RESUMEN – TRABAJO DE GRADO

AUTORES	CECILIA AVILA MARTÍNEZ
FACULTAD	DE INGENIERÍAS
PLAN DE ESTUDIOS	MAESTRIA EN GOBIERNO DE TI
DIRECTOR	ENRIQUE JAVIER SANTIAGO CHINCHILLA
TÍTULO DE LA TESIS	CARACTERIZACIÓN DE UN MODELO DE GOBERNANZA DE TI PARA LAS ENTIDADES DEL ESTADO COMO APOYO AL CUMPLIMIENTO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN EN EL MARCO DE LA ESTRATEGIA DE GOBIERNO EN LINEA

RESUMEN
(70 palabras aproximadamente)

EN LA ACTUALIDAD TODAS LAS ORGANIZACIONES E INCLUSO LOS GOBIERNOS DEPENDEN DE LAS TECNOLOGÍAS DE INFORMACIÓN (TI) PARA SU FUNCIONAMIENTO Y DESARROLLO. EN LA ÚLTIMA DÉCADA, SU USO HA TOMADO GRAN AUGE, QUE HA CONLLEVANDO A LA REGLAMENTACIÓN Y REGULACIÓN DEL MANEJO DE INFORMACIÓN EN LAS ENTIDADES DEL ESTADO POR PARTE DEL GOBIERNO. EN ESTE MARCO EL MINISTERIO DE TECNOLOGÍAS DE LA INFORMACIÓN Y LAS COMUNICACIONES – MINTIC

CARACTERÍSTICAS

PÁGINAS: 192	PLANOS: 0	ILUSTRACIONES: 24	CD-ROM:1

CARACTERIZACIÓN DE UN MODELO DE GOBERNANZA DE TI PARA LAS ENTIDADES DEL ESTADO COMO APOYO AL CUMPLIMIENTO DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN EN EL MARCO DE LA ESTRATEGIA DE GOBIERNO EN LINEA

AUTOR

CECILIA AVILA MARTÍNEZ

Proyecto presentado como requisito para optar el título de Maestría en Gobierno de TI

Director

Ing. ENRIQUE JAVIER SANTIAGO CHINCHILLA

Doctor en Ingeniería de Seguridad de la Información

Codirector

Ing. TORCOROMA VELAZQUEZ PEREZ

Doctora en Educación

UNIVERSIDAD FRANCISCO DE PAULA SANTANDER OCAÑA

FACULTAD DE INGENIERÍAS

MAESTRIA EN GOBIERNO DE TI

Ocaña, Colombia **noviembre, 2019**

Dedicatoria

El presente trabajo de grado va dedicado a nuestro Señor Jesucristo, quien, como mi Padre Celestial, siempre ha sido luz y guía en el caminar de mi vida, colmándome de grandes bendiciones para culminar cada una de mis metas.

A mi Madre María Edith, por ser mi fuerza inspiradora y apoyo incondicional para lograr cada sueño. A mi ángel, mi padre Roberto que desde el cielo me acompaña y guía mis pasos. Gracias a ustedes he logrado convertirme en la mujer que soy. Es un orgullo y privilegio ser su hija, ustedes son los mejores padres.

A mi familia por estar siempre presente, acompañarme y brindarme apoyo moral en cada sueño. En especial a mis sobrinos y ahijado Keiner, quienes con su ternura y amor iluminan y oxigenan cada día de mi vida, siempre los llevo en mi corazón.

A mis amig@s, hermanit@s de vida, por compartir conmigo buenos momentos y otros no tanto. Ustedes siempre han estado ahí, para extender una palabra o abrazo.

A mis colegas Magister Leidy, Dilene y Javier, porque sin el equipo que formamos no hubiera logrado alcanzar esta meta.

Familia, amig@s y colegas, este título también es de ustedes. Cada uno es pilar fundamental para mi vida.

Agradecimientos

Mis primeras palabras de agradecimiento las elevo a mi padre celestial, por protegerme y colmarme de gran fortaleza, sabiduría, salud, prosperidad y amor para alcanzar cada sueño propuesto.

A mi madre María Edith, que, con su demostración de amor y madre ejemplar, me ha enseñado a no desfallecer ni rendirme ante los obstáculos y siempre perseverar. Madre eres la mejor del universo, mi mundo, mi motor… TE AMO.

De manera especial, al Dr. Enrique Santiago Chinchilla, quien con su dirección, conocimiento, enseñanza y colaboración guio, la elaboración de este proyecto de grado. Pilar fundamental en el éxito obtenido.

A la Doctora Torcoroma Velásquez Pérez, Directora de la maestría y codirectora de mi proyecto de grado, por contribuir para alcanzar con éxito la meta propuesta.

A los docentes y personal administrativo de la Maestría de Gobierno de TI de la Universidad Francisco de Paula Santander Ocaña, por aportar y compartir su conocimiento para formarme como magister de Gobierno de Tecnologías de la Información.

Departamento Administrativo Nacional de Estadística – Territorial Centro Oriente, por brindarme el permiso académico y permitir colocar en práctica el conocimiento adquirido. Así como también a mis compañeros de trabajo por su colaboración, paciencia y apoyo en el proceso.

A mis ami@s, herman@s de la vida, gracias por creer en mí y extender una palabra o abrazo en los momentos difíciles. Su apoyo incondicional fue fundamental para lograr este sueño.

A mi gran amigo y diseñador Gráfico Eduardo Rincón, quien siempre capta mis ideas y la convierte con su conocimiento en una realidad, superando mis expectativas.

A mis compañeros colegas y amigos, Jorge Camargo y Deisy Castro por las primeras luces para el diseño del modelo propuesto. Así como también a Leidy Contreras, Dilene Amaya y Javier Blanco, por todo su apoyo y colaboración en el desarrollo del proyecto.

A mi colega y amiga, Ing. Erika Quintero, por su apoyo con el grupo de panel de expertos, su colaboración fue fundamental para la culminación de este proyecto.

Por último y no menos importante, a mis compañeros y amigos de la Maestría Gobierno TI, por el conocimiento, amistad, respeto, risas y enojos compartidos. Hoy hemos logrado culminar con gran éxito este peldaño.

Mil gracias…Se les quiere. Que nuestro padre celestial les bendiga.

Índice

Lista de figuras

Lista de Tablas

Lista de apéndices

Introducción

En la actualidad todas las organizaciones e incluso los gobiernos dependen de las tecnologías de información (TI) para su funcionamiento y desarrollo. En la última década, su uso ha tomado gran auge, que ha conllevando a la reglamentación y regulación del manejo de información en las entidades del estado por parte del gobierno. En este marco el Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC de Colombia ha desarrollado y liderado la estrategia Gobierno Digital, antes Gobierno en Línea - GEL, la cual comprende la implementación del Sistema de Gestión de Seguridad de la Información para las entidades del Estado y su normatividad entre otras disposiciones.

La propuesta "Modelo de Gobernanza de TI para las entidades del estado, como apoyo al cumplimiento del componente de Seguridad y Privacidad de la Información en el marco de la Política de Gobierno Digital", tiene como fin diseñar un patrón de gobernanza TI que se adapte al Modelo de Seguridad y Privacidad de la Información (MSPI) y facilite a las entidades del estado Colombiano el cumplimiento del Decreto 1008 de 2018, por medio del cual se establecen las directrices generales de la política de Gobierno Digital (antes Gobierno en Línea), con un enfoque participativo del estado y los diferentes actores de la sociedad, pilares fundamentales para el desarrollo digital del país, impulsando el uso de la tecnología en los diferentes contextos y generando un valor público.(Política de Gobierno Digital, p8).

El Ministerio de Tecnologías de la Información y las Comunicaciones, plantea una política de Gobierno Digital, a partir de los avances alcanzados en la estrategia de gobierno en Línea, la

cual estaba reglamentada desde los años 90, con una mayor aplicación a partir del Decreto 1078 de 2015, a través del cual se expidió el decreto único reglamentario del sector de tecnologías de información y las comunicaciones, se regulo la implementación y la gestión del Programa de Seguridad y Privacidad de la Información, propuesto por el Ministerio de las Tecnologías de la Información y las Comunicaciones (MinTIC), alineado con el Marco de Referencia de Arquitectura TI a la vez que soporta transversalmente los componentes de la Estrategia: TIC para Servicios, TIC para Gobierno Abierto y TIC para Gestión. La gobernanza de TI integra e institucionaliza las buenas prácticas para garantizar que las TI de la empresa respalden los objetivos de negocio (ISACA, 2015).

El proyecto está estructurado en cinco capítulos. El Capítulo I, presenta el planteamiento del problema, Formulación del Problema, Objetivo General y Específicos, Justificación y Delimitación del problema. En el Capítulo II, se encuentra el Marco Referencial, que contiene: Antecedentes del proyecto, Marco Histórico, Marco Contextual, Marco Conceptual, y Marco Legal. El Capítulo III, Se aborda el enfoque metodológico y contiene: Tipo de Investigación, Población y Muestra, Técnicas e Instrumentos de Recolección de la Información. En el Capítulo IV, se presenta las etapas del desarrollo del proyecto, en la cual se realiza una secuencia lógica de la fundamentación de cada uno de los objetivos específicos para lograr la construcción de un Modelos de Gobernanza de TI, que facilite la dirección, el control y el cumplimiento de los objetivos de la implementación y mantenimiento del MSPI propuesto por el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC) en conformidad con la politica de Gobierno Digital, finalizando con el Capitulo V en la cual se dan a conocer las conclusiones de la propuesta.

Capítulo 1. Modelo de gobernanza de ti para las entidades del estado, como apoyo al cumplimiento del componente de seguridad y privacidad de la información en el marco de la política de gobierno digital.

1.1 Planteamiento del problema

Gobierno TI o de tecnologías de información, es un concepto que "con la promesa de hacer visible el valor que generan, ha venido tomando forma para ser mejor interpretado, implementado y aplicado, a nivel global" (Lozano, 2015). Actualmente existen muchas definiciones; Verhoef (2007), lo enmarca en una estructura de relaciones para dirigir y controlar la función de la tecnología TI dentro de una organización con el fin de alcanzar los objetivos con la agregación de valor y el equilibrio del riesgo, en comparación sobre el retorno TI y sus procesos. Parte del Gobierno TI radica en diseñar, aplicar y evaluar un conjunto de criterios para gobernar la función respectiva de manera óptima. Rahimi, Møller y Hvam (2016), lo explica como un conjunto de reglas, principios, políticas, u organigramas que definen o limitan el campo de acción de los gerentes del área.

De manera paralela Kim, Lee, Koo, y Nam (2013), define gobernanza de TI como un conjunto de prácticas o actividades institucionalizadas que permiten minimizar la incertidumbre y adquirir mejor desempeño en cuanto a la relación de subcontratación entre proveedores de servicios TI y subcontratistas. En relación, Aguilar, Verdún y Tovar (2017), refiere que el IT Governance Institute (ITGI) estableció cinco dominios de cobertura, alineación estratégica de TI con el negocio, la entrega de valor, gestión de riesgos, gestión de recursos y medición de su

desempeño. “El Gobierno de TI es responsabilidad de los ejecutivos de la junta directiva y contempla liderazgo, estructuras y procesos operacionales para garantizar que la TI de la empresa sustente las estrategias y objetivos organizacionales” (Bel, 2015).

En este sentido, la información es el activo más importante que tiene una organización, por lo tanto, su deber es protegerlo. Su seguridad, depende de que se garantice el cumplimiento de su confidencialidad, integridad y disponibilidad, pilares o principios fundamentales de la información (Krutz y Vines, 2002, p.8-16) (Santiago y Sanchez, 2017, p.5). En la actualidad, una organización tiene claro que para permanecer vigente y mejorar la expansión en el mercado, es relevante la interconectividad a internet, automatización del negocio y procesos en línea. Esta tendencia de “tecno – dependencia” así como trae beneficios, también implica riesgos para el activo de información, como consecuencia a las vulnerabilidades en el software y hardware de los productos tecnológicos. De tal forma que la inmersión en la red de redes, así como expande el negocio, también expone a un mayor número de amenazas al activo de la información, debido a que expande el área a controlar. Por lo tanto la implementación de mecanismos para salvaguardar la seguridad de la información, en la actualidad, es una necesidad para las organizaciones (Santiago y Sanchez, 2017, p.7).

De acuerdo con las nuevas tendencias tecnológicas y con el objetivo de guiar a las entidades públicas de orden nacional y territorial en el mejoramiento de los estándares de seguridad de la información, el gobierno colombiano a través del Ministerio de las Tecnologías de la Información y las Comunicaciones (MinTIC), en el marco la estrategia GEL – Gobierno en Línea, diseño el Modelo de Seguridad y privacidad de la información (MSPI), basado en los

referentes de la ISO/IEC 27001 versión 2013, el marco de trabajo de ciberseguridad del NIST, ITIL, la fundamentación legal de la ley Protección de Datos Personales (Ley 1581 de 2012), transparencia y acceso a la información pública (Ley 1712 de 2014, art 4) entre otras, relevantes en la gestión de la seguridad de los activos de información (MinTIC, 2016).

En el contexto de antecedentes internacionales, Brandis, Dzombeta y Haufe (2014), plantearon un modelo para el gobierno de la nube como marco holístico que aborda la gobernanza TI, a través de un patrón que diseña la gestión de requisitos, para la seguridad de la información, el ciclo de vida, la gestión de riesgos y cumplimiento, desde el marco de gobierno de TI. Mientras que en Colombia, MinTIC, diseña un "Modelo de Seguridad y privacidad de la Información para la Estrategia de Gobierno en Línea 2.0", con un enfoque sostenible que va desde la preparación de la entidad para comenzar la implementación, la definición de brechas, hasta la alineación con el sistema de Gestión de Seguridad de la Información (SGSI), (Centro de Investigación de Telecomunicaciones -CINTEL, 2011).

En este ámbito en la Escuela Colombiana de Ingeniería Julio Garavito, presenta una metodología para la medición de la efectividad de los indicadores de Gestión del MSPI (Useche, 2017). Por su parte, Cruz y Martínez (2011) proponen un modelo de integración de MECI y COBIT, para las entidades públicas; que abarca la matriz de relación para los componentes del Modelo Estándar de Control Interno y los objetivos de control de COBIT, con el fin de alinear los controles aplicables a TI con los procesos estipulados para estas entidades. Sumado a ello desarrolla un modelo de madurez que permite conocer en qué etapa de aplicación de gobierno de TI se encuentra la organización.

Por otra parte, Espinoza (2016), refiere el diseño de una propuesta de marco de Gobierno TI para la Secretaria de Educación Superior, Ciencia Tecnología e Innovación SENESCYT, basado en las mejores prácticas, cuyo objeto es desarrollar una propuesta que haga uso de las mejores prácticas de generación de valor óptimo desde TI, en búsqueda de mantener el equilibrio entre las metas estratégicas institucionales y la generación de beneficios. De igual manera en la Universidad de los Llanos, se aplica como caso un Modelo de Gobierno de TI, como apoyo a los procesos administrativos, el cual propone sensibilizar y concientizar a las altas directivas de la institución educativa la necesidad del uso eficaz de las tecnologías (Alvarado, 2017).

El gran uso de herramientas tecnológicas en cumplimiento del objeto misional, obliga a la mayoría de las organizaciones a implementar nuevos patrones enmarcados en estándares que permitan gestionar la seguridad de su información. El MSPI, diseñado por MinTIC, está alineado con el Marco de Referencia de Arquitectura TI y soporta transversalmente los componentes de la Estrategia GEL: TIC para Servicios, TIC para Gobierno Abierto y TIC para Gestión, (MinTIC, 2016). A pesar de que MinTIC ha dispuesto de esté como guía, al momento de la implementación se encuentran dificultades en la realización de las etapas; entre ellas y posiblemente la principal es la falta de profesionales capacitados o con experiencia en implementación de SGSI al interior de las entidades públicas (Ocampo, 2016). Sumado a esto la Alta Gerencia no asume el rol de líder y patrocinador que le corresponde, por lo que lleva a que el proyecto se ve afectado en su desarrollo, teniendo en cuenta que no se le da la importancia requerida, (Ocampo, 2016).

Lo anterior permite deducir que el MSPI, es un modelo orientado a la gestión, denotando la ausencia de un control directo que ayude a ejercer la dirección y complemente la gestión de nuevas tecnologías en la administración pública. En complemento se resalta el área de TI y especialmente en las entidades del estado, la necesidad de instrumentos de control relacionados a procesos claves de TI, que le permitan a la alta gerencia el monitoreo, para prevenir fallas, observar tendencias y encontrar posibilidades de mejoras, (Cruz Medina y Martínez García, 2011). En relación, Chen y Wu (2011), resaltan la importancia que se tiene, que los gerentes TI, cuenten con habilidades a fines con la alineación, sincronización y convergencia de tecnología y negocios, así como también la capacidad para gestionar las mismas. "Las organizaciones dependen cada vez más de las TI para la toma de decisiones con el propósito de sostener el crecimiento del negocio" (Alonso, Verdún Carrillo , y Tovar Caro, 2017).

1.2 Formulación del problema

¿La determinación de las características particulares a considerar en el modelo de Gobernanza de TI; les facilitará a las entidades del estado cumplir con la implementación y gestión del Programa de Seguridad y Privacidad de la Información propuesto por MINTIC y mejorar la eficacia en su adopción?.

1.3 Hipótesis

La adopcion de un modelo de Gobernanza de TI para las entidades del estado, mejora la eficacia de la implementacion del modelo de seguridad y privacidad de la información propuesto dentro del marco de la estrategia de Gobierno Digital.

1.4 Objetivos

1.4.1 Objetivo general. Proponer un modelo de gobierno de TI que facilite la dirección, el control y el cumplimiento de los objetivos de la implementación y mantenimiento del programa de seguridad y privacidad de la información propuesto por el Ministerio de Tecnologías de la Información y las Comunicaciones del gobierno Colombiano a las organizaciones del estado en el marco de Gobierno Digital.

1.4.2 Objetivos específicos. Identificar el marco normativo del estado colombiano para la implementación del MSPI.

Conocer el estado del arte del Modelo de Seguridad y Privacidad de la información propuesto por el ministerio de las TIC en Colombia.

Analizar los marcos de trabajo de gobierno de TI existente que confluyen en los objetivos de gobernanza y gestion del MSPI.

Diseñar un modelo de gobernanza que facilite la Evaluacion, Direccion y el Control del programa de seguridad y privacidad de los activos de informacion de las entidades del estado colombiano.

Validar la coherencia y la efectividad del modelo de gobernanza propuesto, fundamentada en la opinión de una muestra de “Expertos” en Gobierno, Seguridad, Control Interno y Auditoria TI.

1.5 Justificación

En la literatura se encuentra un número relevante de modelos diseñados para dar soporte a la implementación de distintos aspectos del gobierno de TI. En el contexto internacional la Agencia Española de Protección de Datos, diseño una guía de seguridad, con el objeto de facilitar a los responsables del tratamiento de datos personales la adopción de las medidas de seguridad instituidas en el Reglamento de la LOPD (Agencia Española de Protección de Datos, 2017). De igual manera el centro de conocimientos para la ciberseguridad de Europa ENISA - Agencia de la Unión Europea para la Seguridad de las Redes y la Información, desarrollo un modelo de evaluación de herramientas de privacidad en línea, con el fin de brindar más seguridad en su uso, para los usuarios de internet y dispositivos móviles (Hernández, y otros, 2015).

En esta práctica, en Colombia de acuerdo con la reglamentación establecida mediante la estrategia de Gobierno Digital, liderada por MinTIC; las entidades públicas se ven en la necesidad de iniciar la implementación de un Sistema de Gestión de Seguridad de la Información – SGSI, (Ocampo, 2016). Para lo cual MinTIC, da a conocer el Modelo de Seguridad y Privacidad de la Información, basado en buenas prácticas nacionales e internacionales para "suministrar requisitos para el diagnóstico, planificación, implementación, gestión y mejoramiento continuo, del Modelo de Seguridad y Privacidad de la Información - MSPI de la Estrategia de Gobierno en Línea – GEL" (MinTIC, 2016).

En este contexto, en Colombia las instituciones que ejercen funciones públicas, y ejecutan presupuestos provenientes del erario público, deben acogerse al Decreto 1008 de 2018, el cual

modifica al decreto 1078 de 2015. El Decreto en mención, tiene por objeto establecer los "lineamientos generales de la política de Gobierno Digital para Colombia, antes estrategia de Gobierno en Línea, la cual desde ahora debe ser entendida como el uso y aprovechamiento de las tecnologías de la información y las comunicaciones para consolidar un estado y ciudadanos competitivos, proactivos, e innovadores, que generen valor público en un entorno de confianza digital (Decreto 1008, 2018)". De igual manera propone unas líneas de acción orientadas al desarrollo e implementación de la política a través de los componentes TIC para el estado y TIC para la sociedad y tres elementos básicos para su desarrollo como habilitadores transversales Arquitectura, Seguridad y Privacidad y Servicios Ciudadanos Digitales.

Por lo tanto, un modelo de gobernanza de TI para las entidades del estado, como apoyo al cumplimiento del componente de seguridad y privacidad de la información (MSPI), facilitara la alineación de TI al negocio, visionando sostenibilidad en el tiempo, con un retorno claro del aporte de TI hacia la entidad.

El gobierno de TI integra e institucionaliza las buenas prácticas para garantizar que la TI en las entidades públicas soporten los objetivos del negocio. De igual manera, permite que la institución aproveche al máximo su información, maximiza los beneficios, capitaliza las oportunidades y gana ventajas competitivas (Palao, 2010) (Muñoz y Ulloa, 2011). "La gestión de TI es responsabilidad de los ejecutivos y de la junta directiva y hacen parte de ella el liderazgo, las estructuras organizativas y los procesos para garantizar que las mencionadas tecnologías de la empresa sustenten y extiendan las estrategias y objetivos de la empresa" (Brandis, Dzombeta y Haufe, 2014).

1.6 Delimitaciones

Alcance de la solución estará delimitado por los aspectos relacionados con los siguientes literales:

1.6.1 Geográficas. El modelo a desarrollar puede ser implementado en cualquier alcaldía de los municipios del departamento Norte de Santander, que cumpla con el requisito de estar minio en la fase de evaluación de desempeño del Modelo de Seguridad y Privacidad de la información.

1.6.2 Temporales. El periodo de realización del estudio será de doce (12) meses.

1.6.3 Conceptuales. Para la realización de este proyecto se tendrá en cuenta los conceptos de Gobernanza, Gobierno TI, buenas prácticas, Modelo de Seguridad y Privacidad de la Información (MSPI) de MinTIC, Niveles de Madurez y los marcos de Gobierno de TI: ISO/IEC 38500:2015, VAL IT y COBIT 5.0, entre otros.

1.6.4 Operativa. La presente investigación se enfoca en el diseño de un modelo de gobierno de TI que facilite la dirección, el control y el cumplimiento de los objetivos de la implementación y mantenimiento del programa de seguridad y privacidad de la información propuesto por el Ministerio de Tecnologías de la Información y las Comunicaciones del gobierno Colombiano a las organizaciones del estado en el marco de Gobierno Digital, que funcione como apoyo para aquellas entidades públicas del Estado Colombiano, que se propongan trabajar con el modelo en mención.

La rigurosidad operativa del modelo de gobernanza propuesto, estará fundamentada en los resultados de la Investigación y apoyada en la opinión de una muestra representativa de "Expertos" del sector privado y público en el área de Seguridad de la Información, en Gobierno de Tecnologías, Control Interno y Auditoria TI con experiencia en la Implementación del MSPI en entidades públicas. De igual manera cabe resaltar que si durante el desarrollo del proyecto se presenta alguna dificultad en la recopilación de la información, se tendrá en cuenta otras fuentes relacionadas con el tema en estudio, para garantizar el cumplimiento de los objetivos propuestos.

Capítulo 2. Marco referencial

2.1 Marco Histórico

2.1.1 Antecedentes. En el ámbito internacional y nacional, se ha desarrollado estudios, proyectos, artículos, etc., sobre modelo de gobierno TI, o gobernanza TI para entidades públicas, así como modelos de seguridad y privacidad de la información, entre los cuales es preciso destacar los siguientes.

