Oficina de TIC que se encargará de preparar el material de la reunión de los lunes, y de alertar a la jefatura inmediatamente, en caso de que se detecte un nuevo riesgo que clasifique como alto o severo.

e. Preparar al asistente de la jefatura para que procese los nuevos riesgos con fines de clasificarlos, para alertar a la jefatura en caso de riesgos extremos o altos.

f. Cada coordinador de área debe administrar con base a los riesgos detectados, reportando al asistente los nuevos riesgos detectados, mitigados, o nuevos controles que han sido aplicados, a fin de mantener la administración de riesgos actualizada; sin importar para este caso el nivel de riesgo; todos deben ser reportados para procesarlos.

g. Adquisición de un software institucional que facilite la administración basada en riesgos.

Referencias

Arévalo Ascanio, J. G. (2016). *Documentación del sistema de seguridad de la información bajo los requisitos de la norma NTC/ISO/IEC 27001:2013.* Obtenido de http://repositorio.utp.edu.co/dspace/bitstream/handle/11059/13373/T658.562%20A321.pdf?sequence=1&isAllowed=y

Contaduría General Nación. (2021). *Categorización de los municipios.* Obtenido de https://www.contaduria.gov.co/balance-general-y-otros-informes

Función Pública . (2020). *Ley 1151 de 2008.* Obtenido de https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=29774

Función Pública . (2020). *Ley 1581 de 2012.* Obtenido de https://www.funcionpublica.gov.co/eva/gestornormativo/norma.php?i=49981

Función Pública. (2020). *Medición del desempeño institucional.* Obtenido de https://app.powerbi.com/view?r=eyJrIjoiZGE2MzQ1YTQtYWI3ZC00YTdiLWJkY2ItNzI2YmU3YzQ1ZTk5IiwidCI6IjU1MDNhYWMyLTdhMTUtNDZhZi1iNTIwLTJhNjc1YWQxZGYxNiIsImMiOjR9&pageName=ReportSection396d1cd03a850a004c59

Gobernación Cesar. (2020). *Plan estratégico de Tecnología de Información PETI 2020-2023.* Obtenido de https://cesar.gov.co/d/filesmain/meci/mipg/2021/peti_2021.pdf

Mintic . (2020). *Modelo de gestión.* Obtenido de https://mintic.gov.co/arquitecturati/630/w3-propertyvalue-8158.html#modelogestion

Mintic . (2020). *Resolución 500 de 2021.* Obtenido de https://normograma.mintic.gov.co/mintic/docs/resolucion_mintic_0500_2021.htm#:~:text=Por%20la%20cual%20se%20establecen,la%20pol%C3%ADtica%20de%20Gobierno%20Digital.

Mintic. (2020). *Ley 527 de 1999.* Obtenido de https://mintic.gov.co/portal/604/w3-article-3679.html

Presidencia. (2020). *Decreto 1499 de 2017.* Obtenido de

http://es.presidencia.gov.co/normativa/normativa/DECRETO%201499%20DEL%2011%20DE%20SEPTIEMBRE%20DE%202017.pdf

Roca Chillida, J. M. (2019). *¿Qué son las TI?* Obtenido de https://www.informeticplus.com/que-son-las-tecnologias-de-la-informacion

Secretaría Senado. (2020). *Ley 44 DE 1993.* Obtenido de http://www.secretariasenado.gov.co/senado/basedoc/ley_0044_1993.html

Secretaría Senado. (2021). *Constitución Política de la República de Colombia.* Obtenido de http://www.secretariasenado.gov.co/senado/basedoc/constitucion_politica_1991.html

SUIN. (2019). *Decreto 2106 DE 2019.* Obtenido de http://www.suin-juriscol.gov.co/viewDocument.asp?id=30038501#ver_30205980

Apéndices.

Apéndice A. Derechode petición enviado al municipio de sexta categoría del departamento del Cesar

Señores
ALCALDIA DE AGUACHICA.
DEPARTAMENTO DE CESAR.

REFERENCIA: *DERECHO DE PETICIÓN CONSAGRADO EN EL ARTÍCULO 23 DE LA CONSTITUCIÓN POLÍTICA DE COLOMBIA.*
PETICIONARIO: **ERNEY ALBERTO RAMIREZ CAMARGO.**

Yo ERNEY ALBERTO RAMIREZ CAMARGO, mayor de edad e identificado con la cédula de ciudadanía N° 1065889151 en virtud del poder otorga la constitución para el goce efectivo de los derechos consagrados en el ordenamiento jurídico, en ejercicio del derecho de petición consagrado en el artículo 23 de la Constitución Política de Colombia, la ley 1437 de 2011, la Ley 1755 de 2015 con el lleno de los requisitos consagrados en el artículo 13 y demás disposiciones concordantes, me permito realizar la siguiente petición con base en los siguientes:

I. ***HECHOS.***

PRIMERO. Soy una persona de 29 años de edad, soy profesional de Ingeniería de Sistemas, en el momento me encuentro desarrollando la maestría en **Maestría en Gobierno de Tecnologías de la Información de ahora en adelante TI, en la universidad FRANCISCO DE PAULA SANTANDER OCAÑA en la Facultad de Ingenierías.**

SEGUNDO. Mi Propuesta investigativa se llama "**DISEÑO DEL MODELO DE GOBIERNO DE TI, DIRIGIDO A LAS ALCALDÍAS DE SEXTA CATEGORÍA DEL SUR DEL DEPARTAMENTO DEL CESAR, PARA LA GESTIÓN DE RIESGOS DE LA SEGURIDAD DE LA INFORMACIÓN."**

TERCERO. Que, para el desarrollo de la propuesta investigativa, requiero de información de primera mano con fines académicos como lo expongo en esta solicitud, siendo esta información fundamental para el desarrollo de una propuesta que puede ayudar a mejorar los sistemas de información y en general todo el departamento de TI del municipio que usted representa.

II. RAZONES QUE FUNDAMENTAN LA PETICIÓN

En el artículo 23 de la Constitución Política de Colombia consagra el derecho de petición como un derecho fundamental y Constitucional a través del cual las personas pueden presentar solicitudes respetuosas a las autoridades, en los siguientes términos:

"Toda persona tiene derecho a presentar peticiones respetuosas a las autoridades por motivos de interés general o particular y a obtener pronta resolución completa y de fondo sobre la misma. El legislador podrá reglamentar su ejercicio ante organizaciones privadas para garantizar los derechos fundamentales".

Por consiguiente, fue expedida la ley 1755 de 2015 con la finalidad de regular los parámetros para interponer el derecho de petición, la oportunidad para presentarlo, los medios para impugnar las decisiones de las autoridades y demás lineamientos relacionados con el derecho a recibir información.

Así mismo, y de conformidad con lo establecido en el artículo 14 de la ley 1755 de 2015, las peticiones de documentos y de información deberán resolverse dentro de los diez (10) días hábiles siguientes a su recepción, y si en ese lapso, no se ha dado respuesta al peticionario, se entenderá, para todos los efectos legales, que la respectiva solicitud ha sido aceptada y, por consiguiente, la administración ya no podrá negar la entrega de dichos documentos al peticionario, y como

consecuencia las copias se entregarán dentro de los tres (3) días siguientes.

Así las cosas, las peticiones que cumplen con los requisitos legales establecidos deberán ser atendidas en el tiempo que para el efecto a dispuesto el legislador, so pena de verse inmerso en una violación inminente a un derecho constitucional y fundamental que tiene todo ciudadano, ignorando a su vez, los principios de la función pública y el cumplimiento a los fines del Estado.

III. PETICIÓN

En atención a todo lo expuesto, solicito a esta Entidad de forma muy respetuosa y para fines académicos lo siguiente:

PRIMERO. Indicar el estado actual del municipio en lo concerniente al desarrollo de TI.

SEGUNDO. Enviar copia del sistema empleado para la protección de los datos personales o información general del municipio frente al sistema de TI, en concordancia con el ministerio de las tecnologías y los demás estamentos encargados de la información que reposa en la administración de todo tipo.

TERCERO. Realizar un listado de los riesgos a los cuales se encuentra expuesta la información que maneja el municipio.

CUARTO. las debilidades que se identifican en el desarrollo de la ejecución de las actividades de TI. (nota: puede hacer otros hechos con las preguntas de interés para el tema concreto- hay temas sensibles que tienen reserva del estado para informar sobre estos por protección de la soberanía nacional y del municipio)

QUINTO. Todas las otras que considere importantes para mejorar el sistema de TI y la seguridad de la información, en concordancia con las recomendaciones y las exigencias del Ministerio de las tecnologías y la Comunicación.

En caso, de ser negada mi solicitud, requiero se me informe los fundamentos de hecho y de derecho de los puntos que se niega información

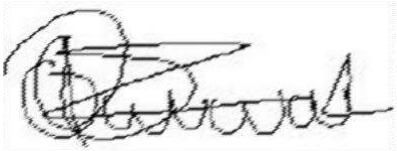
IV.RELACIÓN DE LOSDOCUMENTOS

- Fotocopia de la cédula de ciudadanía del solicitante.
- Copia de certificado de estudio o de materias matriculadas.
- Copia del documento deinvestigación.

V. NOTIFICACIONES

Para efectos de comunicaciones y notificaciones se me encuentra en la dirección cra 8ª # 18-47 barrios las orquídeas, San Martin, Cesar.
Teléfono: 3178641165
Correo electrónico: **aramirezcamargo@hotmail.com**

Atentamente,



ERNEY ALBERTO RAMIREZ CAMARGO.
Cédula de Ciudadanía N°1065889151.