En el marco de modelos de seguridad y privacidad de la información a nivel internacional. La Agencia de la Unión Europea para la Seguridad de las Redes y la Información (ENISA), ha participado activamente en tecnología de mejora de la privacidad (PET, por sus siglas en inglés). Entre sus principales funciones se encuentra el analizar la disponibilidad tecnológica de las PET, así como facilitar plataformas de investigación y diferentes actividades de expertos en privacidad. En el 2015 ENISA, realiza la publicación de un estudio para la protección de la privacidad en línea, denominado Herramientas de privacidad en línea para el público en general, con dos (2) objetivos relevantes, el primero de ellos, definir el nivel actual de la información y orientación que le brindan al cliente externo y el segundo proporcionar un modelo de herramientas de privacidad en línea, que brinde mayor seguridad en el uso e incentive una adopción más amplia a los usuarios de internet y dispositivos móviles (ENISA, 2015).

En marzo de 2016, La Agencia de la Unión Europea para la Seguridad de las Redes y la Información (ENISA) presenta el informe Análisis de preparación para la adopción y evolución de tecnologías de mejora de la privacidad, el cual tiene como fin desarrollar una metodología que

permita la comparación respecto a la madurez de las diferentes tecnologías de mejora de la privacidad (PET). Este manuscrito traza una metodología para recopilar la opinión de expertos e indicadores para una escala de calificación bidimensional. De igual manera realiza unas pruebas pilotos para verificar las escala y metodologías propuestas (ENISA, 2016). Tras un trabajo previo en el área de la ingeniería de privacidad, en diciembre del mismo año, publica "la Matriz de controles de PET: un enfoque sistemático para evaluar las herramientas de privacidad en línea y móviles, como un marco de evaluación y herramienta para la presentación y evaluación sistemáticas de herramientas de privacidad en línea y móviles para usuarios finales" (ENISA, 2016).

Tecnologías de mejora de la privacidad: evolución y estado del arte, es un documento publicado por La Agencia de la Unión Europea para la Seguridad de las Redes y la Información (ENISA) y dado a conocer en marzo de 2017; en el cual se "proporciona recomendaciones sobre cómo construir y mantener una comunidad en línea para las evaluaciones de madurez de PET, que cuenta con la asistencia de la herramienta de ENISA. El enfoque de desarrollo comunitario presentado, busca guiar a los desarrolladores y capacitar a grupos de personas, en el conjunto de habilidades que requieren para participar activamente en el proceso de evaluaciones de PET" (ENISA, 2017).

El gobierno español regula mediante el Decreto 3 de 8 de enero de 2010, el Esquema Nacional de Seguridad (ENS), en el cual determina la política de seguridad a aplicar en el uso de los medios electrónicos. Este sistema (ENS) está constituido por los principios básicos y requisitos mínimos esenciales para la adecuada protección de la información. La finalidad del

ENS es crear las condiciones de confianza necesarias en la utilización de los medios electrónicos, garantizando la seguridad de los sistemas, servicios electrónicos, datos y comunicaciones de tal manera que permita tanto a los ciudadanos como a la administración pública, el ejercicio de sus derechos y el cumplimiento de los deberes (Esquema Nacional de Seguridad - ENS, 2010).

Por su parte la Agencia Española de protección de datos en el 2010, publica un modelo de "Documento de Seguridad", para guiar y facilitar el desarrollo y cumplimiento de la normativa sobre protección de datos a los responsables de ficheros y encargados de tratamientos de datos personales, a la adopción de las disposiciones del Reglamento de desarrollo de la Protección de Datos de carácter personal -LOPD (RLOPD). Este Instrumento recopila en un cuadro el resumen de las medidas de seguridad comprendidas en el citado Título VIII del RLOPD, en el cual se desarrollan las regulaciones de seguridad en el tratamiento de datos de carácter personal y tiene por fin establecer las medidas de índole técnica y organizativa necesarias para garantizar la seguridad que deben reunir los ficheros, los centros de tratamiento, locales, equipos, sistemas, programas, así como las personas que intervengan en el tratamiento de los datos de carácter personal. De igual manera, incluye una relación de comprobaciones para facilitar la realización de la auditoría de seguridad.

En Latino América, en Perú, el 23 de julio del 2004 la PCM a través de la ONGEI, dispone el uso obligatorio de la Norma Técnica Peruana "NTP-ISO/IEC 17799:2004 EDI. Tecnología de la información: Código de Buenas Prácticas para la gestión de la Seguridad de la información" en entidades del Sistema Nacional de Informática. La cual realizo la primera actualización el 25

de agosto del 2007 con la Norma Técnica Peruana "NTP-ISO/IEC 17799:2007 EDI". A la fecha tiene reglamentada en el área de tecnología de información, la NTP-ISO/IEC 27001:2014.

En Colombia, El Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC a través de la Dirección de Estándares y Arquitectura de TI y la Subdirección de Seguridad y Privacidad de TI, por medio del decreto 1078 de 2015, define el componente de seguridad y privacidad de la información, como parte integral de la estrategia GEL. Para lo cual diseña el Modelo de Seguridad y Privacidad de la Información – MSPI, en el año 2010, con última actualización en marzo de 2016. El cual conduce a la preservación de los pilares fundamentales de la seguridad de la información, confidencialidad, integridad, disponibilidad, mediante la aplicación de un proceso de gestión del riesgo, brindando confianza a las partes interesadas acerca de la adecuada gestión de riesgos. En referencia, el Ministerio de Tecnologías de la Información y las Comunicaciones – MinTIC, en los últimos años ha elaborado una serie de documentos asociados al Modelo de Seguridad y Privacidad de la Información, utilizados por las diferentes entidades de orden nacional y territorial, para mejorar sus estándares de seguridad de la información.

En cumplimiento a las buenas prácticas de seguridad; Modelo de Seguridad y Privacidad de la Información – MSPI, es actualizado periódicamente; reuniendo los cambios técnicos de la norma 27001 del 2013, legislación de la Ley de Protección de Datos Personales, Transparencia y Acceso a la Información Pública, entre otras, las cuales se deben tener en cuenta para la gestión de la información; de igual manera específica los nuevos lineamientos que permiten la adopción del protocolo IPv6 en el Estado Colombiano. El modelo en referencia concierta que: "La

planificación e implementación del Modelo de Seguridad y Privacidad de la Información – MSPI, en la Entidad está determinado por las necesidades y objetivos, los requisitos de seguridad, los procesos misionales y el tamaño y estructura de la Entidad" (MSPI, 2016).

De manera complementaria, Ocampo García (2016), A través del trabajo Modelo de Seguridad de la información para las entidades públicas del estado colombiano, da a conocer el Modelo de Seguridad y Privacidad de la Información – MSPI, que comprende desde el marco normativo que lo rige, hasta soluciones a posibles dificultades que pueden encontrar en la implementación.

En el contexto de modelos de gobernanza de TI en entidades públicas se encuentra poca literatura, sin embargo, se puede citar investigaciones como la de Al Qassimi y Rusu (2015), en la cual hace referencia a la Gobernanza de TI para entidades públicas de países en desarrollo. Caso de estudio en una organización gubernamental. Los autores manifiestan que la aplicación del gobierno de TI, es una iniciativa de las organizaciones del sector privado en la década de los 90, como una estrategia para lograr la excelencia, proveer nuevos servicios y aumentar la rentabilidad de las inversiones de TI. Sus resultados y beneficios motivaron algunas del sector público a implementar buenas prácticas de gobierno de TI.

Así mismo en el proceso de revisión literaria Al Qassimi y Rusu, confirman que existe un número muy limitado de investigaciones en el área para el sector público en países en desarrollo. Debido a que predominan los estudios para organizaciones del sector privado, específicamente en los países desarrollados. A su vez destacan un debate entre los países desarrollados y en

desarrollo, que evidencian diferencias relevantes en la de toma de decisiones, enfocadas en el Gobierno Corporativo y de TI. El resultado de esta investigación concluye que existe la necesidad de mejorar las estructuras, procesos y mecanismos que contribuyen a una implementación efectiva de Gobierno de TI en las organizaciones objeto de estudio (Al Qassimia & Rusu, 2015).

En Brasil, Cerqueira y Denner (2017), proponen un estudio acerca de los mecanismos no operacionales que pueden influir en la efectividad de la gobernanza de tecnología de la información en la administración pública. El análisis se realiza a través del diagnóstico de aplicación de un cuestionario a gestores de TI, Profesionales con experiencia en TI que trabajen en organizaciones de la administración pública. Los resultados indicaron que los mecanismos de efectividad en la gobernanza de TI: apoyo de la alta dirección; actuación de la comisión de dirección de TI; utilización del plan estratégico de TI; no tienen influencia en la efectividad percibida de la gobernanza de TI en el sector público. No obstante, La actuación de la gestión de cartera de inversiones de TI influye directa y positivamente en la efectividad; además, es por medio de su presencia como variable mediadora que la actuación de la comisión de TI logra tener un efecto significativo sobre la efectividad de la gobernanza de TI en la administración pública (Cerqueira & Denner dos, 2017) .

De igual manera en el ámbito nacional, Marulanda, López y Valencia (2017), realizaron una investigación acerca del estado y alcances del gobierno de TI y la gestión de TI en las entidades públicas del municipio de Manizales, departamento de Caldas, Colombia. En donde a través de un estudio descriptivo exploratorio y correlacional a 19 entidades estatales, obtuvieron

como resultado que el gobierno de TI es una realidad para una pequeña porción de dichas entidades, recomendando la generación de alianzas con entidades, como las instituciones de educación superior, para avanzar en el desarrollo de estas dinámicas. Además de fortalecer, inversiones en estos recursos, seguir cualificando al talento humano que trabajan con ellos, generar sinergias y resiliencias para abordar e Interiorizar el amplio alcance del gobierno de TI y su gestión, con el objetivo de fortalecer el trabajo colaborativo en los ámbitos local, regional y nacional(Marulanda, López Trujillo, y Valencia Duque, 2017).

En forma paralela Vargas (2017), desarrolla un Modelo de Gobierno de TI como apoyo a los procesos administrativos aplicado como caso en la universidad de los llanos. Proyecto que propone un modelo de Gobierno de TI que: "involucre, sensibilice y concientice a las altas directivas de la institución en la necesidad del uso eficaz de las tecnologías de la información". Política de gobierno de TI específica, que pretende viabilizar el flujo y análisis de la información entre las diferentes dependencias, fusionando el actual sistema de gestión integral y potenciando a la entidad a un nivel superior organizacional (Vargas, 2017).

Con el fin de obtener una mayor precisión en la información del contesto departamental, se elevó la consulta a MinTIC, acerca del porcentaje de avance de implementación del MSPI en que se encuentran las alcaldías de los municipios del departamento Norte de Santander, la cual fue radicada con el número 946548. En respuesta al requerimiento, la coordinadora encargada del Grupo Interno de Trabajo de Seguridad y Privacidad de TI de MinTIC, Fabiana García Prieto, nos indica una tabla con la información general en relación con la implementación del MSPI de acuerdo con el reporte realizado por las alcaldías del departamento en mención.

Tabla 1
Implementación del MSPI

DEPARTAMENTO	ENTIDAD	AVANCE*
Norte de Santander	Alcaldía Villa del Rosario	10%
	Alcaldía Cáchira	13%
	Alcaldía de Toledo	15%
	Alcaldía de los Patios	20%

*El porcentaje de avance respecto a la implementación completa de las 4 fases del MSPI

Cabe aclarar, que de igual manera nos manifiestan que las entidades que no se encuentran en la tabla relacionada anteriormente, a la fecha no han generado reporte de avance ante MinTIC, (Anexo A).

En base a lo anterior en referente bibliográfico, se encontró que la alcaldía de Cúcuta, a través de la resolución 0747 del 31 de octubre de 2017 y la de El Tarra, con la Resolución 11-1411, adoptan un manual de Políticas generales de seguridad y privacidad de la información a aplicar en cada una de ellas.

En relación, las alcaldías de El Carmen y Pamplona, tiene en su página web la Política de Privacidad y Condiciones de Uso del sitio Web, en la cual se abarca los temas relacionados a condiciones generales para el uso de la información, políticas de privacidad en cuanto a Información recopilada y protección de la información personal, confidencialidad, aceptación de los términos, Ley y Jurisdicción aplicable y uso del Portal por parte de los Menores de Edad. La Alcaldía de Pamplonita tiene un documento completo con La Política de Seguridad y Privacidad de la Información con el tratamiento a la protección de los activos de información (funcionarios, contratistas, terceros, información, procesos, tecnologías de información a nivel de hardware y

software), que soportan los procesos de la Entidad y apoyan la implementación del MSPI. (Política de Seguridad y Privacidad de la información Pamplonita, 2017).

La Alcaldía de San Cayetano tiene un manuscrito denominado Política de Seguridad y Privacidad para la estrategia de Gobierno en Línea. En el cual se presenta una estrategia de preparación por parte de la entidad para soportar al Sistema de administración de seguridad de la información de Gobierno en Línea (SASIGEL), como modelo sostenible que cubre tanto la preparación de la alcaldía para comenzar la implementación, la definición de brechas, así como la alineación e implementación con el SGSI, (Política de Seguridad y Privacidad de la información – San Cayetano, 2016). Así mismo La alcaldía del municipio de Teorama Norte de Santander, diseño un plan de seguridad y privacidad de la información con el objetivo de garantizar el buen tratamiento de datos y de información, controlar el uso eficiente y correcto de dichos activos, (Plan de Seguridad y Privacidad de la Información – Teorama, 2018).

Las entidades de alcaldía de los municipios de San José de Cúcuta, el Tarra, El Carmen, Pamplona, Pamplonita y San Cayetano, aunque cuentan con una política de seguridad y Privacidad de la información reglamentada y documentada, MinTIC, no reporta nivel de avance para estas en referencia al MSPI.

Por su parte, las alcaldías de Ábrego, Arboledas, Bochalema, Bucarasica, Cacota, Chinácota, Chitagá, Convención, Cucutilla, Durania, EL Zulia, Gramalote, Hacarí, Herrán, San Calixto, Labateca, La Esperanza, La Playa, Lourdes, Mutiscua, Ocaña Puerto Santander, Ragonvalia, Salazar de las Palmas, Ocaña, Santiago, Sardinata, Santo Domingo de Silos, Tibú y

Villa Caro, contienen una publicación en la página web que hace referencia a Políticas de seguridad de la información, en la cual regula los procedimientos relacionados con bases de datos, adquisición de información, copias de seguridad, registro de usuarios en el sitio web y gestión de sesiones segura. Por lo tanto, es posible evidenciar que la implementación del modelo de Seguridad y privacidad de la Información (MSPI), en este grupo de entidades, se encuentra actualmente en planeación.

2.2 Marco conceptual

A continuación, se definen algunos conceptos claves en los cuales se enmarca el desarrollo de la investigación.

Modelo: Es el resultado de generar una representación de sistemas a fin de analizar fenómenos o procesos (Saavedra y Torres Olaya, 2012). Por su parte Montaño (2014), lo define como: "un Estándar que debe ser aplicado tal y como fue concebido, y puede requerir de adecuaciones en procesos y estructuras por parte de una organización, para poder adoptarlo" (p.2).

Información: En un ambiente corporativo se entiende como: "los datos relevantes para el negocio: clientes, producción, ventas, comportamientos de consumo, desarrollo de productos, servicios ofrecidos, tendencias del mercado, costos, gastos" (Saavedra y Torres Olaya, 2012). La información es el activo más relevante de toda organización y se debe tomar todas las medidas para salvaguardarlo (Santiago y Sánchez, 2017, p.5).

Tecnologías de la información (TI): Hace referencia a la utilización de tecnología (computadoras y dispositivos electrónicos) para el manejo y procesamiento de información específicamente la captura, transformación, almacenamiento, protección, y recuperación de datos e información (Saavedra y Torres Olaya, 2012). Para Baca (2015) Conceptualiza el termino como: "aquellas herramientas que permiten el acceso, la organización, el procesamiento y el análisis de la información de manera óptima y fácil, de tal forma que su utilización implique ventajas competitivas para la empresa" (p.6).

Gobierno TI. Existe un número relevante de definiciones del concepto gobierno de TI. El ITGI (IT Governance Institute), refiere que: "el gobierno de las TI es una parte integral del gobierno de la organización y consiste en el liderazgo de las estructuras y procesos organizativos que aseguran que las TI de la organización sostienen y extienden la estrategia y los objetivos de la organización" (ITGI, 2003) (Ballester, 2010, p.1). Por su parte la norma ISO/IEC 38500:2008, precisa el gobierno de las TI como "el sistema por el que se dirige y controla la utilización actual y futura de la tecnología de la información" (ISO/IEC, 2008) (Ballester, 2010, p.1).

Gobierno corporativo de TIC (Corporate Governance of IT): Según ISACA, a través del ITGI Orozco (2014), define el concepto como: "Un conjunto de responsabilidades y prácticas ejecutadas por la junta directiva y la administración ejecutiva con el fin de proveer dirección estratégica, garantizando que los objetivos sean alcanzados, estableciendo que los riesgos son administrados apropiadamente y verificando que los recursos de la empresa son usados responsablemente". En relación, ISO/IEC 38500 lo conceptualiza como: "es el sistema a través del cual se dirige y controla el actual y futuro uso de las tecnologías de la información"

(Ballester, 2010, p.1,2). La Organización Europea para la Cooperación y el Desarrollo, OECD (2004), definen al gobierno corporativo como "el establecimiento de estructuras organizacionales que determinan los objetivos y la monitorización del desempeño de la organización para asegurar que los objetivos establecidos serán alcanzados. Esta estructura procura una supervisión y seguimiento de las decisiones de la alta dirección, representada en los consejos de administración, para proteger los intereses de los grupos de interés tanto internos como externos a la empresa" (Fernández y Llorens, 2014, p.35).

Parte interesada (Stakeholder): Ballester (2010), en concordancia con ISO/IEC 38500 conceptualizan el termino como: "individuo, grupo u organización que puede afectar, ser afectado, o percibir que va a ser afectado, por una decisión o una actividad" (p.2). De igual manera Freeman (1984), lo define como: "cualquier grupo o individuo que puede afectar o ser afectado por la consecución de los objetivos de la empresa" (p.25).

Principios fundamentales de la Seguridad de la Información. Confidencialidad. Sólo podrá acceder a la información personal autorizado (Gómez y Álvarez, 2012, p.IX). Es decir, solo pude ser conocida por las personas que previamente le han concedido privilegios sobre ella (Santiago y Sánchez, p.5).

Integridad. Hace referencia a que la información solo pude ser modificada dentro del marco de un proceso corporativo legítimo, por personal de la organización con privilegios, en un sitio autorizado, durante un lapso de tiempo (Santiago y Sánchez, p.5). Autor Gómez y Álvarez (2012), definen la integridad como lo exacto y completo de la información (p.IX).

Disponibilidad. Es la garantía que la información sensible de la organización estará accesible los 7 días de la semana, las 24 horas del día, por el personal con privilegios (Santiago y Sánchez, p.5). También se define como la accesibilidad a la información cuando se considere o requiera en los procesos del negocio (Gómez y Álvarez, 2012, p.IX).

Además de los principios o pilares de la información, existen otros mecanismos que apoyan el aseguramiento de la información como:

Autenticación. Proceso de verificación de la identidad del personal, así como los privilegios que tienen sobre los activos de información de las partes que intentan participar en una transacción (Santiago y Sánchez, 2017, p.6). Otra forma de definirlo es como la capacidad de reconocimiento de la identidad de un usuario, es decir si la persona es quien dice ser, para ser usuario autorizado (costas, 2014, p.28).

No Repudio o irrenunciabilidad. Hace referencia a un servicio de seguridad, relacionado estrechamente con la autenticación, para probar la participación de los actores en una comunicación, frente a un tercero (costas, 2014, p.28). Autores como Santiago y Sánchez (2017), definen el concepto como: "un servicio que proporciona la "no renuncia" de la responsabilidad de los actores que participan en una transacción en la cual se haga uso de algún activo de información. Este puede ser No repudio de Origen y/o No repudio de destino y está estandarizado en la ISO-7498-2" (p.6).

Trazabilidad. Registro de las acciones realizadas por un actor, al activo de información

de una organización (Santiago y Sánchez, 2017, p.6).

2.3 Marco Contextual

El Decreto 1008 de 2018, establece las políticas y lineamientos de Tecnología de Información, de estricto cumplimiento para las entidades que integran la administración pública de acuerdo con los términos de la Ley 489 de 1998, artículo 39, así como para los particulares que cumplen funciones administrativas. El proyecto de investigación "modelo de gobernanza de TI para las entidades del estado, como apoyo al cumplimiento del componente de Seguridad y Privacidad de la Información en el marco de la Política de Gobierno Digital", se enmarca en el contexto de las entidades públicas de orden territorial del departamento Norte de Santander, específicamente alcaldías, que quieran adoptar un modelo de gobernanza como apoyo al Modelo de Seguridad y Privacidad de la información.

De acuerdo con la división político-administrativa de Colombia – Divipola, el país está constituido por treinta y dos (32) departamentos, mil cientos uno (1.101) municipios, una (1) Isla de San Andrés, veinte (20) áreas no municipalizadas y seis mil novecientos veintiséis centros poblados (6926) (DANE, 2018)

El departamento Norte de Santander, se creó bajo la presidencia del General Ramón González Valencia, el 20 de julio de 1910 a partir de la expedición de la Ley 25 de 1910, nombrando como capital la ciudad de Cúcuta. Actualmente se encuentra conformado por los municipios de San José de Cúcuta, Ábrego, Arboledas, Bochalema, Bucarasica, Cácota, Cáchira, Chinácota, Chitagá, Convención, Cucutilla, Durania, El Carmen, El Tarra, El Zulia, Gramalote,

Hacarí, Herrán, Labateca, La Esperanza, La Playa, Los Patios, Lourdes, Mutiscua, Ocaña, Pamplona, Pamplonita, Puerto Santander, Ragonvalia, Salazar, San Calixto, San Cayetano, Santiago, Sardinata, Silos, Teorama, Tibú, Toledo, Villa Caro, Villa Del Rosario, (DANE, 2018). En su totalidad 40 municipios.

2.4 Marco Teórico

La expresión de gobierno de tecnología de la información, tiene su fundamentación en la suma de los conceptos "Gobierno", "Tecnología" e "Información". La Real Academia Española (RAE), define el termino gobernanza como "Arte o manera de gobernar que se propone como objetivo el logro de un desarrollo económico, social e institucional duradero, promoviendo un sano equilibrio entre el Estado, la sociedad civil y el mercado de la economía" (RAE, 2017). Muños (2011), retoma el concepto Gobierno como: "el elemento que resulta de organizar a las personas con el propósito de alcanzar los objetivos de la comunidad, de entre los cuales se destacan la protección del territorio, la seguridad de sus habitantes y su desarrollo integral".

Es relevante resaltar la relación directa que hay entre los términos gobierno corporativo y gobierno TI, debido a la correlación de estos en el cumplimiento de las actividades del objeto misional de la organización. Gobierno TI hace parte de Gobierno empresarial, Weill y Ross (20014), enmarcan en un modelo la asociación existente, como se evidencia en la figura 8. Donde es factible observar dicha relación, en el que la evolución de gobierno corporativo a gobierno TI, involucra en el proceso tanto al equipo ejecutivo, como al área de información y TI, mediante estrategias y optimización de conductas.

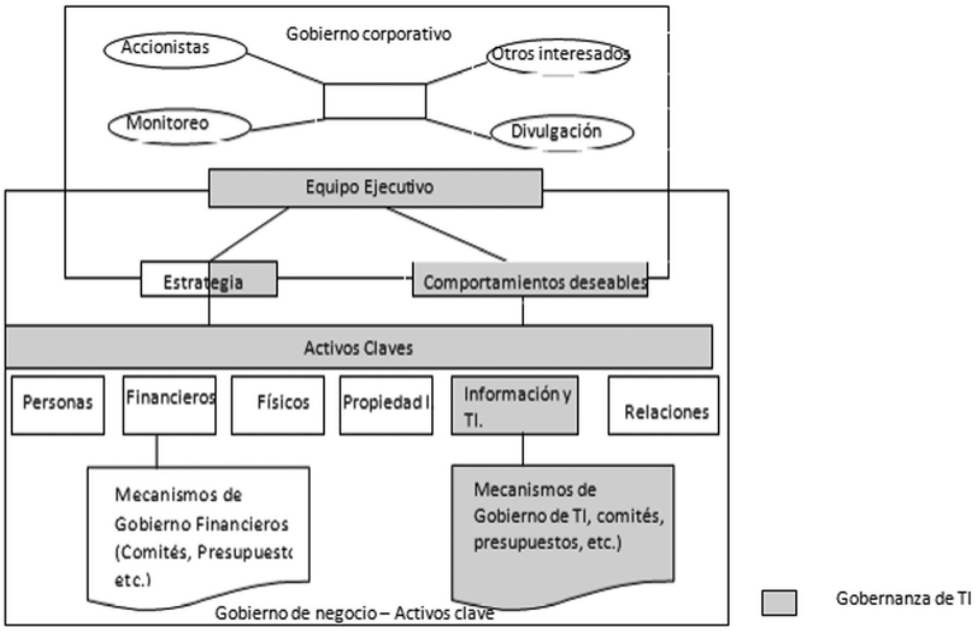

Figura 1. Modelo de Peter Weill y Jeanne W. Ross.
Fuente: (Weill y Ross, 2004).

Aunque Existen múltiples conceptos de gobierno TI, enfocados según el área de estudio de su autor, estos concuerdan en gestión y tecnología de información, ya que básicamente son la razón de ser del proceso.

El uso de la expresión gobierno de tecnología, tuvo sus inició en 1990, fue dado a conocer por primera vez por Loh y Venkatraman (1992) y referenciado posteriormente por Henderson y Venkatraman (1993), para describir el conjunto de componentes que certifican la capacidad de la tecnología de optimizar procesos propios del negocio y desde entonces este concepto ha ido evolucionando a definiciones más aceptadas. Luftman (1996), precisa que: “El gobierno de las TI es la selección y utilización de relaciones, tales como alianzas estratégicas, para alcanzar las principales competencias en TI”. Grembergem (2002), define: “El gobierno de las TI es la capacidad de la que dispone el Consejo de Dirección, la administración ejecutiva y la

administración de las TI para controlar la planificación y la implementación de estrategias de TI y así asegurar la alineación entre negocio y TI". Años más tarde, Grembergen y Guldentops (2004), afirma que "el gobierno de las TI se define como las estructuras de dirección y de organización, procesos y mecanismos de relación que aseguran que las TI den soporte y extiendan las estrategias y objetivos de la organización" (Vargas, 2017).

Por su parte IT Governance Insitute (ITGI) (2003): manifiesta que: "La gestión del gobierno de las TI es responsabilidad del consejo de administración y de la dirección ejecutiva. Es una parte integral de la gobernanza empresarial y consiste en el liderazgo y estructuras organizativas y procesos que aseguren que la organización de las TI sostiene y extiende las estrategias y objetivos organizacionales". De igual manera, Weill y Ross (2004): dicen que "El gobierno de las TI especifica los procedimientos de toma de decisiones y los esquemas de responsabilidad para alcanzar el comportamiento deseado en el uso de las TI". Otro concepto de gobierno de TI lo plantea ITGI (2008a), como: "el uso eficiente de los recursos de TI para apoyar el cumplimiento de los objetivos del negocio". (Muños, 2011).

El gobierno de TI integra y estandariza las buenas prácticas para garantizar que TI en la organización pueda soportar los objetivos del negocio y así mismo Facilite que la empresa aproveche su información, maximice los beneficios, capitalice las oportunidades y gane ventajas competitivas (Palao, 2010). Por lo tanto, la alta gerencia es la responsable del gobierno de TI. Los referentes anteriores permiten concluir que: "un buen gobierno de TI es crítico para asegurar que las decisiones de TI estén alineadas a los objetivos de la empresa" (Garbarino, 2010) (Muños, 2011).

El IT Governance Institute, establece cuatro principios fundamentales para el gobierno de TI (ITGI, 2007):

- Dirigir y controlar
- Responsabilidad
- Rendición de cuentas
- Actividades

El gobierno de TI tiene tanto actores internos como externos, con distintos requerimientos, a los que debe responder. Los internos agrupan la alta gerencia de la organización y de los procesos, así como auditores TI. Entre los externos se pueden mencionar clientes, auditores externos, proveedores, entes de control entre otros.

Las actividades del gobierno de TI se pueden agrupar en cinco áreas de enfoque que son ilustradas en la Figura 9 (ITGI, 2007):

Figura 2. Áreas de enfoque del gobierno de TI.
Fuente: (ITGI, 2007).

Tabla 2

Áreas de enfoque de gobierno de TI ITGI

Alineamiento estratégico	Se enfoca en asegurar el enlace de los planes del negocio y de TI; en definir, mantener y validar la proposición de valor de TI y en alinear las operaciones de TI con las operaciones de la empresa. Según el informe IT Governance Broad Briefing del ITGI (ITGI, 2003) la pregunta clave es si la inversión de una empresa de TI está en armonía con sus objetivos estratégicos (la intención, la estrategia actual y objetivos de la empresa) y por lo tanto la construcción de las capacidades necesarias para ofrecer un valor empresarial. Este estado de la armonía que se conoce como "la alineación." Es complejo, multifacético y nunca del todo logrado.
Entrega de valor	Se refiere a ejecutar la proposición de valor a través de todo el ciclo de entrega, asegurando que TI entrega los beneficios acordados alineados con la estrategia, concentrándose en la optimización de costos, y demostrando el valor intrínseco de TI. Según el informe IT Governance Broad Briefing del ITGI (ITGI, 2003) dice que la entrega de valor de las TI se traduce en entregar a tiempo y dentro del presupuesto. "El valor de IT está en el ojo del espectador".
Administración de riesgos	Requiere: - Conciencia de riesgo por parte de los directores superiores de la empresa. - Un claro entendimiento del apetito de riesgo de la empresa. - Un entendimiento de los requerimientos de cumplimiento. - Transparencia sobre los riesgos significativos de la empresa. - Implementar las responsabilidades de la administración de riesgos dentro de la organización.
Administración de recursos	Se refiere a la inversión óptima y a la adecuada administración de los recursos críticos de TI tales como: aplicaciones, información, infraestructura, datos.
Medición del desempeño	Da seguimiento y supervisa la estrategia de implementación, la finalización de proyectos, el desempeño de procesos y la entrega de servicio. Si no hay forma de medir y evaluar las actividades de TI, no es posible gobernarlas ni asegurar el alineamiento, la entrega de valor, la administración de riesgos y el uso efectivo de los recursos.

Fuente: (ITGI, 2007) (Muñoz, 2011).

Marcos de gobierno TI. Con el fin de lograr una relación eficiente entre los componentes de gobierno TI, se hace necesario el diseño de marcos, que permitan estructurar de manera organizada las operaciones, entre los cuales se encuentran:

Objetivos de control para la información y la tecnología relacionada (Control Objectives for Information and Related Technology - COBIT). Creado por IT Governance Institute - ITGI (ITGI, 2007; ITGI, 2008), evolucionando a través de un conjunto de adaptaciones y mejoras, pasando por COBIT 4.1 hasta llegar a COBIT 5 (ISACA, 2011; OGC, 2008). COBIT 5 provee: "un marco integral que ayuda a las empresas a alcanzar sus objetivos para el gobierno y la gestión de las TI corporativas, mediante la optimización de los niveles de riesgo y la gestión de recursos..." (ISACA, 2012).

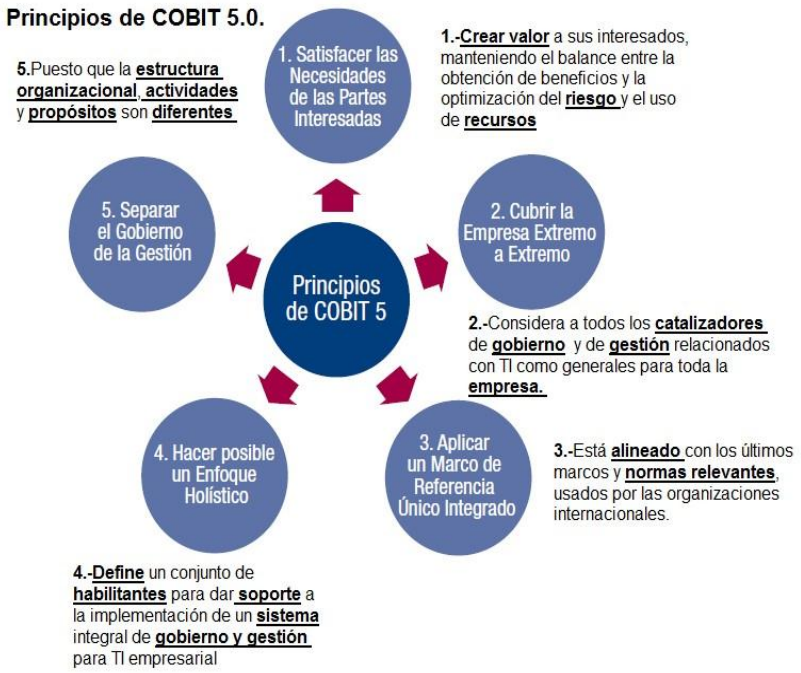

Figura 3. Principios COBIT 5.
Fuente: (ISACA, 2012).

COBIT 5 es una solución integral para todo tamaño y tipo de línea de negocio, ya que permite optimizar las inversiones realizadas en TI, asegura la entrega del servicio y define una medida como referencia para conocer el estado del proceso. Su uso asegura que TI satisfaga los requerimientos del negocio, debido a que se encuentra orientado a procesos en una estructura manejable de control más que de ejecución, estos controles parten de las necesidades de las partes interesadas tanto internas como externas, según sus 5 principios. Ver Figura Nro. 11(Espinoza Aguirre, 2016).

Primer principio "Satisfacer las necesidades de las partes interesadas", crear valor a las partes interesadas, manteniendo el equilibrio entre la obtención de beneficios y la optimización del riesgo, así como el uso de recursos. COBIT 5 "*convierte las metas de TI en objetivos de la empresa…*" (ISACA, 2012, p.14) dando un enfoque de cascada. Ver la Figura Nro.11.

Figura 4. Cascada de Metas de COBIT.
Fuente: (ISACA, 2012, p.18).

La cascada de metas de COBIT 5 estructura las necesidades de las partes interesadas en

objetivos corporativos y en metas relacionadas a TI. (ISACA, 2012, p.17)(Espinoza Aguirre, 2016).

Se apoya en los objetivos estratégicos institucionales:

- Se definen las necesidades de las partes interesadas, clasificándolas en 4 dimensiones (financiera, cliente, interna, aprendizaje), detalladas en el cuadro de mando integral (*Balanced Scorecard*). Para posteriormente ser mapeadas en metas empresariales (ISACA, 2012, p.14).
- Metas Corporativas: los objetivos de la organización se alinean a los objetivos de TI.
- Las metas de TI, se clasifican en 5 grupos de procesos:
    - Alinear, planifica y organizar.
    - Construir, Adquirir e Implementar.
    - Entregar dar servicio y soporte.
    - Evaluar, orientar y supervisar.
    - Supervisar evaluar y valorar.

El segundo principio “Cubrir la empresa extremo a extremo” (ISACA, 2012, p.14), abarca todos los catalizadores de gobierno y de gestión relacionados con TI generales para toda la organización.

El tercer principio "Aplicar un Marco de Referencia Único Integrado" (ISACA, 2012, p.13), alineado con los estándares y prácticas usadas por organizaciones internacionales en el ámbito como: ITIL, TOGAF, PMBOK, COSO, PRINCE2, ISO/IEC 38500, etc.

El cuarto principio "Hacer posible un Enfoque Holístico" (ISACA, 2012, p.14), estructura las habilidades que soportan la implementación de un sistema integral de gobierno y gestión para TI empresarial, a partir de 7 catalizadores. (ISACA, 2012, p. 15).

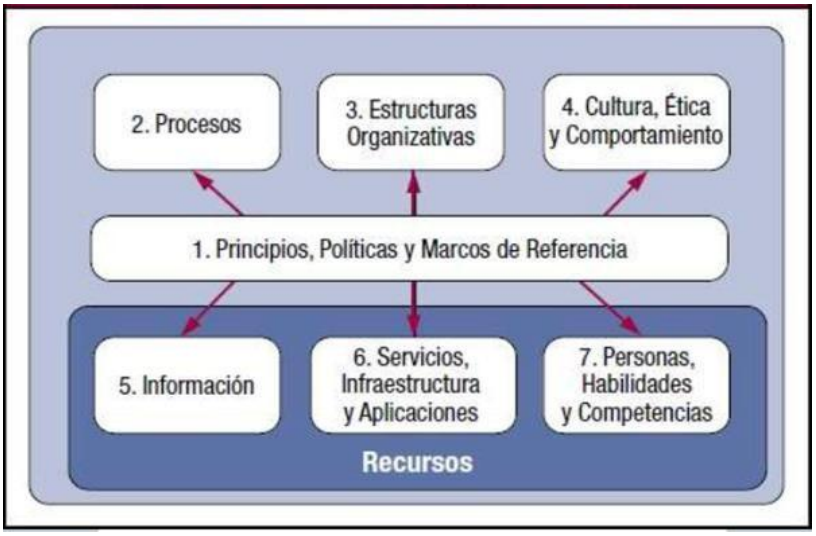

Figura 5. Siete Catalizadores de COBIT 5.
Fuente: (ISACA, 2012).

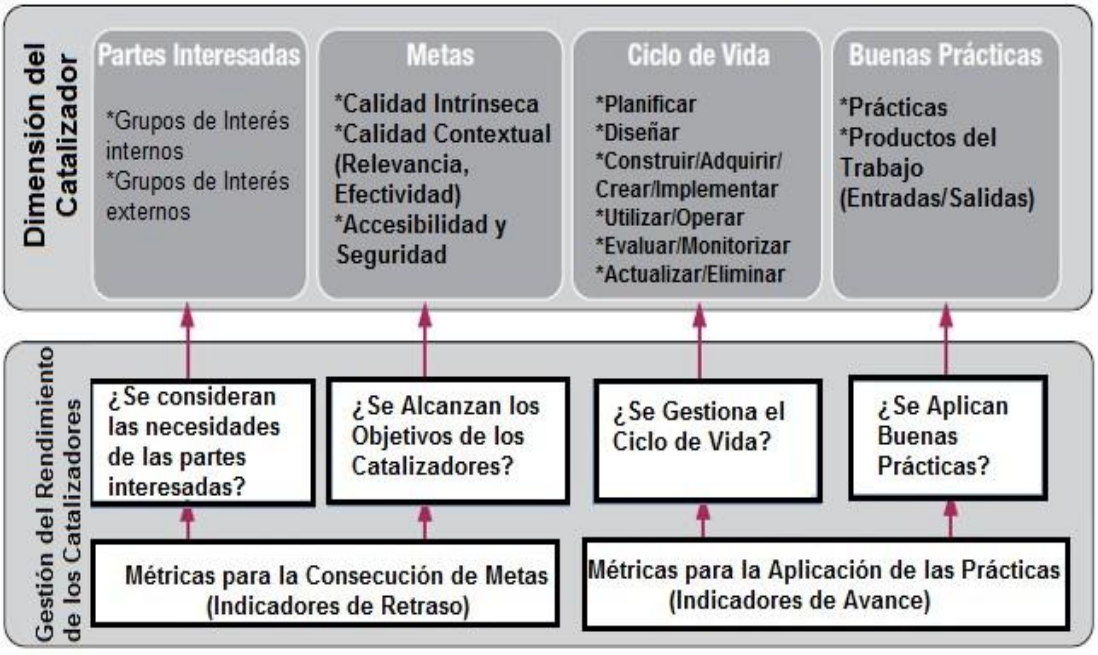

Figura 6. Dimensiones de los habilitantes de COBIT 5.
Fuente: (ISACA, 2012)

El quinto principio "Separar el Gobierno de la Gestión", teniendo en cuenta que la estructura organizacional, actividades y propósitos son diferentes, se encuentran divididos en el modelo de procesos.

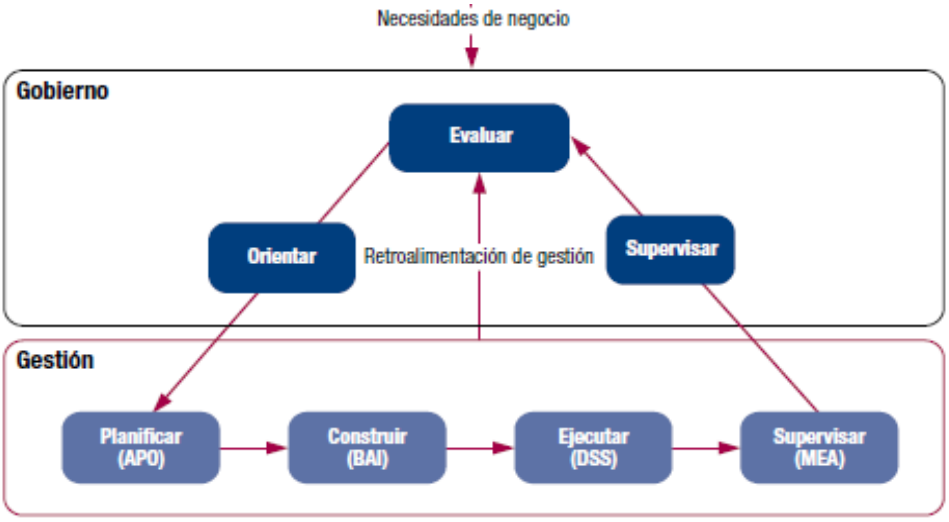

Figura 7. Dominios del Modelo de Referencia de procesos.
Fuente: (ISACA, 2012, p.32)

Gobierno está compuesto por: "cinco procesos de gobierno; dentro de cada proceso se define prácticas de evaluación, orientación y supervisión (EDM)" (ISACA, 2012, p.32). Mientras que la gestión "Contienen cuatro dominios, en consonancia con las áreas de responsabilidad de planificar, construir, ejecutar y supervisar (Plan, Build, Rund and Monitor-PBRM), y proporciona cobertura extrema a extremo de TI. (ISACA, 2012, p.32)(Espinoza, 2016)(Espinoza Aguirre, 2016)(Espinoza Aguirre, 2016)(Espinoza Aguirre, 2016)(Espinoza Aguirre, 2016)(Espinoza Aguirre, 2016).

Descripción de los dominios de COBIT versión 5.0. Los dominios del Estándar de Gobierno de TI definidos por ISACA para facilitar la Gobernanza y la gestión de las Tecnologías de la Información a nivel corporativo se describen a continuación:

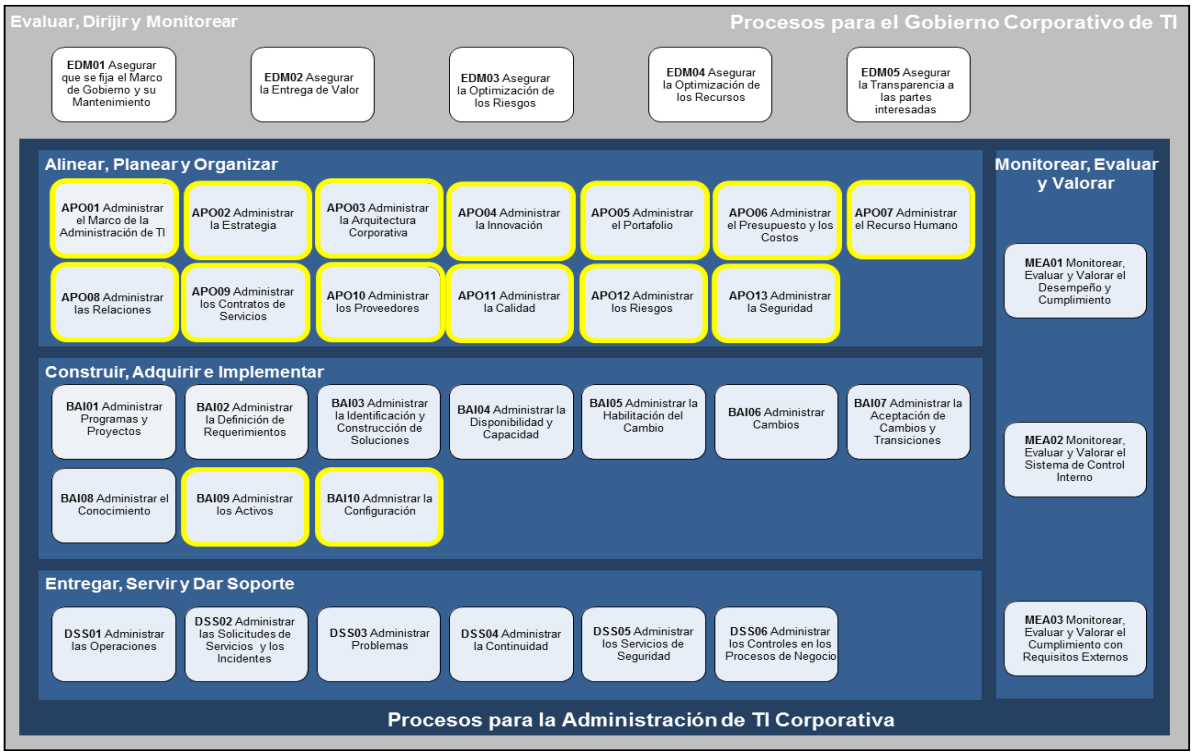

Figura 8. Dominios de COBIT versión 5.0.
Fuente: (ISACA, 2012, p.32)

Dominio de Gobierno. Contiene cinco (5) procesos de gobiernos y dentro de cada uno de estos se definen las prácticas para Evaluar, Dirigir y Monitorear (EDM).

Evaluar, Dirigir y Monitorear (EDM). Asegura que los objetivos de la organización se logren, evaluando las necesidades de las partes interesadas.

Procesos

- EDM01 Asegurar que se fija el marco de gobierno y su mantenimiento. Este Proceso se enfoca en: "analizar y articular los requerimientos para el gobierno de TI de la empresa, pone en marcha y mantiene efectivas las estructuras, procesos, práctica, facilitadores con claridad

de las responsabilidades y la autoridad para alcanzar la misión, las metas y los objetivos de la empresa" (ISACA, 2012).

- EDM02 Asegurar la entrega de valor o Entrega de beneficios. Hace referencia a: "Optimizar la contribución al valor del negocio desde los procesos de negocio, de los de servicios TI y activos de las TI resultado de la inversión hecha por TI a unos costes aceptables" (ISACA, 2012).
- EDM03 Asegurar la optimización de los riesgos. Consiste en: "Asegurar que el apetito y la tolerancia al riesgo de la empresa son entendidos, articulados y comunicados y que el riesgo para el valor de la empresa relacionado con el uso de las TI es identificado y gestionado" (ISACA, 2012).
- EDM04 Asegurar la Optimización de los Recursos. "Asegurar que las adecuadas y suficientes capacidades relacionadas con las TI (personas, procesos y tecnologías) están disponibles para soportar eficazmente los objetivos de la empresa a un coste óptimo" (ISACA, 2012).
- EDM05 Asegurar la Transparencia a las partes interesadas. "Asegurar que la medición y la elaboración de informes en cuanto a conformidad y desempeño de las TI de la empresa son transparentes, con aprobación por las partes interesadas de las metas, las métricas y las acciones correctivas necesarias" (ISACA, 2012).

Dominio de Gestión. Consta de cuatro (4) dominios de administración, están alineados con las áreas de responsabilidad de planificar, construir, ejecutar y monitorear (Plan, Build, Run and Monitor- PBRM), y proporciona una cobertura de extremo a extremo a TI en la organización.