Apéndice B. Lista de verificación sistema de seguridad de la información

NO.	DATOS E INFORMACIÓN A RECOLECTAR PARA LA EVALUACIÓN	C	NC
	Lista de información BASICA a solicitar		
1	Tipo de entidad (Nacional, Territorial A, Territorial B o C)		
2	Misión		
3	Análisis de contexto: La entidad debe determinar los aspectos externos e internos que son necesarios para cumplir su propósito y que afectan su capacidad para lograr los resultados previstos en el MSPI.		
4	Mapa de Procesos		
5	Organigrama de la entidad, detallando el área de seguridad de la información o quien haga sus veces		
6	Políticas de seguridad de la información formalizada y firmada		
7	Organigrama, roles y responsabilidades de seguridad de la información, asignación del recurso humano y comunicación de roles y responsabilidades.		
8	Documento con el resultado de la autoevaluación realizada a la Entidad, de la gestión de la seguridad y privacidad de la información e infraestructura de red de comunicaciones (IPv4/IPv6), revisado y aprobado por la alta dirección		
9	Documento con el resultado de la herramienta de la encuesta de diagnóstico de seguridad y privacidad de la información, revisado, aprobado y aceptado por la alta dirección		
10	Documento con el resultado de la estratificación de la entidad, aceptado y aprobado por la alta dirección		
11	Objetivo, alcance y límites del MSPI (Modelo de Seguridad y Privacidad de la Información)		

12	Procedimientos de control documental del MSPI
13	Metodología de Gestión de riesgos
14	Riesgos identificados y valorados de acuerdo a la metodología
15	Planes de tratamiento de los riesgos
16	Formatos de acuerdos contractuales con empleados y contratistas para establecer responsabilidades de las partes en seguridad de la información
17	Procedimiento de verificación de antecedentes para candidatos a un empleo en la entidad
18	Documento con el plan de comunicación, sensibilización y capacitación en seguridad de la información, revisado y aprobado por la alta Dirección, con sus respectivos soportes.
19	Documento que haga claridad sobre el proceso disciplinario en caso de incumplimiento de las políticas de seguridad de la información
20	Inventario de activos de información clasificados, de la entidad, revisado y aprobado por la alta dirección
21	Inventario de áreas de procesamiento de información y telecomunicaciones
22	Diagrama de red de alto nivel o arquitectura de TI
23	Inclusión de la seguridad de la información en la gestión de proyectos
24	Inventario de partes externas o terceros a los que se transfiere información de la entidad
25	Formato de acuerdo de transferencia de información
26	Inventario de proveedores que tengan acceso a los activos de información, indicando el servicio que prestan o bienes que venden
27	Reporte de eventos e incidentes de seguridad de la información de los últimos 12 meses.
28	Plan de continuidad de la Entidad aprobado

29	Inventario de obligaciones legales, estatutarias, reglamentarias, normativas relacionadas con seguridad de la información
30	Listado de auditorías relacionadas con seguridad de la información realizadas en la entidad
31	Procedimientos, manuales, guías, directrices, lineamientos, estándares, instructivos relacionados con seguridad de la información, el modelo de seguridad y privacidad de la información de MinTic y Gobierno en Línea.
32	Indicadores y métricas de seguridad de la información definidos.
33	Declaración de aplicabilidad
34	Aceptación de los riesgos residuales por parte de los dueños de los riesgos
	Lista de información para aquellas entidades que hayan avanzado en la fase de IMPLEMENTACIÓN
35	Documento con la estrategia de planificación y control operacional, revisado y aprobado por la alta Dirección.
36	Avance en la ejecución del plan de tratamiento de riesgos
37	Indicadores de gestión del MSPI definidos, revisados y aprobados por la alta Dirección.
	Lista de información para aquellas entidades que hayan avanzado en la fase de EVALUACIÓN DE DESEMPEÑO
38	Documento con el plan de seguimiento, evaluación, análisis y resultados del MSPI, revisado y aprobado por la alta Dirección.
39	Documento con el plan de auditorías internas y resultados, de acuerdo a lo establecido en el plan de auditorías, revisado y aprobado por la alta Dirección.
40	Resultado del seguimiento, evaluación y análisis del plan de tratamiento de riesgos, revisado y aprobado por la alta Dirección.

	Lista de información para aquellas entidades que hayan avanzado en la fase de MEJORA CONTINUA
41	Documento con el plan de seguimiento, evaluación y análisis para el MSPI, revisado y aprobado por la alta Dirección.
42	Documento con el consolidado de las auditorías realizadas de acuerdo con el plan de auditorías, revisado y aprobado por la alta dirección y verifique como se asegura que los hallazgos, brechas, debilidades y oportunidades de mejora se subsanen, para asegurar la mejora continua.