Alinear, Planear y Organizar (APO). Este dominio está conformado por trece (13) procesos que cubren las estrategias y las tácticas, relacionadas con identificar la manera en que TI puede contribuir mejorar los objetivos del negocio. Es relevante mencionar que la realización de la visión estratégica requiere ser planeada, comunicada y administrada desde diferentes perspectivas; y finalmente, la implementación de una estructura organizacional y tecnológica apropiada.

Procesos

- APO01 Administrar el Marco de la Administración de TI. "Aclarar y mantener el gobierno de la misión y la visión corporativa de TI. Implementar y mantener mecanismos y autoridades para la gestión de la información y el uso de TI en la empresa para apoyar los objetivos de gobierno en consonancia con las políticas y los principios rectores" (ISACA, 2012).
- APO02 Administrar la Estrategia. "Proporcionar una visión holística del negocio actual y del entorno de TI, la dirección futura, y las iniciativas necesarias para migrar al entorno deseado. Aprovechar los bloques y componentes de la estructura empresarial, incluyendo los servicios externalizados y las capacidades relacionadas que permitan una respuesta ágil, confiable y eficiente a los objetivos estratégicos" (ISACA, 2012).
- APO03 Administrar la Arquitectura Corporativa." Establecer una arquitectura común compuesta por los procesos de negocio, la información, los datos, las aplicaciones y las capas de la arquitectura tecnológica de manera eficaz y eficiente para la realización de las estrategias de la empresa y de TI mediante la creación de modelos clave y prácticas que describan las líneas de partida y las arquitecturas objetivo. Define los requisitos para la taxonomía, las normas, las

directrices, los procedimientos, as plantillas y las herramientas y proporcionar un vínculo para estos componentes" (ISACA, 2012).

- APO04 Administrar la Innovación. "Analizar cuáles son las oportunidades para la innovación empresarial o qué mejora puede crearse con las nuevas tecnologías, servicios o innovaciones empresariales facilitadas por TI, así como a través de las tecnologías ya existentes y por la innovación en procesos empresariales y de TI. Influir en la planificación estratégica y en las decisiones de la arquitectura de empresa" (ISACA, 2012).
- APO05 Administrar el Portafolio. "Ejecutar el conjunto de direcciones estratégicas para la inversión alineada con la visión de la arquitectura empresarial, las características deseadas de inversión, los portafolios de servicios relacionados, considerar las diferentes categorías de inversión y recursos y las restricciones de financiación. Evaluar, priorizar y equilibrar programas y servicios, gestionar la demanda con los recursos y restricciones de fondos, basados en su alineamiento con los objetivos estratégicos, así como en su valor y riesgo corporativo. Supervisar el rendimiento global del portafolio de servicios y programas, proponiendo ajustes si fuesen necesarios en respuesta al rendimiento de programas y servicios o al cambio en las prioridades corporativas" (ISACA, 2012).
- APO06 Administrar el Presupuesto y los Costes. "Gestionar las actividades financieras relacionadas con las TI tanto en el negocio como en las funciones de TI, abarcando presupuesto, coste y gestión del beneficio, y la priorización del gasto mediante el uso de prácticas presupuestarias formales y un sistema justo y equitativo de reparto de costes a la empresa" (ISACA, 2012).
- APO07 Administrar el Recurso Humano. "Proporcionar un enfoque estructurado para garantizar una óptima estructuración, ubicación, capacidades de decisión y habilidades de los

recursos humanos. Esto incluye la comunicación de las funciones y responsabilidades definidas, la formación y planes de desarrollo personal y las expectativas de desempeño, con el apoyo de gente competente y motivada" (ISACA, 2012).

- APO08 Administrar las Relaciones. "Gestionar las relaciones entre el negocio y TI de modo formal y transparente, enfocándolas hacia el objetivo común de obtener resultados empresariales exitosos apoyando los objetivos estratégicos y dentro de las restricciones del presupuesto y los riesgos tolerables. Basar la relación en la confianza mutua, usando términos entendibles, lenguaje común y voluntad de asumir la propiedad y responsabilidad en las decisiones claves" (ISACA, 2012).
- APO09 Administrar los Contratos de Servicios. "Alinear los servicios basados en TI y los niveles de servicio con las necesidades y expectativas de la empresa, incluyendo identificación, especificación, diseño, publicación, acuerdo y supervisión de los servicios TI, niveles de servicio e indicadores de rendimiento" (ISACA, 2012).
- APO10 Administrar los Proveedores. "Administrar todos los servicios de TI prestados por todo tipo de proveedores para satisfacer las necesidades del negocio, incluyendo la selección de los proveedores, la gestión de las relaciones, la gestión de los contratos y la revisión y supervisión del desempeño, para una eficacia y cumplimiento adecuados" (ISACA, 2012).
- APO11 Administrar la Calidad. "Definir y comunicar los requisitos de calidad en todos los procesos, procedimientos y resultados relacionados de la organización, incluyendo controles, vigilancia constante y el uso de prácticas probadas y estándares de mejora continua y esfuerzos de eficiencia" (ISACA, 2012).

- APO12 Administrar los Riesgos. “Identificar, evaluar y reducir los riesgos relacionados con TI de forma continua, dentro de niveles de tolerancia establecidos por la dirección ejecutiva de la empresa” (ISACA, 2012).
- APO13 Administrar la Seguridad. “Definir, operar y supervisar un sistema para la gestión de la seguridad de la información” (ISACA, 2012).

Construir, Adquirir e Implementar (BAI). Este dominio como su nombre lo indica es el encargado de diseñar e implementar las soluciones que indica APO. La alta dirección pretende con este dominio que los nuevos proyectos generen soluciones que permitan satisfacer las necesidades del negocio, dentro del presupuesto y tiempos establecidos. Adicional, que los nuevos sistemas una vez implementados funcionen de manera satisfactoria y los cambios no afecten las operaciones actuales del negocio. Con el objeto de cumplir una estrategia de Tecnología de Información, la solución de TI requiere ser identificadas, desarrolladas o adquiridas, implementadas e integradas en los procesos del negocio.

Procesos

- BAI01 Administrar Programas y Proyectos. “Gestionar todos los programas y proyectos del portafolio de inversiones de forma coordinada y en línea con la estrategia corporativa. Iniciar, planificar, controlar y ejecutar programas y proyectos y cerrarlos con una revisión post-implementación” (ISACA, 2012).
- BAI02 Administrar la Definición de Requerimientos. “Identificar soluciones y analizar requerimientos antes de la adquisición o creación para asegurar que estén en línea con los

requerimientos estratégicos de la organización y que cubren los procesos de negocios, aplicaciones, información/datos, infraestructura y servicios" (ISACA, 2012) .

- BAI03 Administrar la Identificación y Construcción de Soluciones. "Establecer y mantener soluciones identificadas en línea con los requerimientos de la empresa que abarcan el diseño, desarrollo, compras/contratación y asociación con proveedores/fabricantes. Gestionar la configuración, preparación de pruebas, realización de pruebas, gestión de requerimientos y mantenimiento de procesos de negocio, aplicaciones, datos/información, infraestructura y servicios" (ISACA, 2012).
- BAI04 Administrar la Disponibilidad y Capacidad. "Equilibrar las necesidades actuales y futuras de disponibilidad, rendimiento y capacidad con una provisión de servicio efectiva en costes. Incluye la evaluación de las capacidades actuales, la previsión de necesidades futuras basadas en los requerimientos del negocio" (ISACA, 2012).
- BAI05 Administrar la Habilitación del Cambio. "Maximizar la probabilidad de la implementación exitosa en toda la empresa del cambio organizativo de forma rápida y con riesgo reducido, cubriendo el ciclo de vida completo del cambio y todos las partes interesadas del negocio y de TI" (ISACA, 2012).
- BAI06 Administrar Cambios. "Gestiona todos los cambios de una forma controlada, incluyendo cambios estándar y de mantenimiento de emergencia en relación con los procesos de negocio, aplicaciones e infraestructura. Esto incluye normas y procedimientos de cambio, análisis de impacto, priorización y autorización, cambios de emergencia, seguimiento, reporte, cierre y documentación" (ISACA, 2012).
- BAI07 Administrar la Aceptación de Cambios y Transiciones. "Aceptar formalmente y hacer operativas las nuevas soluciones, incluyendo la planificación de la implementación, la

conversión de los datos y los sistemas, las pruebas de aceptación, la comunicación, la preparación del lanzamiento, el paso a producción de procesos de negocio o servicios TI nuevos o modificados, el soporte temprano en producción y una revisión post-implementación" (ISACA, 2012).

- BAI08 Administrar el Conocimiento. "Mantener la disponibilidad de conocimiento relevante, actual, validado y fiable para dar soporte a todas las actividades de los procesos y facilitar la toma de decisiones. Planificar la identificación, recopilación, organización, mantenimiento, uso y retirada de conocimiento" (ISACA, 2012).
- BAI09 Administrar los Activos. "Gestionar los activos de TI a través de su ciclo de vida para asegurar que su uso aporta valor a un coste óptimo, que se mantendrán en funcionamiento, que están justificados y protegidos físicamente, y que los activos que son fundamentales para apoyar la capacidad del servicio son fiables y están disponibles. Administrar las licencias de software para asegurar que se adquiere el número óptimo, se mantienen y despliegan en relación con el uso necesario para el negocio y que el software instalado cumple con los acuerdos de licencia" (ISACA, 2012).
- BAI10 Administrar la Configuración. "Definir y mantener las definiciones y relaciones entre los principales recursos y capacidades necesarios para la prestación de los servicios proporcionados por TI, incluyendo la recopilación de información de configuración, el establecimiento de líneas de referencia, la verificación y auditoría de la información de configuración y la actualización del repositorio de configuración" (ISACA, 2012).

Entregar, Servir y Dar Soporte (DSS). Procesos de dominios de soporte y entrega, que involucra la entrega en sí de los servicios requeridos, entre los cuales se encuentra la prestación

del servicio, la administración de la seguridad y de la continuidad, el soporte a los usuarios del servicio, la administración de los datos y de las instalaciones operativas. Proceso que integra los componentes necesarios para una adecuada administración y soporte de TI. El dominio DSS facilita la gestión y adecuada administración de los servicios de TI en la organización.

Procesos

- DSS01 Administrar las Operaciones. “Coordinar y ejecutar las actividades y los procedimientos operativos requeridos para entregar servicios de TI tanto internos como externalizados, incluyendo la ejecución de procedimientos operativos estándar predefinidos y las actividades de monitorización requeridas” (ISACA, 2012).
- DSS02 Administrar las Solicitudes de Servicios y los Incidentes. “Proveer una respuesta oportuna y efectiva a las peticiones de usuario y la resolución de todo tipo de incidentes. Recuperar el servicio normal; registrar y completar las peticiones de usuario; y registrar, investigar, diagnosticar, escalar y resolver incidentes” (ISACA, 2012).
- DSS03 Administrar Problemas. “Identificar y clasificar problemas y sus causas raíz y proporcionar resolución en tiempo para prevenir incidentes recurrentes. Proporcionar recomendaciones de mejora” (ISACA, 2012).
- DSS04 Administrar la Continuidad. “Establecer y mantener un plan para permitir al negocio y a TI responder a incidentes e interrupciones de servicio para la operación continua de los procesos críticos para el negocio y los servicios TI requeridos y mantener la disponibilidad de la información a un nivel aceptable para la empresa” (ISACA, 2012).

- DSS05 Administrar los Servicios de Seguridad. “Proteger la información de la empresa para mantener aceptable el nivel de riesgo de seguridad de la información de acuerdo con la política de seguridad. Establecer y mantener los roles de seguridad y privilegios de acceso de la información y realizar la supervisión de la seguridad” (ISACA, 2012).
- DSS06 Administrar los Controles en los Procesos de Negocio. “Definir y mantener controles apropiados de proceso de negocio para asegurar que la información relacionada y procesada dentro de la organización o de forma externa satisface todos los requerimientos relevantes para el control de la información” (ISACA, 2012).

Monitorear, Evaluar y Valorar (MEA). El dominio MEA, incluye tres (3) procesos que contienen la administración del desempeño, el monitoreo del control interno, la conformidad y la aplicación del gobierno. Los procesos de TI deben de ser evaluados periódicamente, para conocer su calidad y cumplimiento de los requerimientos de control.

Procesos

- MEA01 Monitorear, Evaluar y Valorar el Desempeño y Cumplimiento. “Recolectar, validar y evaluar métricas y objetivos de negocio, de TI y de procesos. Supervisar que los procesos se están realizando acorde al rendimiento acordado y conforme a los objetivos y métricas y se proporcionan informes de forma sistemática y planificada” (ISACA, 2012).
- MEA02 Monitorear, Evaluar y Valorar el Sistema de Control Interno. “Facilitar a la Dirección la identificación de deficiencias e ineficiencias en el control y el inicio de acciones de mejora. Planificar, organizar y mantener normas para la evaluación del control interno y las actividades de aseguramiento” (ISACA, 2012).

- MEA03 Monitorear, Evaluar y Valorar el Cumplimiento con Requisitos Externos. “Evaluar el cumplimiento de requisitos regulatorios y contractuales tanto en los procesos de TI como en los procesos de negocio dependientes de las tecnologías de la información. Obtener garantías de que se han identificado, se cumple con los requisitos y se ha integrado el cumplimiento de TI en el cumplimiento de la empresa general” (ISACA, 2012).

ISO 38500 Corporate Governance of Information Technology. La norma ISO 38500, tiene su origen en el año 2005, fundamentada en la norma Australiana AS8015:2005, publicada en junio de 2008 y adoptada posteriormente por la ISO/IEC, dando lugar a la norma en referencia. El objetivo de esta norma es: “Proveer un marco de principios y buenas prácticas a la hora de evaluar, dirigir y controlar la utilización de TI en las organizaciones” (Garbarino, 2014). Entre los principios que establece para ofrecer un buen gobierno corporativo de TI se encuentran: Responsabilidad, estrategia, adquisición, desempeño, conformidad y comportamiento humano (ISO/IEC, 2008, Sylvester, 2011) (Garbarino, 2014).

El modelo de buen gobierno corporativo de TI, se basa en tres actividades primordiales: evaluar el uso actual y futuro de las TI, liderar la preparación directa e implementación de planes y políticas para garantizar que el uso de las TI cumple con los objetivos de negocio, supervisar la conformidad con las políticas y el desempeño frente a los planes.

Alcance, aplicación y objetivos. ISO/IEC 38500:2013 define una serie de principios que pueden ser aplicados en cualquier de las entidades, tanto públicas como privadas, sin ánimo de

lucro o entidades gubernamentales, independiente de su tamaño o sector (Ballester, 2010). Así como del nivel de alcance de su uso de TI en la organización (ISO / IEC, 2015).

El propósito de este estándar es:

- Promover el asesoramiento de las actividades de gobierno TI en la alta dirección de las organizaciones.
- Conseguir el apoyo y confianza de las partes interesadas (stakeholders), a través de la realización correcta de las actividades de gobierno en la implantación de la norma.
- Proporciona las bases para realizar la evaluación objetiva del Gobierno de las TI.

Beneficios. Los beneficios principales que puede obtener una gobernación con la implementación y seguimiento de ISO/IEC 38500, son:

- **Conformidad**. El nivel directivo que ejerza un adecuado gobierno sobre las TI podrá reaccionar y abordar de manera más adecuada los riesgos asociados con la seguridad de la información, ley de protección de datos, propiedad intelectual, responsabilidad social corporativa entre algunos de ellos. Dando cumplimiento así a la normatividad legal vigente.
- **Gestión de costes eficiente.** Un Buen gobierno TI también tiene la responsabilidad de generar beneficios, a través del funcionamiento adecuado de los activos TI, continuidad del negocio, alineación de TI con sus necesidades, asignación eficiente de recursos, etc. En algunas ocasiones

se debe tomar la decisión de asumir riesgos económicos pues el retorno de inversión no está siempre está asegurado.

Principios de la Norma ISO/IEC 38500. La norma identifica seis (6) principios de buen gobierno corporativo de TI. Cada principio establece una serie de directrices generales para guiar la toma de decisiones. No obstante, estas indicaciones, no describen algún tipo de actividad o proceso alguno para su implementación. Por lo cual el cómo hacerlo depende de los criterios de los usuarios de cada organización en la que se vayan a aplicar.

- **Responsabilidad**. Los encargados de Tecnología de la Información (TI) en la organización deben comprender y aceptar las responsabilidades sobre las acciones y medidas que requiere el desarrollo de las actividades asignadas.
- **Estrategia**. La estrategia de negocio debe satisfacer las necesidades presentes y futuras de TI y de la organización, las cuales deben estar alineadas.
- **Adquisición**. Analizar las necesidades de la inversión y evaluar la relación coste y beneficio, así como los riesgos.
- **Desempeño**. Las tecnologías de la información deben proporcionar servicios que satisfagan las necesidades presentes y futuras.
- **Conformidad**. Cumplir con los requerimientos del marco regulatorio y normatividad vigente.
- **Conducta Humana**. Definir las políticas, prácticas y decisiones enfocadas al respeto del talento humano.

El Modelo de gobierno definido por la norma UNE- ISO/IEC 38500, se ilustra en la figura 9.

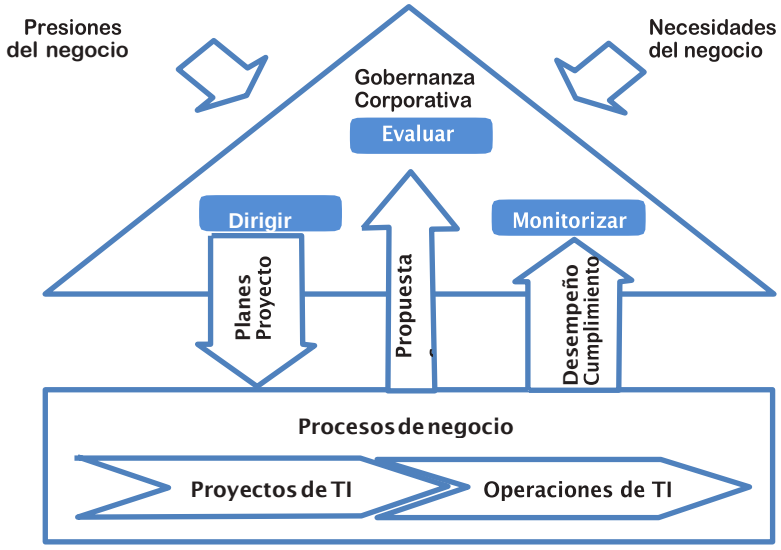

Figura 9. Modelo de gobierno corporativo de las TI.
Fuente: (ISO/IEC, 2008).

El modelo define tres acciones principales para el gobierno de TI. Evaluar, dirigir y monitorizar.

- Evaluar el uso actual y futuro de TI, incluyendo estrategias, planes de implementación, acuerdos de aprovisionamiento, etc.
- Dirigir la ejecución y cumplimiento de planes y políticas de TI, con el fin de asegurar que su uso satisface los objetivos de la organización.
- Monitorizar mediante sistemas de medición, el cumplimiento de las políticas y rendimiento de TI, asegurando que esté de acuerdo con lo planificado.

Modelo de Seguridad y Privacidad de la Información (MSPI). El también llamado MSPI, es un Modelo definido por el Ministerio de las TIC y alineado con la política de Gobierno Digital, descrita en el decreto 1008 del 2018 es el resultado de la fusión entre los

principales elementos de la Norma ISO/IEC 27000 junto con el Framework de Ciberseguridad del NIST , los fundamentos de la Arquitectura Empresarial, las mejores prácticas de ITIL y los lineamiento del estado Colombiano con respecto a la privacidad de la información y el tratamiento de datos personales definido por la ley 1581 del 2012.

El Objetivo principal de este Modelo es el definir los lineamientos y proporcionar las herramientas mínimas necesarias para ayudar a las organizaciones del sector Gobierno y a las del sector privado que así lo deseen, a gestionar la Seguridad y la privacidad de la información generada internamente dentro de sus procesos corporativos al igual que la entregadas por las otras organizaciones. Dicho de otra manera, la adopción correcta del MSPI permite que se reduzca el riesgo del compromiso de los activos de información y se brinden las garantías en términos de la confidencialidad, integridad y disponibilidad de estos.

El MSPI está basado en el ciclo de mejora continua adoptado por varios sistemas de gestión y conocido como el Ciclo de DEMING tal como su modelo principal de referencia ISO 27000.

Figura 10. Ciclo de Deming.
Fuente: Autor del proyecto

Este ciclo de mejora continua permite que se pueda realizar la adopción, gestión y afinamiento permanente de las actividades encaminadas a reducir la exposición a múltiples amenazas que podrían afectar la seguridad de la información.

En concordancia con el ciclo de mejora continua, las actividades del modelo en cuestión, están distribuidas en cuatro (4) fases posteriores a la de Diagnostico. Para facilitar la adopción del MSPI, el Ministerio de las TIC ha dispuesto una serie de guías alcanzables a través del URL:

Las fases deben ejecutarse de forma secuencial, ya que los resultados obtenidos en cada fase son empleados como entradas para la fase siguiente.

A continuación, se describen las Fases del Modelo de Seguridad y Privacidad de la Información definido por los lineamientos del Gobierno Digital.

***Figura** 11*. Fases de la Adopción del MSPI.
Fuente: Autor del proyecto

Fase de Diagnostico. Este Modelo de Seguridad y Privacidad de la Información requiere la ejecución de una fase previa a la planificación, llamada fase de diagnóstico que tiene como fin determinar el estado actual de la organización con respecto al cumplimiento de los lineamientos de seguridad y privacidad de la información definidos por el estado colombiano.

Las principales actividades de esta fase son:

- Identificar el Estado actual de la Entidad en cuanto a los lineamientos de Seguridad del Estado.
- Identificación del Nivel de Madurez de la organización con respecto al cumplimiento de los lineamientos de seguridad y la adopción del MSPI.
- Levantamiento de información referente a los principales activos de la organización.
- Identificación de las principales vulnerabilidades y amenazas a las que están expuestos los principales procesos y activos de información al igual que la efectividad de los controles implementados (si existen).

El levantamiento de información y la identificación de fallos técnicos y administrativos de los procesos corporativos y de los activos de información, se realiza aplicando la metodología de pruebas de efectividad, definida por MinTIC como parte del modelo de seguridad. Esta metodología se aprecia en la figura siguiente:

Figura 12. Componentes de la metodología de pruebas de efectividad **(MinTIC, 2016)**.
Fuente: MinTIC

Fase de Planificación. Una vez finalizado el diagnostico e identificado el análisis GAP (brecha o diferencia entre un estado ideal y el estado actual identificado), entre los requerimientos del MSPI y el estado actual de la seguridad de la información en la organización, se procede con la definición de la estrategia referente a la planificación de la adopción del Modelo de Seguridad y privacidad de la Información que incluye:

- Determinar el Contexto de la Organización
- Liderazgo
- Planificación
- Soporte

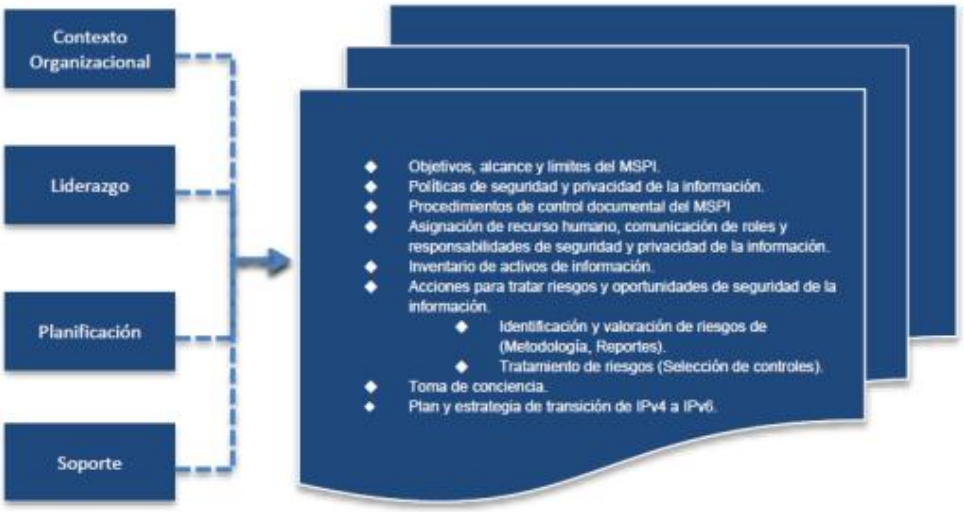

Figura 13. Principales componentes de la fase de Planificación **(Findeter, 2018)**.
Fuente: Documento Modelo de Seguridad y Privacidad de la Información estrategia de Gobierno en Línea – Findeter.

En esta etapa se definen los lineamientos, se definen las bases y se construyen los instrumentos necesarios que facilitaran la implementación del MSPI.

A continuación, se relacionan las principales actividades de la fase de Planificación.

- La definición los objetivos, del alcance y de los límites del SGSI.
- Se asignan los responsables de la gestión de la Seguridad y la privacidad de la información.
- Se construyen las políticas de seguridad de la Información.
- Definir el plan de capacitación, comunicación y sensibilización del nuevo SGSI contenidos en las políticas de seguridad.
- Se construye la documentación requerida para la operación del SGSI que incluye:
    - Procedimientos de seguridad de la información:
        - Procedimiento de control de documentos

- Procedimiento para auditorías internas
- Procedimiento para la clasificación de activos
- Procedimiento para la gestión de incidentes de seguridad de la información.
- Procedimiento de gestión de llaves criptográficas
- Procedimientos de Backup.
- Otros procedimientos.
  - Formatos, instructivos y demás documentación requerida por el MSPI

- Se realiza el inventario y la clasificación de activos de información.
- Se realiza el análisis de riesgos al que están expuestos los activos de información.
- Se construye el plan de tratamiento de riesgos
- Construcción del plan de diagnóstico referente a la transición del direccionamiento IPv4 actual a IPv6.

Fase de Implementación. En esta fase se procede a operacionalizar los lineamientos definidos en la planificación al igual que las políticas, procedimientos y demás instrumentos construidos en la fase anterior.

Figura 14. Principales componentes de la fase de Implementación **(Findeter, 2018)**.
Fuente: Documento Modelo de Seguridad y Privacidad de la Información estrategia de Gobierno en Línea – Findeter.

A continuación, se relacionan las principales actividades referentes a la Implementación del MSPI:

- Realizar la planificación y el control de la operación corporativa
- Realizar la Implementación de los planes de:
  - Tratamiento de riesgos (resultante del análisis de riesgos)
  - plan de capacitación, comunicaciones y sensibilización.
  - Entre otros.
- Implementar los procedimientos de:
  - Control de documentos
  - Backups
  - Gestión de incidentes de seguridad
  - Auditorías internas
  - Gestión de llaves criptográficas.
  - Seguridad en las Operaciones.
  - Entre otros.
- Definir los indicadores de gestión que permitan medir el cumplimiento de los lineamientos del SGSI. Tales como:
  - La efectividad de los controles
  - La Eficiencia del SGSI adoptado
  - Proveer los estados de seguridad de los principales componentes del sistema
  - Entre otros.
- Definir la estrategia del plan de implementación del direccionamiento IPv6 en la plataforma de TI.

Las actividades más importantes de esta fase están orientadas al tratamiento del riesgo identificado, basados en las necesidades de seguridad de la información y en la declaración de aplicabilidad previamente construida, como también en la puesta en producción de las medidas de seguridad y controles técnico- administrativos que faciliten la ejecución de los procesos de negocio y el resto de la operación corporativa de forma segura.

Fase de Evaluación de desempeño. Una vez finalizada la implementación, el MSPI define que debe llevarse a cabo el seguimiento y la monitorización del nuevo SGSI.

***Figura** 15.* Principales componentes de la fase de Evaluación de Desempeño **(Findeter, 2018)**.
Fuente: Documento Modelo de Seguridad y Privacidad de la Información estrategia de Gobierno en Línea – Findeter.

Esta medición del desempeño se realiza a partir del resultado de los indicadores de gestión que miden la efectividad, la eficiencia y la eficacia de las acciones implementadas en la fase anterior.

Las principales actividades de esta fase se relacionan a continuación:

- Monitoreo, medición, análisis y evaluación del plan de tratamiento de riesgos a partir de la medición de la efectividad de los controles técnicos y demás contramedidas administrativas adoptadas por la organización.
- Revisión de la efectividad del SGSI por parte de la alta dirección.

Fase de Mejora continua. En esta fase, se toman los resultados obtenidos de la monitorización, medición y evaluación del nuevo SGSI como parámetros de entrada para diseñar un plan para el mejoramiento continuo de la postura de seguridad de la organización.

La fase se centra en la ejecución de:

- Las Acciones correctivas requeridas
- La Mejora continua del sistema de gestión de seguridad.

***Figura** 16*. Principales componentes de la fase de Mejora Continua **(Findeter, 2018)**.
Fuente: Documento Modelo de Seguridad y Privacidad de la Información estrategia de Gobierno en Línea – Findeter.

Las principales actividades de esta fase son:

- La creación de un plan de mejoramiento del SGSI
- El plan de comunicación de los resultados

- Realización de los ajustes necesarios a las políticas, procedimientos, controles y demás elementos del SGSI.

Modelo de Madurez del Modelo de Seguridad y Privacidad de la Información (MSPI). El modelo, permite identificar el estado actual del nivel de madurez del MSPI, en el que están las entidades. La valoración se realiza a través de seis niveles, denominados como, inexistente, inicial, repetible, definido, administrado y optimizado. Cada uno esta enumerado en su orden respectivo desde nivel cero al cinco, como lo ilustra la figura 7. (MinTIC, 2015) (Useche, 2016).

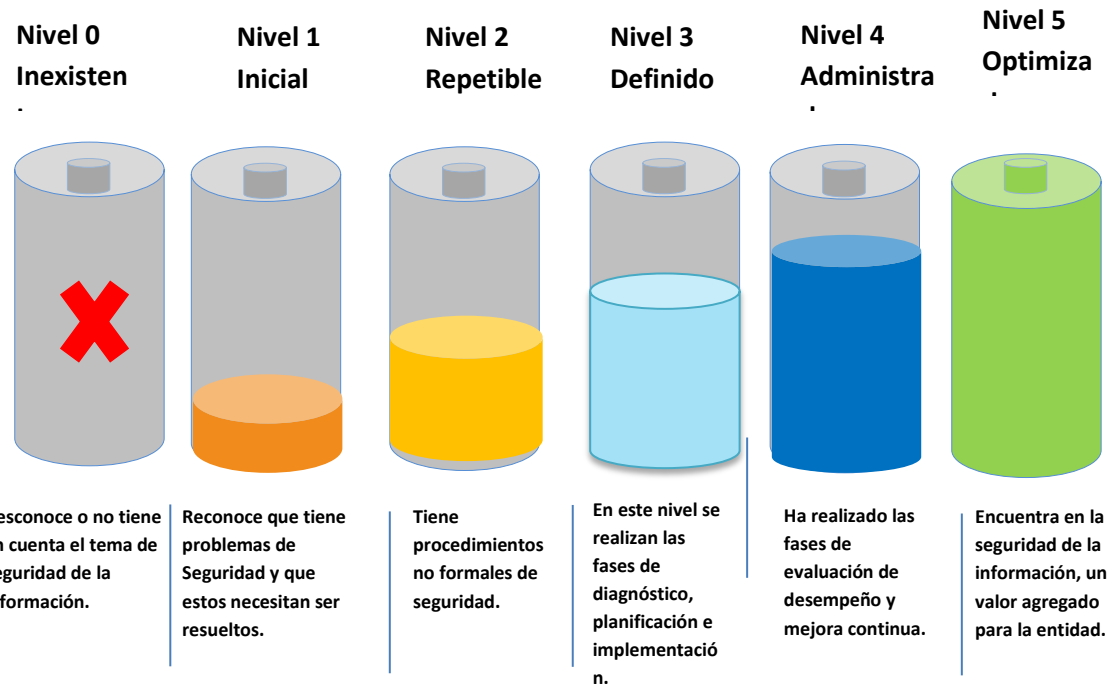

***Figura** 17*. Niveles de madurez del MSPI.
Fuente: MinTIC (2015).

Normas y estándares de gobierno TI

PMBok. Un grupo de profesionales en el año 1969 fundaron el Instituto de Gerencia de Proyectos (PMI) (PMI, 2012; PMI, 2008), constituyéndose como una asociación profesional sin ánimo de lucro, que se encarga de reunir las mejores prácticas a nivel internacional en gerencia de proyectos, diseñando la guía PMBok. Según PMBok, un proyecto se define como un esfuerzo temporal que se lleva a cabo para crear un producto, servicio o resultado único (Paliza, 2009). Y La dirección de proyectos como la aplicación de conocimientos, habilidades, herramientas y técnicas a aplicar en las actividades del proyecto para cumplir con los requisitos del mismo (PMI, 2008, p.12).

La guía consta de 42 procesos de la dirección de proyectos; agrupados en 5 grandes procesos (Sparano, 2011): Initiating processes, planing processes, closing processes, executing processes y monitoring y controlling processes (PMI, 2008, p.43), vinculados entre sí a través de los resultados, donde las salidas de unos, son las entradas de otros.

CMMI (Capability Maturity Model Integration). El Instituto de Ingeniería de Software (Software Engineering Institute) conocido como SEI (SEI, 2012a), es el que creó y mantiene el modelo de calidad CMM – CMMI (Gracia, 2005) (ISACA, 2012). La primera versión tiene como enfoque el área de software; evolucionando hasta incluir las áreas de Adquisición (SEI, 2012c) y Servicios (SEI, 2012d). CMM - CMMI es un modelo de calidad del software, que clasifica las empresas de acuerdo con los niveles de madurez procesos, que permiten medir los procesos que se realizan para producir software, buscando su optimización (Gracia, 2005).

Actualmente existen dos áreas de interés: Desarrollo y Adquisición. Definiendo dos formas de organización, el escalonado y el continuo, su uso depende de las características de la organización.

ISO 20000. La ISO (International Organization for Standards) y la IEC (International Electrotechnical Commission), en diciembre del 2005, realizaron la publicación de la ISO 20000 - Norma para la Calidad de la Gestión de Servicios TI. La cual se basa en el modelo de referencia " Information Technology Infrastructure Library" (ITIL) y el estándar británico BS 15000. Situación que permite completa compatibilidad del estándar en referencia con ITIL 3.1 (Martínez, 2010) (Aenonor, 2009) (Garbarino, 2014). La ISO 20000, promueve: "la adopción de un modelo de procesos integrados destinado a mejorar la eficacia en la prestación de los servicios tecnológicos y establece las directrices para una gestión de servicios de TI de calidad" (Turbitt, 2006) (Garbarino, 2014) (Vargas, 2014).

ISO/IEC 20000:2005 está codificado en dos documentos ISO/IEC 20000-1 (2005) e ISO/IEC 20000-2 (2005), bajo el título Gestión de Servicio de Tecnología de la Información. La ISO/IEC ISO 20000-1 (2005), contiene la fundamentación teórica de los lineamientos a adoptar para gestionar los servicios de TI. Por su parte la ISO/IEC 20000-2 (2005), describe las mejores prácticas para la gestión de los servicios TI, basado en el referente del primer documento (Vargas, 2014).

ITIL (Information Technology Infraestructure Library). ITIL describe un conjunto de buenas prácticas para la gestión de servicios TI. Fue creado en los años 80, por la CCTA (Central

Computing and Telecommunications Agency), como respuesta a una necesidad del gobierno británico. ITIL entrega una serie de libros donde define las mejores prácticas y lineamientos para la gestión de servicios TI. En sus primeras versiones el compendio de estos superaba los treinta, y fue evolucionando hasta llegar a su tercera versión, llamada ITIL v3, sintetizándose en un conjunto de cinco libros denominados: ITIL service strategy, ITIL service design, ITIL Service Transition, ITIL Service Operation, ITIL Continual Service Improvement.

2.5 Marco Legal

De acuerdo con la normativa en Colombia, desde la década de los años 90, se viene hablando de la temática gestión pública, estatutos anti tramites y del derecho fundamental que tienen las personas a conservar su intimidad personal y familiar, el buen nombre, así como conocer, actualizar y rectificar la información que se haya almacenado en bancos de datos y en archivos de las entidades públicas y privadas, consagrado en el artículo 15 de la Constitución Política de Colombia.

El 28 de agosto del año 2000, el Gobierno nacional genera el plan de acción y emite la Directiva Presidencial 02, a través de la cual establece la obligatoriedad a las entidades de carácter público a cumplir con la “Estrategia de Gobierno en Línea”. En el 2008, a través del decreto 1151, determina las directrices generales de la Estrategia de Gobierno en Línea de Colombia, y reglamenta algunos artículos de la Ley 962 de 2005, en la cual se indica al Ministerio de Comunicaciones, la responsabilidad de coordinar la implementación de la Estrategia de Gobierno En Línea; así mismo, la elaboración el "Manual de Políticas y Estándares

para la Gestión de información, Trámites y Servicios del Estado Colombiano a través de Medios Electrónicos".

En relación, en diciembre del año 2008, el Congreso de la república expide la Ley 1266, donde establece las disposiciones generales de habeas data, regula el manejo de la información, y define el concepto del término dato personal como “cualquier pieza de información vinculada a una o varias personas determinadas o determinables o que puedan asociarse con una persona natural o jurídica”.

Así mismo la Ley 1273 del 5 de enero de 2009, modifica el Código Penal, a partir del cual se crea un nuevo bien jurídico tutelado - denominado “De la protección de la información y de los datos” - y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones”. Esta Ley tipifica como delito las conductas concernientes al manejo de datos personales.

Por su parte, el Consejo Nacional de Política Económica y Social, adscrito al Departamento Nacional de Planeación, por medio de CONPES 3701 del 14 de julio de 2011, estable los Lineamientos de Política para Ciberseguridad y Ciberdefensa, con el objetivo de “Fortalecer las capacidades del Estado para enfrentar las amenazas que atentan contra su seguridad y defensa en el ámbito cibernético (ciberseguridad y Ciberdefensa), creando el ambiente y las condiciones necesarias para brindar protección en el ciberespacio (CONPES, 2011)”.

El Decreto 2693 de 2012, el cual “establece los lineamientos generales de la Estrategia de Gobierno en Línea”, así como el tiempo que tienen las diferentes entidades oficiales para su implementación y respectivo cumplimiento de las a las acciones establecidas en cada componente. De igual manera reglamenta algunos artículos de las leyes 1341 de 2009 y 1450 de 2011.

En concordancia, el 17 de octubre de 2012, se expide la Ley 1581, Por la cual se dictan las disposiciones generales de la Ley de protección de datos personales. Tiene por objeto: “desarrollar el derecho constitucional que tienen todas las personas a conocer, actualizar y rectificar las informaciones que se hayan recogido sobre ellas en bases de datos o archivos, y los demás derechos, libertades y garantías constitucionales a que se refiere el artículo 15 de la Constitución Política; así como el derecho a la información consagrado en el artículo 20 de la misma (ley 1481, 2012)”.

Garantiza la protección, almacenamiento y buen uso de los datos personales. En esta misma línea, se desarrolló un marco jurídico que incluye el reconocimiento de los datos e información como bien jurídico tutelado.

En este sentido, la Ley 1581 de 2012, reglamentada parcialmente por el Decreto 1377 del 27 de junio de 2013. Dicta disposiciones generales para la protección de datos personales y a su vez Adiciona en el artículo 3 a los contemplados en la ley en mención, los conceptos de aviso de privacidad, dato público, datos sensibles, Transferencia y transmisión.

El Decreto 2573 de 12 de diciembre de 2014. Determina las directrices generales de la Estrategia de Gobierno en línea, y reglamenta algunos artículos de la Ley 1341 de 2009 y determina otras disposiciones.

En complemento el 6 de marzo de 2014, se expide Ley de transparencia y acceso a la información pública, Ley 1712, con el fin de garantizar la transparencia mediante la publicación oportuna y proactiva de información pública (producida, generada, adquirida y controlada) no clasificada o reservada. Se basa en la transparencia, buena fe, calidad, gratuidad, celeridad, eficacia, facilitación, no discriminación.

El 26 de mayo 2015, a través del Decreto 1078, se expide el Decreto Único Reglamentario del Sector de las Tecnologías de la Información y las Comunicaciones. El cual establece el direccionamiento que tienen las entidades públicas para atender, planear, adquirir y usar TI, en el marco de cumplimiento de la Estrategia de Gobierno en Línea.

El Decreto 415 de 7 de marzo 2016. "Adiciona al Decreto Único Reglamentario del sector de la Función Pública, Decreto Numero 1083 de 2015, en lo relacionado con la definición de los lineamientos para el fortalecimiento institucional en materia de tecnologías de la información y las comunicaciones." El decreto en mención indica a las entidades de orden territorial a adoptar los lineamientos normalizados para las entidades estatales en referencia al fortalecimiento institucional y ejecución de los planes, programas y proyectos relacionados al área de tecnologías y sistemas de información en la entidad pertinente.

En referencia, el 11 de abril de 2016 el Consejo Nacional de Política Económica y Social, adscrito al Departamento Nacional de Planeación, expide el documento CONPES 3854 - Política Nacional de Seguridad Digital. En el cual se adopta la gestión de riesgo como núcleo central para la implementación de manera proactiva. El objetivo de esta Política es "Fortalecer las capacidades de las múltiples partes interesadas para identificar, gestionar, tratar y mitigar los riesgos de seguridad digital en sus actividades socioeconómicas en el entorno digital, en un marco de cooperación, colaboración y asistencia. Lo anterior, con el fin de contribuir al crecimiento de la economía digital nacional, lo que a su vez impulsará una mayor prosperidad económica y social en el país (CONPES, 2016)."

El Decreto 1413 de 2017. Por el cual se adiciona el título 17 a la parte 2 del libro 2 del Decreto Único Reglamentario del sector de Tecnologías de la Información y las Comunicaciones, Decreto 1078 de 2015, para reglamentarse parcialmente el capítulo IV del título III de la Ley 1437 de 2011 y el artículo 45 de la Ley 1753 de 2015 estableciendo lineamientos generales en el uso y operación de los servicios ciudadanos digitales.

Este año, en el Decreto 612 del 4 de abril de 2018. Se fijan directrices para la integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado.

La más reciente norma relacionada con el gobierno de Tecnología de la Información, es el Decreto 1008 del 14 de junio de 2018. El cual Modifica el Decreto 1078 de 2015 y establece los Lineamientos generales de la política de Gobierno Digital, por la cual se fijan directrices para la

integración de los planes institucionales y estratégicos al Plan de Acción por parte de las entidades del Estado Digital. Tiene como objeto: establecer "lineamientos generales de la Política de Gobierno Digital para Colombia, antes estrategia de Gobierno en Línea, la cual desde ahora debe ser entendida como: el uso y aprovechamiento de las tecnologías de la información y las comunicaciones para consolidar un Estado y ciudadanos competitivos, proactivos, e innovadores, que generen valor público en un entorno de confianza digital (Decreto 1008, 2018)".

Normatividad Derechos de Autor. El Artículo 61 de la Constitución Política de Colombia de 1991. Manifiesta que el estado salvaguarda la propiedad intelectual por el tiempo y en los formalismos establecidos en la ley. (Constitución Política de Colombia, 1991, art. 61).

La Ley 23 del 28 de enero de 1982. Determina las disposiciones generales y especiales que rigen la protección de los derechos de autor en Colombia. En el Artículo 1. Transcribe que: "Los autores de obras literarias, científicas y artísticas gozarán de protección para sus obras en la forma prescrita por la presente ley y, en cuanto fuere compatible con ella, por el derecho común. También protege esta ley a los intérpretes o ejecutantes, a los productores de fonogramas y a los organismos de radiodifusión, en sus derechos conexos a los del autor" (Ley 23, 1982).

Así mismo en el Artículo 2. Señala que: Los derechos de autor recaen sobre las obras científicas, literarias y artísticas las cuales se comprenden todas las creaciones del espíritu en el campo científico, literario y artístico, cualquiera que sea el modo o forma de expresión y

cualquiera que sea su destinación, tales como: los libros, folletos y otros escritos (…) (Ley 23, 1982).

La Ley 599 de 2000. Expide y reglamenta el Código Penal Colombiano. El Artículo 270, tipifica la penalización con cárcel y/o sanción pecuniaria aplicada a los ciudadanos que incurran en la violación a los derechos morales de autor. En los casos de que publique, total o parcialmente, sin autorización previa y expresa del titular del derecho, una obra inédita de carácter literario, artístico, científico, cinematográfico, audiovisual o fonograma, programa de ordenador o soporte lógico. Así como también cuando inscriba en el registro de autor con nombre de persona distinta del autor verdadero, o con título cambiado o suprimido, o con el texto alterado, deformado, modificado o mutilado, o mencionando falsamente el nombre del editor o productor de una obra de carácter literario, artístico, científico, audiovisual o fonograma, programa de ordenador o soporte lógico. O que por cualquier medio o procedimiento compendie, mutile o transforme, sin autorización previa o expresa de su titular, una obra de carácter literario, artístico, científico, audiovisual o fonograma, programa de ordenador o soporte lógico. (Ley 599, 2000).

Capitulo3. Diseño metodológico

A continuación, se describe el plan general de la investigación propuesta en donde se referencia, el tipo de investigación y el modelo metodológico principalmente.

3.1 Tipo de investigación

El desarrollo de la propuesta de caracterización de un modelo de gobernanza de TI para las entidades del estado, como apoyo al cumplimiento del componente de Seguridad y Privacidad de la Información en el marco de la estrategia de Gobierno Digital, se realizó bajo el enfoque de investigación cuantitativo con un paradigma positivista con alcance de estudio descriptivo, apoyada en actividades de campo que faciliten la recolección y análisis de la información obtenida referente a los diferentes modelos de gobernanza de TI, que podrían facilitar la caracterización del modelo requerido para la adopción efectiva del MSPI por parte de las entidades del sector gobierno. Teniendo en consideración el apoyo metodológico que surge del análisis documental como base de la estructura epistémica para generar un acercamiento al fenómeno de estudio.

Esta investigación permitirá que, a partir de diferentes modelos de gobierno de TI, se pueda realizar desde la deducción hacia la inducción, la caracterización más adecuada para el modelo de gobierno orientado al MSPI. La investigación cuantitativa parte de una idea que va acotándose y, una vez delimitada, define los objetivos y preguntas de investigación, realiza una revisión de la literatura, la cual permite construir el marco teórico del proyecto. Continua con el análisis de los objetivos y preguntas, para obtener posibles hipótesis; procediendo a la

elaboración del plan o diseño de investigación y selección de la muestra. Por último, se realiza el proceso de recolección de datos a través de uno o más instrumentos de medición, se analizan y publican los resultados encontrados (Hernández, Fernández, y Baptista, 2014, p.4). Por su parte, el paradigma del positivismo se inquieta con las definiciones operacionales, la objetividad, la replicabilidad, la causalidad y afines. (Bryman, 1984, p.77).

Hernández, Fernández, y Baptista (2014), manifiestan que, en vez de considerar tipos de investigación, se debe hablar es de alcance de estudio; debido a que de este depende la estrategia de investigación. El diseño, los procedimientos y otros componentes, serán de acuerdo a si el alcance es exploratorio, descriptivo, correlacional o explicativo (p.90). El alcance descriptivo de una investigación busca: "especificar propiedades y características importantes de cualquier fenómeno que se analice. Describe tendencias de un grupo o población" (Hernández, Fernández, y Baptista, 2014, p.92).

3.2 Seguimiento metodológico del proyecto

Tabla 3
Modelo Metodológico

OBJETIVOS DE LA INVESTIGACIÓN	ACTIVIDADES POR OBJETIVO	INDICADOR POR ACTIVIDAD
Obj 1. Identificar el marco normativo del estado colombiano para la implementación del MSPI.	Act 1. Interpretar el contenido del Decreto 1008 del 14 de junio 2018, en el cual el Gobierno Colombiano hace referencia al MSPI	Ind 1. Matriz del marco normativo para identificar los requerimientos de la política de Gobierno Digital en referencia al Modelo de Seguridad y Privacidad de la Información – MSPI propuesto por MinTIC.
Obj 2. Conocer el estado el arte del Modelo de Seguridad y Privacidad de la información propuesto	Act 1. Analizar la documentacion referente al Modelo de seguridad y privacidad propuesto y las	Ind 2. Número y relación de documentos entregables en cada fase del MSPI Ind 3. Número de

Tabla 3. Continuación

por el ministerio de las TIC en Colombia.	guias publicadas por el MINTIC.	procedimientos de seguridad que deben construirse.
Obj 3. Identificar que marcos de trabajo de gobierno de TI existentes podrían ayudar a alcanzar los objetivos de gobernanza y gestión del MSPI.	Act 1. Revisión de Liteeratura de los modelos de gobierno de TI existentes: ISO/IEC 38500:2015, VAL IT y COBIT 5.0.	Ind 4. Número de modelos de Gobierno aplicables al MSPI. Ind 5. Porcentaje de características aplicables a la gobernanza del MSPI.
Obj 4. Diseñar un modelo de gobernanza que facilite la evaluación, dirección y el control del programa de seguridad y privacidad de los activos de información de las entidades del estado colombiano.	Act 1. Determinar los atributos y características requeridas para el buen gobierno de TI alineado con el MSPI. Act 2. Determinar los componentes de dirección y control requeridos por el nuevo modelo de gobierno de TI. Act 3. Construir la propuesta de caracterización del nuevo modelo de Gobierno de TI.	Ind 6. Cantidad de características requeridas por el nuevo modelo de gobierno. Ind 7. Número de componentes de dirección y control requeridos. Ind 8. Propuesta inicial de caracterización del nuevo modelo de gobernanza
Obj 5. Validar la coherencia y la efectividad del modelo de gobernanza propuesto, fundamentada en la opinión de una muestra de "Expertos" en Gobierno, Seguridad, Control Interno y Auditoria TI, de entidades públicas.	Act 1. Elaboración de un instrumento para evaluar el nivel de coherencia y efectividad del modelo de gobernanza propuesto. Act 2. Aplicar el instrumento de diagnostico de la actividad acterior (actividad 1) a cada uno de expertos en gobierno de TI, seguridad de la informacion, Auditoria y control interno.	Ind 9. Instrumento que permite evaluar la coherencia y la efectividad del modelo de gobernanza propuesto. Ind 10. Nivel de coherencia y la efectividad del modelo de gobernanza propuesto

Fuente: Elaboración propia.

3.3 Población

En palabras de Tamayo (2012), la población es la totalidad de un fenómeno de estudio, que incluye todas las unidades de análisis que integran determinado fenómeno y que debe ser cuantificado para una investigación, integrando un conjunto N de entidades que tienen una(s)

característica en común. Se nombra población porque constituye la totalidad del fenómeno adscrito como objeto de estudio en una investigación. Por su parte Hueso y Cascant (2012), conceptualiza el termino de población como el conjunto de todos los sujetos sobre los que se desea conocer cierta información, en relación al fenómeno que se investiga (p.10).

La población que involucra este proyecto son las entidades de orden nacional y territorial de Colombia. La ley 489 de 1998, articulo 39, señala: "La Administración Pública se integra por los organismos que conforman la Rama Ejecutiva del Poder Público y por todos los demás organismos y entidades de naturaleza pública que de manera permanente tienen a su cargo el ejercicio de las actividades y funciones administrativas o la prestación de servicios públicos del Estado Colombiano".

3.4 Muestra

Como lo referencia Hernández, Fernández, y Baptista (2014), la muestra es un subconjunto de elementos que pertenecen a un conjunto definido por sus características al que denominamos población (p.175). En concordancia Hueso y Cascant (2012), define la muestra como: "el subconjunto de la población que se selecciona para el estudio, esperando que lo que se averigüe en la muestra nos dé una idea sobre la población en su conjunto" (p.10).

Considerando que el alcance del proyecto está limitado a las entidades de orden territorial del departamento de Norte de Santander y teniendo en cuenta que las alcaldías de todos los 40

municipios del departamento deben cumplir con los lineamientos de Gobierno Digital definidos por MinTIC.

El proyecto de investigación emplea como muestra el juicio de expertos de nueve, con perfil profesional en el área relacionada a Gobierno TI, Seguridad, Control Interno, Auditoria TI o experiencia en implementación del Modelo de Seguridad y Privacidad e la información – MSPI, a fin de otorgar rigurosidad científica al estudio que se viene planteando

3.5 Técnicas de recolección de la información

Rodríguez, (2008) señala al referirse a las técnicas e instrumentos de investigación, como los medios empleados por el investigador para recolectar la información, entre los que se destacan las encuestas, el cuestionario, la entrevista, la observación y el análisis documental (p.10). En opinión de Hernández, Fernández, y Baptista (2014), conceptualiza como las herramientas que permiten recolectar los datos importantes sobre los atributos, conceptos o variables de las unidades que son objeto de muestreo, análisis o casos (p.198).

Para la realización de la caracterización de un modelo de gobernanza de TI para las entidades del estado, como apoyo al cumplimiento del componente de Seguridad y Privacidad de la Información en el marco de la estrategia de Gobierno Digital", se utilizarán la técnica de análisis de documentos e instrumentos de campo como: entrevistas, encuestas observación directa principalmente. En primer lugar, se realiza un análisis e interpretación de los Decretos 1008 del 14 de junio de 2018 y 1078, expedido el 26 de mayo del 2015 del Gobierno

Colombiano, el cual hace referencia al MSPI, que permitirá al investigador identificar las entidades obligadas a realizar la implementación del MSPI, así como los plazos establecidos para su cumplimiento.

Seguidamente se procede a realizar un análisis de la documentación referente al Modelo de seguridad y privacidad propuesto por MinTIC, así como las guías publicadas, para conocer los entregables en cada una de las fases del MSPI y el número de procedimientos de seguridad a construir.

Se realizará revisión de Literatura de los modelos de gobierno de TI existentes: ISO/IEC 38500:2015, VAL IT y COBIT 5.0, con el fin de conocer la estructura de cada uno de estos modelos e identificar los principales principios que se puedan adaptar al MSPI.

3.6 Análisis de la información

El análisis de los resultados es el proceso de organizar los datos obtenidos como resultado de la aplicación del instrumento de recolección de información en tablas, cuadros o matrices, de acuerdo con el orden establecido en los objetivos específicos, las variables, dimensiones e indicadores (Pelekais, Kadi, Seijo y Neuman, 2015, p.172).

Para Construir la propuesta de caracterización del nuevo modelo de Gobierno de TI, después del análisis de la información se compararán las estructuras de cada modelo y se identificarán las similitudes y diferencias entre ellas. Se determinarán los requisitos en común de

las normas en mención, que permitan establecer la base de un modelo que se adapte a las condiciones del Modelo de Seguridad y Privacidad de la Información MPSI.

Capítulo 4. Presentación de resultados

El desarrollo de la propuesta modelo de gobernanza de TI para las entidades del estado, como apoyo al cumplimiento del componente de Seguridad y Privacidad de la Información en el marco de la política de Gobierno Digital, es un proceso en el cual se contemplan una serie de actividades. La primera, comienza con la identificación del marco normativo del estado colombiano para la implementación del MSPI. El gobierno nacional ha establecido los lineamientos para la Estrategia Gobierno en los decretos 1151 de 2008, 2573 de 2014, 1078 de 2015 y la Política de Gobierno Digital en el 1008 de 2018.

Después del marco regulatorio, se procede a conocer el estado del arte del Modelo de Seguridad y Privacidad de la Información – MSPI, la documentación de las metas, resultados e instrumentos de la fases del ciclo de operación, así como las guías publicadas por el MinTIC, para pasar a la identificación de los marcos y/o estándares de TI existentes y poder articular este modelo a un marco de gobierno de TI, para posteriormente llegar al diseño, y finalizar con una validación de la coherencia y efectividad del modelo.

4.1 Marco normativo del estado colombiano para la implementación del MSPI.

La política de gobierno Digital en Colombia, ha venido evolucionando constantemente. Sus inicios se dieron con el decreto 1151 de 2008, mediante el cual el gobierno nacional define los lineamientos generales de la Estrategia de Gobierno en línea - GEL, luego con el Decreto 2573 de 2014, disposiciones compiladas por el Decreto 1078 de 2015, denominado “Decreto

Único Reglamentario del sector TIC", establece los plazos e instrumentos de la Estrategia GEL, para garantizar el aprovechamiento de las TIC, y contribuir así a la construcción de un Estado más abierto, eficiente, transparente, más participativo y con mejores servicios con la colaboración de toda la sociedad.

En este enfoque en el 2018, mediante el Decreto 1008, se presenta la transición de Gobierno en Línea a Gobierno Digital. Política que tiene como objetivo "Promover el uso y aprovechamiento de las tecnologías de la información y las comunicaciones para consolidar un Estado y ciudadanos competitivos, proactivos, e innovadores, que generen valor público en un entorno de confianza digital" (MinTIC, 2018).

4.2 Interpretación de la estrategia Gobierno en Línea y la Política Gobierno Digital

Tabla 4
Estrategia Gobierno en Línea

Decreto / **Elemento**	**Decreto 1078 de 2015** **Estrategia Gobierno en Linea - GEL**	**Decreto 1008 de 2018** **Politica Gobierno Digital**	**Interpretación**
Objeto	Definir los Lineamientos instrumentos y plazos de la Estrategia Gobiernos en Línea - GEL, para garantizar el máximo aprovechamiento de las Tecnologías de la Información y las Comunicaciones, con el fin de contribuir con la construcción de un Estado abierto, más eficiente, más transparente y más participativo y que	Promover el uso y aprovechamiento de las TIC para consolidar un Estado y ciudadanos competitivos, proactivos, e innovadores, que generan valor público en un entorno de confianza digital.	La política de Gobierno digital apunta al aprovechamiento de la tecnología por parte del estado, ciudadanos y grupos de interes, para que éstos adquieran las competencias y capacidades específicas para el cumplimiento de las necesidades, asi como la

Tabla 4. Continuación

	preste mejores servicios con la colaboración de toda la Sociedad. (Decreto 2573 de 2014, Art.1)		solución de problemáticas públicas (MinTIC, 2018).
Ambito de Aplicación	Entidades que conforman la administración Pública de acuerdo con la Ley 489 de 1998, articulo 39, asi como los particulares que cumplen con funciones administrativas.		Se mantiene el ambito de aplicación.
Principios	La Estrategia GEL, de desarrolla de acuerdo a los principios del debido proceso, igualdad, imparcialidad, buena fe, moralidad, participación, responsabilidad, transparencia, publicidad, coordiandción, eficacia, economia, celeridad contemplados en el articulo 209 de la Constitución Politica, asi como tambien en el Articulo 3 de la Ley 489 de 1998 y el Articulo 3 de la Ley 1437 de 2011. Adicinal, seran fundamentos: - Excelentecia en servicio ciudadano. - Apertura y reutilización de datos públicos. - Estandarización. - Interoperabilidad. - Neutralidad Tecnológica. - Innovación. - Colaboración. (Decreto 2573 de 2014, art 4)	Principios que rigen la función, procedimeintos administrativos, asi como los que orientan el sector TIC, en particular: - Innovación - Competitividad - Proactividad - Seguridad de la información	Prevalecen los principos regulados el Articulo 3 de la Ley 489 de 1998 y el Articulo 3 de la Ley 1437 de 2011. Asi como el del sector de las TIC, Innovación, se adiciona Competitividad, proactividad y Seguridad de la información
Estructura	Establece cuatro (4) componentes: 1.TIC para Servicios: - Trámites y servicios en línea. - Servicios enfocados a dar soluciones al	Se desarrolla a través de dos componentes, tres habilitadores transversales y su articulación contribuye al logro de los cinco (5) propósitos de	La estrucutra de la Estrategia GEL a la de Politica Digita, cambia de cuatro (4) a dos (2) componentes

Tabla 4. Continuación

	usuario. Con calidad, facilidad de uso y mejoramiento continúo. 2.TIC para Gobierno Abierto: Actividades en focadas a la construcción de un estado: - Transparente. - Participativo. - Colaborativo. 3.TIC para Gestión: Comprende: - Planeación y Gestión Tecnologica. - Mejora de procesos internos e intercambio de información. - Gestión y aprovechamiento de la información. - Toma de decisiones. - Mejoramiento continuo. - Capacidades Institucionales. **4.**Seguridad y Privacidad de la Información. Acciones transversales a los componestes de la estructura GEL, tendientes a la protección de la información y sistemas de información.	política de Gobierno Digital. Componentes: - TIC para el Estado - TIC para la Sociedad Habilitadores transversales : - Arquitectura - Seguridad de la Información - Servicios Ciudadanos Digitales. Propósitos de política de Gobierno Digital. 1.Habilitar y mejorar la provisión de Servicios Digitales de confianza y calidad. 2.Lograr procesos internos, seguros y eficientes a través del fortalecimiento de las capacidades de gestión de tecnologías de información. 3.Tomar decisiones basadas en datos a partir del aumento el uso y aprovechamiento de la información. 4.Empoderar a los ciudadanos a través de la consolidación de un Estado Abierto. 5.Impulsar el desarrollo de territorios y ciudades inteligentes para la solución de retos y problemáticas sociales a través del aprovechamiento de las TIC.	(TIC para el estado y TIC para la Sociedad). Adiciona una serie de elementos habilitadores que permiten que las entidades, independientemente de sus recursos y capacidad, puedan realizar la implementación de acuerdo a las necesidades y caracterisitcas de las mismas.
Responsables de implementación	Entidades de orden Nacional: - Comité Institucional	- Líder de la política de Gobierno Digital. Ministerio TIC a través de la Dirección de	- Se establece la insitucionalidad al desarrollo en el estado.

Tabla 4. Continuación

	de Desarrollo Aministrativo. Entidades de orden territorial y demas sujetos obligados: - Consejo de gobierno o quien haga sus veces. En caso de no existir la dependencia de mayor nivel jerarquico en la entidad. En tramites electronicos: - La instancia orientadora en articulación con el Comité Antitrámites ó su responsable.	Gobierno Digital, o quien haga sus veces. - Responsable institucional de la política de Gobierno Digital. Representante Legal de cada sujeto obligado. - Responsable de orientar la implementación de la Política de Gobierno Digital. Comités institucionales de Gestión y Desempeño. - Responsable de liderar la implementación de la Política de Gobierno Digital. Director, jefe de oficina o Coordinador de Tecnologías y Sistemas de la Información y las Comunicaciones o quien haga sus veces. Las demás áreas serán corresponsables de la implementación de la Política de Gobierno Digital en los temas de su competencia.	- La asignación de roles y responsabilidades se hace a los actores involucrados en la implementación de la Politica de Gobierno Digital. - Se desarrolla un esquema institucional alineado al Decreto 1499 de 2017, en el cual se ajustan las instancias de dirección y coordinación del Sistema de Planeación y Gestión y se crean los comités institucionales, departamentales, distritales y municipales de gestión y desempeño (MinTIC, 2018).
Seguimiento y Evaluación	Porcentaje por componente y plazo de cumplimento.	MinTIC, a trtaves de la Dirección de Gobierno Digital realizara seguimiento y evaluación a traves de: - Indicadores de cumplimiento e indicadores de resultados. - Sello de excelencia de Gobierno Digital. El seguimiento y evaluación del avance de la política se realizará con un enfoque de mejoramiento continuo, verificando que cada sujeto obligado, presente resultados anuales	Las entidades reportan el logro de los propositos de la politica a partir de los fierentes proyectos e inicitiavivas que hacen uso de las TIC (MinTIC, 2018).

Tabla 4. Continuación

		mejores que en la vigencia anterior y de acuerdo con a segmentación de entidades.	
Plazo de Implementación	Los Plazo de los sujetos del Orden Nacional y territorial obligados a implementar las actividades establecidas en el Manual de Gobierne en línea están definidos en el Artículo 2.2.9.1.3.2.	No tiene establecido plazos de implementación.	El avance en implementación se mide a partir de las metas reportadas en cada vigencia (MinTIC, 2018).

Fuente. Manual de Gobierno en Linea 2018.

4.3 Alcance**.**

Las Entidades obligadas a realizar la implementación del MSPI, de acuerdo con el Decreto 1008 de 14 de junio de 2018, son las descritas en la Ley 489 de 1998, articulo 38.

La Ley 489 de 1998 en el artículo 38, especifica las entidades que conforman el sector de la administración pública en el orden nacional, territorial y descentralizado, que deben implementar y colocar en funcionamiento los respectivos componentes de la Política de Gobierno Digital, atendiendo los requisitos legales exigidos.

A continuación, en la Tabla 5, se relaciona las entidades que conforman cada uno de los sectores mencionados de acuerdo con su naturaleza jurídica:

Tabla 5
Entidades que conforman los sectores

LEY 489 DE 1998, ARTICULO 38	
Entidades de orden nacional	• Presidencia de la República, • Ministerios • Departamentos Administrativos • Superintendencias sin personería jurídica • Unidades Administrativas Especiales sin personería jurídica
Entidades de orden territorial	• Gobernaciones: El estado colombiano se encuentra dividido en 32 gobernaciones las cuales se encuentran clasificadas por categorías (especial, primera, segunda, tercera y cuarta). • Alcaldías: clasificadas por categorías (especial, primera, segunda, tercera, cuarta, quinta y sexta). • Secretarías de despacho • Departamentos administrativos
Entidades descentralizadas	• Establecimientos públicos, • Empresas industriales y comerciales del Estado. • Superintendencias. • Unidades administrativas especiales con personería jurídica. • Empresas sociales del Estado. • Empresas oficiales de servicios públicos domiciliarios. • Institutos científicos y tecnológicos. • Sociedades públicas. • Sociedades de economía mixta. • Entidades administrativas nacionales con personería jurídica que cree, organice o autorice la ley para que formen parte de la Rama Ejecutiva del Poder Público.

Fuente Propia.

Adicional el Parágrafo 1º, del artículo 38 de la Ley 489 de 1998, referencia que: "Las sociedades públicas y las sociedades de economía mixta en las que el Estado posea el noventa por ciento (90%) o más de su capital social, se someten al régimen previsto para las empresas industriales y comerciales del Estado".

4.4 Estado del arte del Modelo de Seguridad y Privacidad de la Información propuesto por el Ministerio de las TIC en Colombia.

4.4.1 Descripción del ciclo de Operación del Modelo de Seguridad y Privacidad de la Información – MSPI. En el presente literal se explica de manera detallada el ciclo de funcionamiento del ciclo de operación del MSPI. Contiene la descripción de cada una de las fases, con las metas, resultados e instrumentos del MSPI a utilizar y alineación a la guía marco de referencia de arquitectura empresarial – MRAE.

.
.

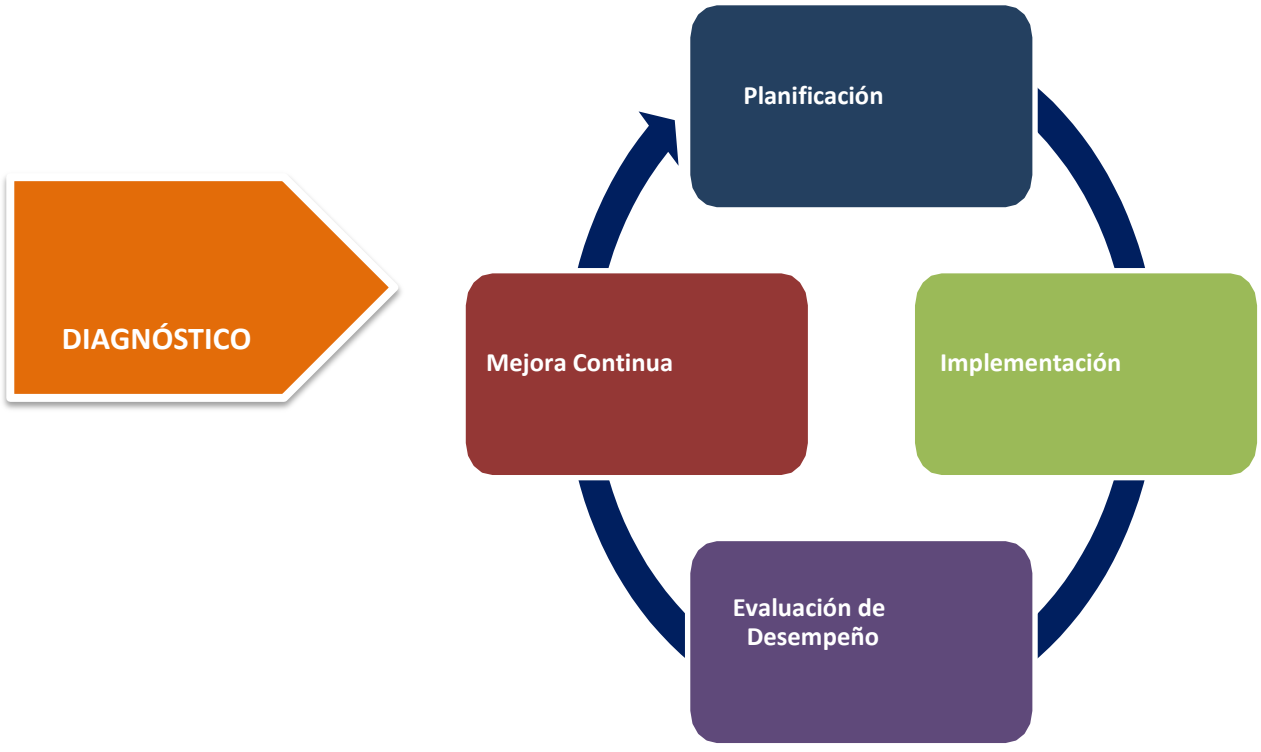

Figura 18. Ciclo de operación del Modelo de Seguridad y Privacidad de la Información - MSPI
Fuente: MinTIC (2016)

4.4.2 Metas, Resultados e Instrumentos de la Fases del Ciclo de operación del Modelo de Seguridad y Privacidad de la Información - MSPI.

Tabla 6

Metas, Resultados e Instrumentos de la Fases del Ciclo de operación del Modelo de Seguridad y Privacidad de la Información - MSPI.

Fase de Diagnóstico - etapas previas a la implementación			
Metas	**Resultados**	**Instrumentos MSPI**	**Alineación MRAE**
Determinar el estado actual de la gestión de seguridad y privacidad de la información al interior de la Entidad.	Diligenciamiento de la herramienta.	Herramienta de diagnóstico.	LI.ES.01 LI.ES.02 LI.GO.01 LI.GO.04 LI.GO.05
Identificar el nivel de madurez de seguridad y privacidad de la información en la Entidad	Diligenciamiento de la herramienta e identificación del nivel de madurez de la entidad.	Herramienta de diagnóstico	LI.GO.07 LI.ST.14
Identificar vulnerabilidades técnicas y administrativas que sirvan como insumo para la fase de planificación.	Documento con los hallazgos encontrados en las pruebas de vulnerabilidad.	Herramienta de diagnóstico	
Fase de Planificación			
Política de Seguridad y Privacidad de la Información	Documento con la política de seguridad de la información, debidamente aprobado por la alta Dirección y socializada al interior de la Entidad.	Guía No 2 – Política General MSPI	LI.ES.02 LI.ES.06 LI.ES.07 LI.ES.08 LI.ES.09
Políticas de seguridad y privacidad de la información	Manual con las políticas de seguridad y privacidad de la información, debidamente aprobadas por la alta dirección y socializadas al interior de la Entidad.	Guía no 2 - Política General MSPI	LI.ES.10 LI.GO.01 LI.GO.04 LI.GO.07 LI.GO.08 LI.GO.09
Procedimientos de seguridad de la información.	Procedimientos, debidamente documentados, socializados y aprobados por el comité que integre los sistemas de gestión institucional.	Guía No 3 - Procedimientos de Seguridad y Privacidad de la Información.	LI.GO.10 LI.INF.01 LI.INF.02 LI.INF.09 LI.INF.10
Roles y responsabilidades de seguridad y privacidad de la información.	Acto administrativo a través del cual se crea o se modifica las funciones del comité gestión institucional (o el que haga sus veces), en donde se incluyan los temas de seguridad de la información en la entidad, revisado y aprobado por la alta Dirección, deberá designarse quien será el encargado de seguridad de la información dentro de la entidad.	Guía No 4 - Roles y responsabilidades de seguridad y privacidad de la información.	LI.INF.11 LI.INF.14 LI.SIS.22 LI.SIS.23 LI.SIS.01 LI.ST.05 LI.ST.06 LI.ST.09 LI.ST.10 LI.ST.12 LI.ST.13 LI.ST.14

Tabla 6. Continuación

Inventario de activos de información.	Documento con la metodología para identificación, clasificación y valoración de activos de información, validado por el comité de seguridad de la información o quien haga sus veces y revisado y aprobado por la alta dirección. Matriz con la identificación, valoración y clasificación de activos de información. Documento con la caracterización de activos de información, que contengan datos personales Inventario de activos de IPv6	Guía No 5 - Gestión De Activos Guía No 20 - Transición Ipv4 a Ipv6	LI.UA.01 LI.UA.02 LI.UA.03 LI.UA.04 LI.UA.05 LI.UA.06
Integración del MSPI con el Sistema de Gestión documental	Integración del MSPI, con el sistema de gestión documental de la entidad.	Guía No 6 - Gestión Documental	
Identificación, Valoración y tratamiento de riesgo.	Documento con la metodología de gestión de riesgos. Documento con el análisis y evaluación de riesgos. Documento con el plan de tratamiento de riesgos. Documento con la declaración de aplicabilidad. Documentos revisados y aprobados por la alta Dirección.	Guía No 7 - Gestión de Riesgos Guía No 8 - Controles de Seguridad	
Plan de Comunicaciones.	Documento con el plan de comunicación, sensibilización y capacitación para la entidad.	Guía No 14 - Plan de comunicación, sensibilización y capacitación	
Plan de diagnóstico de IPv4 a IPv6.	Documento con el Plan de diagnóstico para la transición de IPv4 a IPv6.	Guía No 20 - Transición IPv4 a IPv6	
Fase de Implementación			
Planificación y Control Operacional.	Documento con la estrategia de planificación y control operacional, revisado y aprobado por la alta Dirección.	Documento con el plan de tratamiento de riesgos. Documento con la declaración de aplicabilidad.	LI.ES.09 LI.ES.10 LI.GO.04 LI.GO.09 LI.GO.10 LI.GO.14
Implementación del plan de tratamiento de riesgos.	Informe de la ejecución del plan de tratamiento de riesgos aprobado por el dueño de cada proceso.	Documento con la declaración de aplicabilidad. Documento con el plan de tratamiento de riesgos.	LI.GO.15 LI.INF.09 LI.INF.10 LI.INF.11 LI.INF.14 LI.INF.15
Indicadores De Gestión.	Documento con la descripción de los indicadores de gestión de seguridad y privacidad de la información.	Guía No 9 - Indicadores de Gestión SI.	LI.SIS.22 LI.SIS.23 LI.ST.05 LI.ST.06
Plan de Transición de IPv4 a IPv6	Documento con las estrategias del plan de implementación de IPv6 en la entidad, aprobado por la	Documento con el Plan de diagnóstico para la transición de	LI.ST.09 LI.ST.10 LI.ST.12

Tabla 6. Continuación

	Oficina de TI.	IPv4 a IPv6. Guía No 20 - Transición de IPv4 a IPv6 para Colombia. Guía No 19 – Aseguramiento del Protocolo IPv6.	LI.ST.13 LI.UA.01
Fase de Evaluación del Desempeño			
Plan de revisión y seguimiento, a la implementación del MSPI. Plan de Ejecución de Auditorias	Documento con el plan de seguimiento y revisión del MSPI revisado y aprobado por la alta Dirección. Documento con el plan de ejecución de auditorías y revisiones independientes al MSPI, revisado y aprobado por la Alta Dirección.	Guía No 16 – Evaluación del desempeño. Guía No 15 – Guía de Auditoría.	LI.ES.12 LI.ES.13 LI.GO.03 LI.GO.11 LI.GO.12 LI.INF.09 LI.INF.11 LI.INF.13 LI.INF.14 LI.INF.15 LI.SIS.23 LI.ST.05 LI.ST.06 LI.ST.08 LI.ST.15 LI.UA.07 LI.UA.08
Fase de Mejora Continua			
Plan de mejora continua	Documento con el plan de mejoramiento. Documento con el plan de comunicación de resultados.	Resultados de la ejecución del Plan de Revisión y Seguimiento, a la Implementación del MSPI. Resultados del plan de ejecución de auditorías y revisiones independientes al MSPI. Guía No 17 – Mejora Continua	LI.GO.03 LI.GO.12 LI.GO.13 LI.INF.14 LI.INF.15 LI.ST.15 LI.UA.9 LI.UA.10

Fuente. (MinTIC, 2016)

4.5 Marcos de trabajo de gobierno de TI existente que confluyen en los objetivos de gobernanza y gestión.

En esta fase se realiza la revisión de Literatura de los marcos de gobierno de TI, para identificar cuales aplican específicamente para el diseño y desarrollo de un modelo de gobernanza de TI para las entidades del estado, que apoye al cumplimiento del componente de

seguridad y privacidad de la información en el marco de la Política de Gobierno Digital, de acuerdo con las características del negocio que para la investigación son las entidades públicas de Colombia, en particular Alcaldías Municipales.

En la actualidad la industria de TI y un número significativo de organizaciones a nivel mundial trabajan en pro de definir las mejores prácticas en cada uno de los procesos, teniendo en cuenta la complejidad que cada día aumenta por los cambios del entorno del negocio. Gómez (2015), Manifiesta que aunque existen múltiples herramientas que soportan el proceso de gestión de TI, para el área de implementación de Gobierno TI, existe un número muy limitado.

4.5.1 Herramientas para la implementación de Gobierno de TI. A continuación, se relacionan los estándares que se alinean a las áreas de TI.

Tabla 7

Herramientas para la implementación del Gobierno de las T.I.

	ESTÁNDAR INTERNACIONAL	ESTÁNDAR NACIONAL	MARCO DE REFENCIA
Gobierno de las T.I.	ISO 38500	AS 8015 COSO [b]	COBIT
Planificación T.I.		PSI-Métrica 3	
Valor de las T.I.			Val IT
Gestión Servicios T.I.	ISO/IEC 20000	BS 15000	COBIT ITIL MOF
Gestión de Proyectos.		UNE 15781	PMBOK PRINCE2 APMs IPMA
Desarrollo Software.	ISO 12207	Ticket Métrica 3	CMMI
	ISO 15504		Bootstrap
Gestión de Riesgos.		AS/NZS 4360 COSO Magerit UNE 71504	
Gestión de Seguridad.	ISO 27000	NIST-800 series BS	ASCI-33 COBIT
	ISO 13335	7799-2 GAO´s	ISF ENV12924
	ISO 13569	FISCAM	SEI´s OCTAVE
	ISO 17799	German BSI	SEI´s SW-CMM
	ISO 15408		BPM
Gestión de Continuidad.	ISO /IEC 25999	PAS-56 AS/NZS 4360 HB 221-2004 BS25999	
Gestión de la Calidad.	ISO 9001	EFQM BNQP SixSigma	
Auditoria.	ISO 19011		COBIT

Fuente. (Fernández, 2009) (Gómez, 2015).

Por su parte ITIG, realizo un estudio en el cual detalla cuales de sus productos apoyan la implementación de Gobierno TI y permiten la adopción de la norma UNE- ISO/IEC 38500. Describiendo por cada producto que principio de la norma y que acción del modelo soporta (IT Governance Institute, 2009). (Ver tabla 8).

Tabla 8

Relación de productos ITGI e ISO/IEC 38500

Áreas de ISO/IEC 38500									
Producto ITGI	**Principios ISO/IEC 38500**						**Tareas**		
	Responsabilidades	**Estrategias**	**Adquisición**	**Desempeño**	**Conformidad**	**Comportamiento humano**	**Evaluar**	**Dirigir**	**Monitorizar**
Board Briefing on IT Governance, 2nd Edition	√	√				√	√	√	√
Unlocking Value: An Executive Primer on the Critical Role of IT Governance	√	√				√	√	√	√
COBIT®	√	√	√	√	√	√	√	√	√
Val IT™	√	√	√	√	√	√	√	√	√
IT Governance Implementation Guide: Using COBIT® and Val IT, 2nd Edition							√	√	√
IT Assurance Guide: Using COBIT®				√	√		√		√
COBIT® Quickstart™, 2nd Edition							√	√	
Enterprise Value: Governance of IT Investments, Getting Started With Value Management							√		
COBIT® Security Baseline™, 2nd Edition	√						√	√	
Enterprise Value: Governance of IT Investments, The Business Case			√	√			√	√	√

Fuente. (IT Governance Institute, 2009)

En concordancia con el enfoque teórico definido en Gobierno y Gestión de TI, así como la operación del negocio (entidades Públicas de Colombia), se precisa que el marco de referencia para el desarrollo de la propuesta es ISO/IEC 38500 y COBIT. La norma ISO/IEC 38500 define

las tareas a realizar, mas no define el cómo, ni el responsable de ejecutarla, debilidades que se fortalecen con COBIT, en el cual se establece los lineamientos de cómo hacer cada una de estas. A su vez cabe mencionar que COBIT cuenta con varias versiones, para el proyecto se ha elegido la versión 5, debido a que integra a VAL IT y proporciona un mayor número de posibilidades en el momento de definir los criterios para realizar la evaluación del nivel de madurez de la organización, en comparación con otras versiones (Gómez, 2015).

4.5.2 Norma UNE - ISO/IEC 38500. ISO/IEC 38500 es una norma española asesora de alto nivel, basado en principios. Que facilita la orientación general al cuerpo de gobierno sobre el uso eficaz, eficiente y aceptable en la Tecnología de la Información en las organizaciones **(UNE-ISO/IEC 38500, 2013)**.

El objetivo de esta norma es: "Promover el uso eficaz, eficiente y aceptable de la TI en todas las organizaciones por medio de:

- Asegurar a las partes interesadas (incluidos clientes, accionistas y empleados) que si siguen la norma, pueden confiar en la gobernanza corporativa de la TI dentro de la organización;
- Informar y orientar a los administradores sobre el gobierno del uso de la TI en su organización; y
- Proporcionar una base de referencia para la evaluación objetiva de la gobernanza corporativa de la TI" (UNE-ISO/IEC 38500, 2013).

Principios de la norma. ISO 38500, define 6 principios para un buen gobierno corporativo de TI.

- Principio 1 - Responsabilidad: establecer, comprender y aceptar las responsabilidades definidas en TI.
- Principio 2 - Estrategia: planificar la TI para que las estrategias de negocio porten las capacidades actuales y futuras de las tecnologías de la información y las comunicaciones (TIC).
- Principio 3- Adquisición: adquirir TI de manera en base a un análisis apropiado y continuo, manteniendo equilibrio entre los beneficios, las oportunidades, los costes y los riesgos.
- Principio 4 - Rendimiento: asegurarse de que TI satisface las necesidades actuales y futuras brindando soporte al negocio con servicios de calidad.
- Principio 5- Conformidad: asegurarse de que la función de TI está en concordancia con la legislación y normativa vigente.
- Principio 6 – Factor humano: asegurar que la política de TI respeta el factor humano.

Adicional a conformidad de los principios, los directores deben gobernar las Tecnologías de la Información (TI) a través de tres tareas principales (Evaluar, Dirigir y Supervisar).

- Evaluar el uso de las TI.
- Prepara e implementar planes y políticas.
- Monitorear el cumplimiento de las políticas y el desempeño en relación con los planes.

Beneficios de la Utilización de la norma UNE - ISO/IEC 38500

- Provee un marco de 6 principios básicos para el uso eficaz, eficiente y aceptable de las TI. Su seguimiento y correcta aplicación permite a los directores u/o Administradores mitigar los riesgos y propiciar oportunidades derivadas del uso de las TI (UNE-ISO/IEC 38500, 2013).

- Establece un modelo de gobierno de tecnología de la información.
- Proporciona un vocabulario específico para el Gobierno de Tecnología de la Información (TI).
- Su ámbito de aplicación está dado para todas las organizaciones, independiente de su tamaño, rama de actividad, diseño u/o estructura.
- Asegurar el cumplimiento de la legislación vigente referenciado para el uso de aceptable de las TI.
- El uso de los lineamientos establecidos en UNE - ISO/IEC 38500, aumenta la probabilidad de cumplimiento de las obligaciones de los directivos.
- La adecuada gobernanza TI, permite a los directivos asegurar que el uso de TI contribuye positivamente al desempeño de la organización, cumplimiento al logro de los objetivos, la continuidad, así como sostenibilidad del negocio (UNE-ISO/IEC 38500, 2013).

4.5.3 COBIT. COBIT (Control Objectives for Information and related Technology) es un estándar internacional, abierto para el control de las TI, desarrollado, y promovido por el IT Governance Institute (ITGI, 2007**).**

COBIT, se define como un conjunto de mejores prácticas para el manejo de información. Creado por la asociación para la Auditoria y Control de Sistemas de Información fue publicado (ISACA por sus siglas en Inglés), y el Instituto de Administración de las Tecnologías de la información (ITGI, en inglés: IT Governance Insitute) en el año 1992.

COBIT público su primera versión en el año 1996 y actualizada a su segunda edición en el año 1998 donde se adiciona los lineamientos de gestión. Posteriormente en el 2000 se lanzó la

tercera edición, con publicación en línea en el año 2003. En diciembre de 2005 aparece la versión 4, la cual en mayo de 2007 realiza una revisión pasando a COBIT 4.1. En el 20012, lista el lanzamiento de COBIT 5, con el objeto de consolidar e integrar COBIT 4.1, Val IT 2.0, los marcos de TI de riesgo, y se extrajeron del Marco de garantía de TI de ISACA (ITAF) y el modelo de negocio para la seguridad de la información (BMIS), así como la alineación con marcos y estándares como ITIL, ISO, PMBOK, PRINCE2 y TOGAF.

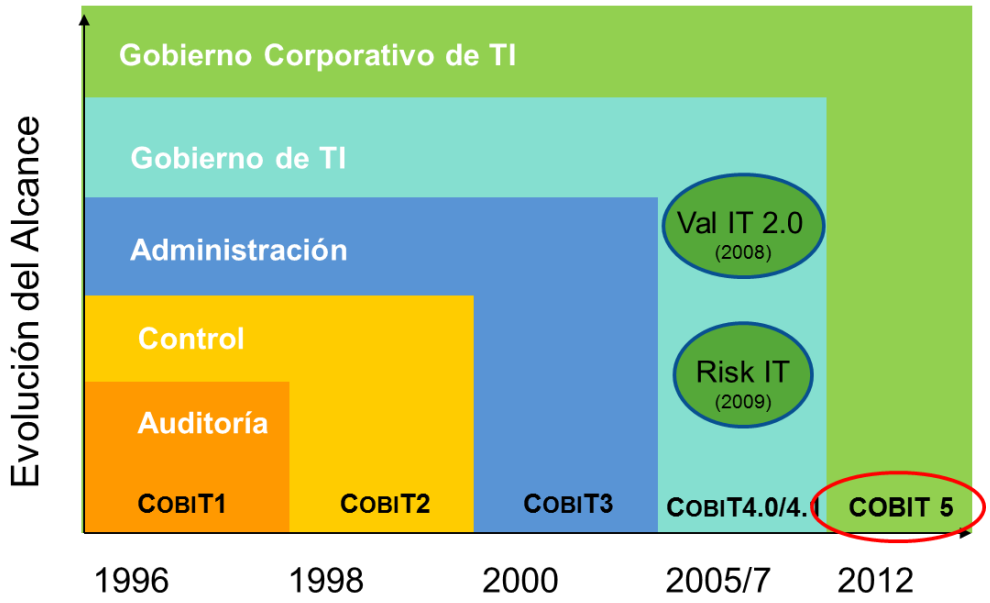

*Figura 19.*Un Marco Empresarial de ISACA,
Fuente. www.isaca.org/cobit

Beneficios de la Utilización de COBIT

- Marco de referencia conocido y aceptado a nivel mundial, que provee buenas prácticas para el Gobierno TI, la auditoria y el control.
- Esta alineada con ISO 38500.
- Es el marco de trabajo con mayor aceptación para la implementación de Gobierno de TI, su alcance cubre casi todas las disciplinas de TI.

- La función de TI en las organizaciones se enfoca más al negocio.
- Mayor creación de valor del negocio a través de un gobierno y una gestión efectiva de la información.
- Incremento en creación de valor del negocio a través de un gobierno y una gestión efectiva de los activos tecnológicos.
- Aseveración del cumplimiento de los requerimientos legales.
- Proactividad del talento humano en la creación de valor a partir de la gestión de las tecnologías de la información.
- Mayor compromiso de las partes interesadas (Stakeholders).
- El Modelo de referencia de COBIT 5 Incorpora los contenidos de COBIT 4.1, VAL IT y Risk IT.

4.5.4 Comparación de Modelos La tabla 9 muestra un resumen conciso entre los framework de gobierno TI utilizado en el desarrollo de la propuesta**.**

Tabla 9
Comparación de Modelos

Framework	Objetivo	Definición de IT Governance	Estructura y/o principios	Dominio	Referencia
ISO 38500	Promover el uso efectivo, eficiente y aceptable de TI en las organizaciones, con el fin de generar confianza en los grupos de interés (stakeholders) en el gobierno corporativo de las TI. Informar y guiar a la alta dirección en el gobierno de TI en su organización. Proveer los	ISO / IEC 38500, define el gobierno corporativo de TI como" el sistema mediante el cual se dirige y controla el uso actual y futuro de las tecnologías de la información".	1. Responsabilidad 2. Estrategia 3. Adquisición 4. Rendimiento 5. Conformidad 6. Factor Humano	1. Evaluar 2. Dirigir 3. Monitorizar	(ISO/IEC,38 500, 2008)

Tabla 9. Continuación

	fundamentos para la evaluación objetiva por parte de la alta dirección del gobierno de TI.				
COBIT 5	Proporcionar un framework que facilite a las organizaciones alcanzar sus objetivos a través del gobierno y la gestión de las TI corporativas. "Permitir a las TI ser gobernadas y gestionadas de un modo holístico para toda la empresa, abarcando al negocio completo de principio a fin y las áreas funcionales de responsabilidad de TI" (ISACA, 2012)	Es un framework que permite comprender el gobierno y la gestión de TI de una empresa. Así como conocer el nivel de madurez en que se encuentra las TI de la organización, establecer la brecha entre los requerimientos de control, ejes técnicos y los riesgos del negocio.	1. Satisfacer las Necesidades de las Partes Interesadas. 2. Cubrir la empresa de extremo a extremo. 3. Aplicar un Marco de Referencia único integrado. 4. Hacer Posible un Enfoque Holístico. 5. Separar el Gobierno de la Gestión	Gobierno 1. Evaluar 2. Orientar 3. Supervisar Gestión 1. Alinear, Planificar y Organizar. 2. Construir, Adquirir e Implementar. 3. Entregar, Dar Servicio y Soporte. 4. Supervisar, Evaluar y Valorar	**(Isaca, 2012)**

Fuente. Autor del proyecto

4.5.5 Alineación ISO / IEC 38500: 2008 con COBIT 5. Los procesos de gobierno tratan los objetivos de las partes interesadas –entrega de valor, optimización del riesgo y de recursos – e incluye prácticas y actividades orientadas a evaluar opciones estratégicas, proporcionando la dirección de TI y supervisando la salida (Evaluar, orientar y supervisar [EDM] – en completa alineación con las tareas del estándar ISO/IEC 38500, (Matias, 2017).

ISO/IEC 38500:2008 Implementa el gobierno de tecnología de la información como un ciclo de tres (3) actividades (Evaluar – Dirigir y Monitorear), que se efectúan sobre una serie de principios, centrándose en qué se debe hacer y se complementa con COBIT que se

focaliza en cómo hacerlo. La figura 20, ilustra la interacción de las prácticas de gobierno, con las de gestión.

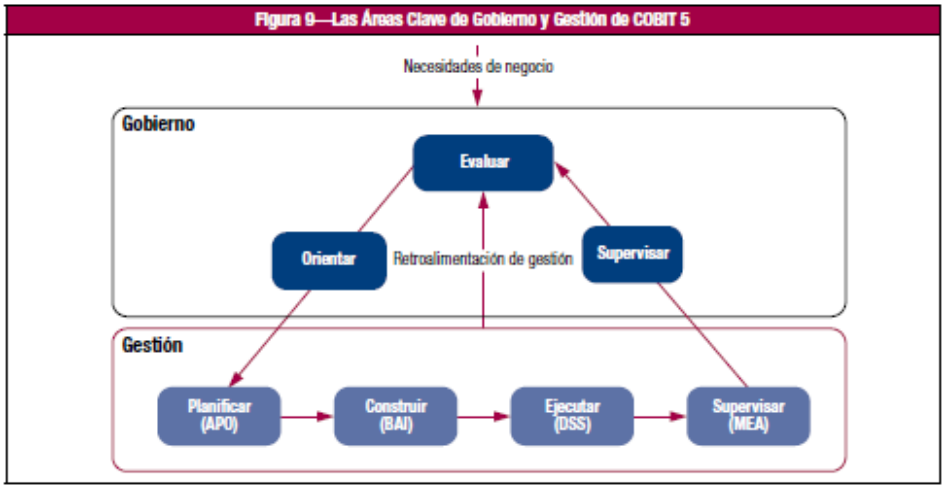

Figura 20. Las áreas clave de gobierno y gestión de Cobit 5
Fuente. Autor del proyecto

En relación, las tareas de evaluar, dirigir y monitorizar del estándar ISO/IEC 38500, estarían cubiertas en el dominio EDM de COBIT 5, en el que cada uno de sus procesos tiene establecidas las actividades de evaluar, orientar y supervisar.

4.5.6 Adopción del estándar ISO/IEC 38500 mediante COBIT 5. A continuación, se describen los principios de la norma ISO/IEC 38500 y los respectivos procesos de COBIT que los portan.

Tabla 10
Mapeo entre los principios de ISO/IEC 38500 mediante COBIT 5

ISO / IEC 38500	COBIT 5
1. Principio Responsabilidad. En la organización los roles están definidos en función de TI y el talento humano tiene la autoridad para realizar las acciones y medidas de las actividades de las que son responsables.	COBIT 5 en los catalizadores procesos y estructuras organizativas, describe los roles y responsabilidades de los stakeholders e involucrados en su implementación. El proceso EDM05 asegura la transparencia hacia

Tabla 10. Continuación

	las partes interesadas, explica el rol del nivel directivo en la supervisión y evaluación del gobierno TI, así como el desempeño de TI, a través de un método genérico que permite establecer las metas y métricas en relación.
2. Principio Estrategia. La planificación estratégica de negocio de la organización tiene en consideración la capacidad actual y futura de TI. Los planes estratégicos de TI satisfacen las necesidades actuales y previstas derivadas de la estrategia de negocio, denominado **(Ballester, 2010)**, alineación del negocio con TI.	En el Dominio de Gobierno, Proceso EDM 02 Asegurar la entrega de beneficios. Provee las orientaciones para realiza la gestión de inversiones en TI y cómo casos del negocio deben ser apoyadas por los objetivos empresariales. El Dominio de Gestión Alinear, Planear y Organizar (APO), referencia los procesos relacionados con la gestión y la planificación de tecnología de información. Adicionando una serie de ejemplos que colaboran con la alineación de las metas corporativas y los procesos TI.
3. Principio Adquisición. Establece que todas las inversiones deben ser transparentes y equilibradas. A su vez tiene que representar una relación coste y beneficio, y comprender el riesgo y oportunidad ventajosa para la organización. Este análisis permite determinar el impacto actual y futuro de la inversión.	El dominio de Gobierno – Evaluar, Orientar y Supervisar (EDM), provee los lineamientos para realizar el análisis de los requerimientos para gobernar y gestionar las inversiones en negocio posibilitadas por las TI. Asegurando el logro de los beneficios con la optimización de costes de los recursos, e identificando el impacto de los riegos de TI ene l valor de la organización. El Dominio Alinear, Planear y Organizar APO - proceso APO05 – se encarga de planificar, alinear y organizar las tareas relacionadas a la adquisición. El Dominio Construir Adquirir e implementar – BAI, define los procesos indispensables para adquirir e implementar soluciones TI, desde la definición de requerimientos, la identificación de viabilidad de las soluciones, documentación, formación y habilitación de usuarios, así como las operaciones para el funcionamiento de los nuevos sistemas. El Dominio Supervisar – Evaluar y Valorar (MEA) – en combinación con el proceso EDM05, definen como pueden realizarse la evaluación y supervisión de la adquisición, así como los lineamientos de control interno para garantizar la gestión correcta.
4. Principio Rendimiento. La Tecnología de información debe ser apropiada para el propósito que ha sido implementada. Para realizar la medición eficaz del desempeño, se debe tener en cuenta la definición clara de las metas de rendimiento y el establecimiento de métricas eficaces para supervisar el logro de estas.	COBIT 5 facilita orientación a los directivos para establecer metas de TI, alineadas a las metas del negocio. Así mismo describe los lineamientos para realizar la supervisión a través de las metas y métricas del cumplimiento de los objetivos. El Proceso APO02 – Gestionar la estrategia y APO09 – Gestionar los acuerdos de servicios. Se centra en definición de metas. El establecimiento de

Tabla 10. Continuación

	los servicios.
	El Proceso MEA01, orienta la responsabilidad de la gestión ejecutiva para realizar la supervisión, evaluación y valoración del rendimiento de los procesos de TI y la conformidad con los requisitos establecidos.
5. Principio Conformidad. El avance de tecnología implica un mayor número de requerimientos de cumplimiento legal para la organización. Garantizar el cumplimiento de los requisitos regulatorios de acuerdo con la normativa vigente.	El proceso APO02 se encarga de alienar la estrategia TI y los objetivos del negocio. El Proceso MEA02 – Supervisar, Evaluar y valorar el sistema de control interno. Realiza la valoración de los controles para detectar posibles deficiencias y elaborar mecanismos de mejora que permitan satisfacer los requisitos de conformidad. El Proceso MEA03 – supervisar, evaluar y valorar la conformidad con los requerimientos externos. Garantiza que se identifique y se cumplan los requerimientos externos de conformidad de todos los procesos relacionados con TI.
6. Principio Factor Humano. Gestión del talento humano. La implementación de cualquier cambio facilitado por las TI, incluyendo el gobierno de las TI en sí mismo, depende de las personas, por lo que se hace necesario la definición de políticas, prácticas y decisiones TI, relacionadas con de comportamiento humano, tanto dentro de la empresa como con los clientes y socios del negocio.	El proceso APO07, Gestiona los Recursos Humanos. Tiene como objetivo mejorar las habilidades y capacidad del talento humano con el fin de logar de manera más eficiente y eficaz las metas de la organización. El Proceso BAI02 se encarga de la gestionar la definición de requisitos. El proceso BAI05 Gestionar la facilitación del cambio organizativo y BAI08 Gestionar el conocimiento. Hace referencia a la formación necesaria del talento humano para responder a los cambios y realizar las actividades de manera correcta.

Fuente. Autor del proyecto

Partiendo de las indicaciones anteriores se ha elaborado la tabla 10, en la que se presenta el mapeo correspondiente entre los principios de ISO/IEC 38500 y su alineación con los Procesos, catalizadores y demás elementos del marco de referencia de COBIT 5.

COBIT 5.0			ISO/IEC 38500					
DOMINIOS Y CATALIZADORES			PRINCIPIOS					
Dominio de Gobierno	Procesos		Responsabilidad	Estrategia	Adquisición	Rendimiento	Conformidad	Comportamiento Humano
Evaluar, Orientar y Supervisar (EDM)	EDM01	Asegurar el establecimiento y mantenimiento del marco de referencia de gobierno						
	EDM02	Asegurar la entrega de beneficios						
	EDM03	Asegurar la optimización del riesgo						
	EDM04	Asegurar la optimización de recursos						
	EDM05	Asegurar la transparencia hacia las partes interesadas						
Dominio de Gestión	Procesos							
Alinear, Planear y Organizar (APO)	APO01	Gestionar el Marco de Gestión de TI						
	APO02	Gestionar la Estrategia						
	APO03	Gestionar la Arquitectura Empresarial						
	APO04	Gestionar la Innovación						
	APO05	Gestionar el Portafolio						
	APO06	Gestionar el Presupuesto y los Costes						
	APO07	Gestionar los Recursos Humanos						
	AP008	Gestionar las relaciones						
	AP009	Gestionar los acuerdos de servicio						
	APO10	Gestionar los Proveedores						
	APO11	Gestionar la Calidad						
	APO12	Gestionar el Riesgo						
	APO13	Gestionar la Seguridad						
Construir, Adquirir e Implementar (BAI)	BAI01	Proyectos						
	BAI02	Gestionar la Definición de Requisitos						
	BAI03	Gestionar la Identificación y Construcción de Soluciones						
	BAI04	Gestionar la Disponibilidad y la Capacidad						
	BAI05	Gestionar la Facilitación del Cambio Organizativo						
	BAI06	Gestionar los Cambios						
	BAI07	Gestionar la Aceptación del Cambio y la Transición						
	BAI08	Gestionar el Conocimiento						
	BAI09	Gestionar los Activos						
	BAI10	Gestionar la Configuración						
Entregar, Dar Servicio y Soporte (DSS)	DSS01	Gestionar Operaciones						
	DSS02	Gestionar Peticiones e Incidentes de Servicio						
	DSS03	Gestionar Problemas						
	DSS04	Gestionar la Continuidad						
	DSS05	Gestionar Servicios de Seguridad						
	DSS06	Gestionar Controles de Proceso de Negocio						
Supervisar, Evaluar y Valorar (MEA)	MEA01	Supervisar, Evaluar y Valorar el Rendimiento y la Conformidad						
	MEA02	Supervisar, Evaluar y Valorar el Sistema de Control Interno						
	MEA03	Supervisar, Evaluar y Valorar la Conformidad con los Requerimientos Externos						
CATALIZADORES	1	Principios, políticas y marcos de referencia						
	2	Procesos						
	3	Estructuras Organizativas						
	4	Cultura, ética y comportamiento						
	5	Información						
	6	Servicios, infraestructuras y aplicaciones						
	7	Personas, habilidades y competencias						
Matriz RACI								
Metas Empresariales								
Metas relacionadas a TI								
Metas y Metricas								
Evaluación de capacidades								

Figura 21. Mapeo entre los principios de ISO/IEC 38500 mediante COBIT 5
Fuente. Autor del proyecto

4.6 Diseño del modelo de gobernanza que facilita la Evaluacion, Direccion y el Control del programa de seguridad y privacidad de los activos de informacion de las entidades del estado colombiano.

A continuación, se relaciona el modelo de Gobernanza de TI propuesto por el autor, resultado de la convergencia entre el marco de Gobierno seleccionado (COBIT versión 5), y los requerimientos del Estado con respecto a la implementación de Gobierno Digital; con el fin de facilitar la Evaluación, Dirección y Monitorización del proceso de Adopción y Gestión del Modelo de Seguridad y Privacidad de la Información alineado con el decreto 1008 del 2018.

4.6.1 Modelo de Gobernanza Propuesto. El modelo de Gobierno TI propuesto está orientado a las entidades del estado que estén obligadas a cumplir con la adopción del Modelo de Seguridad y Privacidad de la Información. Este modelo, está basado en el marco de gobierno definidor por COBIT 5 que define las prácticas para Evaluar el uso actual y futuro de TI en la organización, para Orientar la implementación de los planes y políticas que aseguren la utilización de TI en el alcance de los objetivos corporativos y los lineamientos para Supervisar su desempeño a través del sistema de medición adecuado.

El modelo propuesto, se encuentra alineado con el MSPI como estrategia para el cumplimiento de la Política de Gobierno Digital. Su adopción debe garantizar el cumplimiento de los objetivos corporativos, la generación de valor y el cumplimiento de las regulaciones legales vigentes y demás requisitos de las partes interesadas que se relacionan a continuación:

- **Funcionarios de la institución:** individuos que laboran en la institución pública que adopte el modelo propuesto, que son responsables de la gestión de la información corporativa, los cuales deben contar con lineamientos, procedimientos claros y demás herramientas que agilicen y mejoren sus actividades en cuanto al uso seguro de la información.

- **Proveedores:** Empresas que suministran productos y/o servicios a la institución pública, regulados por el estado y el mercado, de los cuales se recabe información o que dentro de los servicios contratados, deban hacer uso de información de responsabilidad de la institución.

- **Clientes:** Organizaciones o miembros de la comunidad que reciban productos y/o servicios de la institución pública y de los cuales se obtenga información.

- **Contratistas:** individuos que prestan servicios a la institución pública a través de contratos de outsourcing y que dentro de sus actividades hagan uso de información institucional.

- **Entidades de control:** Organizaciones como el Ministerio de las TIC, la procuraduría y demás organizaciones estatales que definen las políticas y lineamientos a cumplir en términos de la protección de la seguridad y la privacidad de la información propia y de terceros que es utilizada dentro de los procesos institucionales por las entidades del sector público.

- **Entes territoriales relacionados con la institución:** Cualquier institución regulada por el Gobierno Colombiano que tenga alguna relación con la institución que adopte el modelo propuesto. Y con la cual se intercambie información que por regulación deba ser cubierta por el MSPI.

4.6.2 Estructura del Modelo de Gobierno Propuesto. El modelo de Gobierno propuesto está estructurado por dominios alineados con los niveles de acuerdo a la pirámide organizacional, las metas de TI y las fases de Modelo de Seguridad y Privacidad de la Información propuesto por MinTIC.

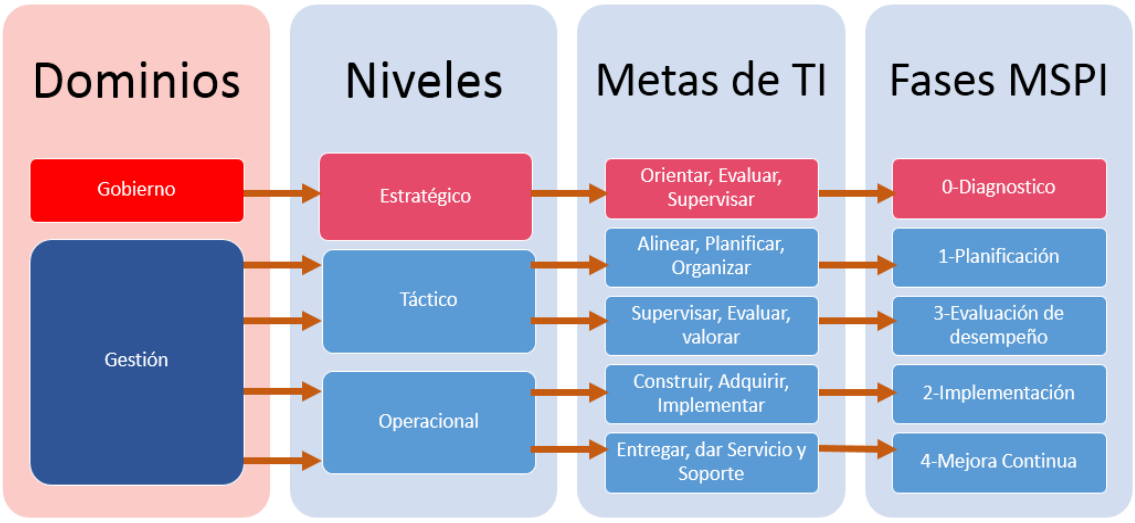

***Figura 22*. Estructura del Modelo de Gobierno propuesto**
Fuente. Autor del proyecto

La Estructura del modelo propuesto alinea las fases del Modelo de Seguridad y Privacidad de la información, orientado principalmente a la gestión de la seguridad de los activos de información, con las metas de TI y procesos del dominio de gestión de COBIT 5, con el fin de facilitar la aplicación de los principales procesos de gobierno propuestos por ISACA al MSPI.

El Modelo consta de 3 Etapas que incluyen actividades de Gobierno y de gestión durante toda la puesta en marcha posterior monitorización del Sistema de gestión de Seguridad y privacidad propuesto por el estado Colombiano.

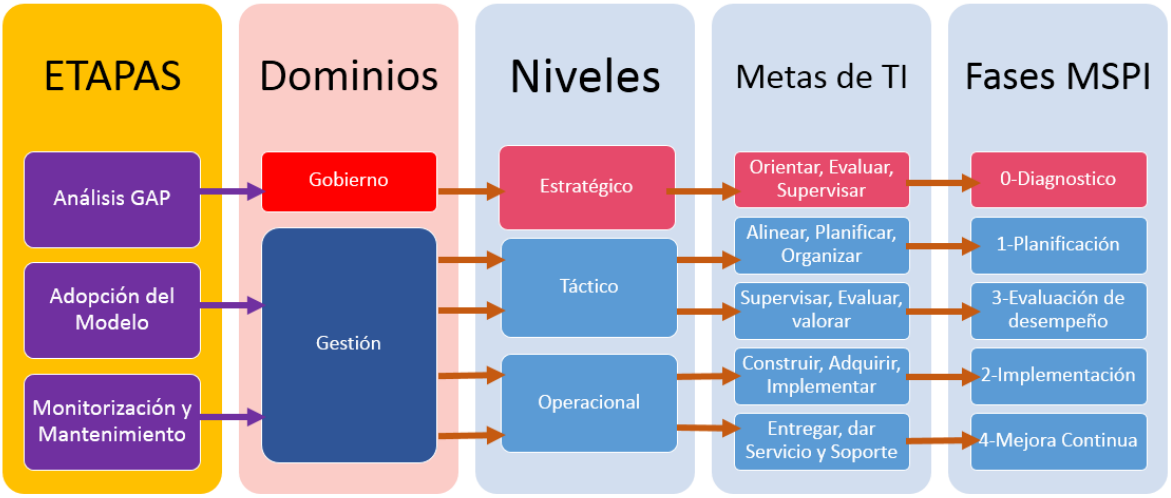

Figura 23. Etapas del Modelo Propuesto alineadas con los dominios del modelo de referencia de procesos
Fuente. Autor del proyecto

Como se aprecia en la figura anterior, las etapas del modelo propuesto son:

- Análisis GAP
- Adopción del Modelo
- Monitorización y Mantenimiento

Las etapas están alineadas con los dominios de Gobierno y Gestión de TI, las metas de TI de COBIT 5.0 y las requeridas para la puesta en producción del MSPI.

A continuación se describe cada una de las etapas del modelo propuesto:

Análisis GAP: El objetivo de esta etapa es la definición de la estrategia necesaria para cumplir con los lineamientos del gobierno referente a la puesta en marcha del Modelo de

Seguridad y Privacidad de la información. Para esto es necesario evaluar el uso actual de la tecnológica y la postura de organización en cuanto a la protección de los activos de información tanto físicos como digitales, de manera que pueda identificarse el nivel de cumplimiento que posee la institución con respecto a las exigencias de la política de Gobierno digital y así poder orientar eficazmente la implementación del MSPI requerido, y realizar la supervisión necesaria sobre este sistema garantizando su continuidad, pertinencia y efectividad.

Adopción del Modelo: Una vez identificadas las necesidades de seguridad de los activos de información de la institución y la brecha referente al cumplimiento de los lineamientos del MSPI, se pasa a la etapa de adopción del modelo propuesto, en la cual realizan las actividades de gestión del nivel táctico y operacional referentes a la organización y la planificación del nuevo sistema de gestión de seguridad y privacidad de la información. A nivel de gestión, en esta etapa principalmente se realiza la clasificación y el análisis de riesgos a los que están expuestos los activos de información de la organización.

Mantenimiento y Monitorización: de manera similar a la etapa anterior, en esta se realizan algunas actividades referentes a la gestión del MSPI, teniendo como objetivo la construcción del sistema de gestión planificado, la adquisición de los recursos necesarios para su operación e implementación, como también la revisión periódica de los procesos de aseguramiento y la mejora continua.

Las principales actividades de esta etapa comprenden la implementación de los controles definidos en el documento de declaración de aplicabilidad de acuerdo con el Anexo A de la

norma técnica NTC-27001, la ejecución del plan de auditorías, la identificación de oportunidades de mejora y los ajustes necesarios para garantizar la operación continua del Sistema de gestión de seguridad y privacidad de la información al igual que la confidencialidad, integridad y disponibilidad de la información reservada de la institución gubernamental.

4.6.3 Alineación de los procesos y actividades del Modelo de gobernanza propuesto.

Con el objetivo de identificar la pertinencia de los procesos de Gobernanza propuestos por COBIT 5.0 que le faciliten al Modelo propuesto la Dirección, Evaluación y la Monitorización de la puesta en marcha del MSPI; se procede a realizar la alineación de los procesos del estándar de Gobierno seleccionado, con las actividades requeridas para la adopción del Modelo de Seguridad y Privacidad de la Información definido por la política de Gobierno digital a las organizaciones del estado.

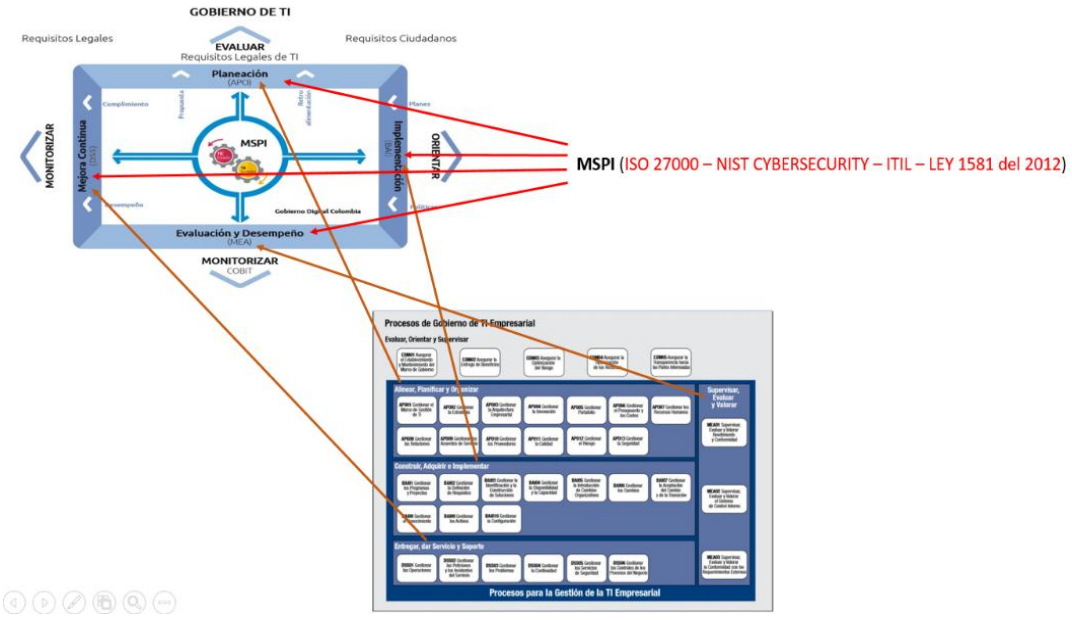

Figura 24. Alineación de las Metas de TI de COBIT 5.0 con el MSPI de MinTIC
Fuente. Autor del proyecto

A continuación, se puede apreciar la alineación de los procesos de COBIT 5.0 con las Actividades del MSPI y su indicador, enmarcadas en las fases del ciclo de mejora continua propuesto por DEMING.

Tabla 11.
Alineación de los procesos de COBIT 5.0 con las actividades del MSPI.

COBIT	Procesos COBIT	FASES MSPI	Actividades del MSPI	Resultado/Indicador
EVALUAR	• [APO01] Gestionar Marco de Gestión de TI • [APO02] Gestionar la Estrategia • [APO04] Gestionar la Innovación • [APO05] Gestionar Portafolio • [APO06] Gestionar el Presupuesto Y los costes • [APO13] Gestionar La seguridad • [APO03] Gestionar Arquitectura Empresarial • [APO11] Gestionar la	PLANEACION	Definición de las Políticas de Seguridad y Privacidad de la Información. Diseño de los procedimientos de Seguridad de la Información.	Documento de políticas de Seguridad. (Revisado y aprobado por la dirección). Procedimientos de seguridad de la Información. (Revisado y aprobado por la

Tabla 11. Continuación

	Calidad		dirección)
	• [APO13] Gestionar La seguridad		
	• [APO08] Gestionar las Relaciones • [APO13] Gestionar La seguridad	Definición de Roles y Responsabilidades de Seguridad y privacidad de la Información	• Nombramiento de Responsable del MSPI (Oficial de Seguridad) • Creación/Adición de Funciones de seguridad de la información al Comité de Gestión Institucional.
	• [BAI09] Gestionar Activos • [APO13] Gestionar la Seguridad	Inventario de Activos de Información	• Documento metodología de identificación, clasificación y valoración de activos (Revisado y aprobado por la dirección). • Matriz de clasificación y valoración de activos de información. • Documento con la caracterización de activos de información, que contengan datos personales • Documento con Inventario de activos computacionales que soporten/sean compatibles con direccionamiento IPv6.

Tabla 11. Continuación

	• [APO13] Gestionar La seguridad • [APO12] Gestionar El Riesgo. • [APO08] Gestionar las Relaciones • [APO09] Gestionar los Acuerdos de Servicios • [APO10] Gestionar los proveedores • [APO13] Gestionar La seguridad	Integración del MSPI con el Sistema de Gestión Documental Identificación, Valoración y tratamiento de riesgo.	• Etiquetado y Control de documentos del MSPI • Documento con la metodología de gestión de riesgos. • Documento con el análisis y evaluación de riesgos. • Documento con el plan de tratamiento de riesgos. • Documento con la declaración de aplicabilidad. • Documentos revisados y aprobados por la alta Dirección.
	[APO07] Gestionar los Recursos Humanos • [APO13] Gestionar la Seguridad	Plan de Comunicaciones Plan de diagnóstico de IPv4 a IPv6 Planificación y	Documento con el plan de comunicación, sensibilización y capacitación para la entidad. Documento con el informe de los activos computacionales que soportan IPv6. Documento con la estrategia de planificación y

Tabla 11. Continuación

			Control Operacional	control operacional (Revisado y aprobado por la dirección).
DIRIGIR/ ORIENTAR	• [BAI01] Gestionar los programas y proyectos • [BAI02] Gestionar la Definición de los requisitos • [BAI03] Gestionar la Identificación y Construcción de Soluciones • [BAI04] Gestionar la Disponibilidad y la capacidad • [BAI05] Gestionar la Introducción de Cambios organizativos • [BAI06] Gestionar los Cambios • [BAI07] Gestionar la aceptación del cambio y la transición • [BAI08] Gestionar el Conocimiento	IMPLEMENTACION	Implementación del Plan de tratamiento de Riesgos	• Informe con la ejecución del plan de tratamiento de riesgos aprobado por cada dueño de procesos. Anexos de acuerdo a los controles relacionados en la declaración de aplicabilidad: • Informe de implementación/puesta en producción de procedimientos de seguridad de la información en los diferentes procesos de la organización. • Informe de implementación de controles de acceso. • Informe de implementación de controles de perímetro. • Informe de implementación de controles criptográficos. • Informe de ejecución de las actividades de concienciación de

Tabla 11. Continuación

	• [BAI09] Gestionar los Activos • [BAI10] Gestionar la Configuración • [APO13] Gestionar la Seguridad		los funcionarios y contratistas de la organización. • Informes de todos los controles técnicos y administrativos referentes a los controles definidos en el plan de implementación.
	• [APO13] Gestionar la Seguridad	Indicadores de Gestión	Documento con la descripción de los indicadores de gestión de seguridad y privacidad de la información.
	• [BAI01] Gestionar los programas y proyectos	Plan de Transición de IPv4 a IPv6	Documento con las estrategias del plan de implementación de IPv6 en la entidad, aprobado por la Oficina de TI.
	• [APO13] Gestionar la Seguridad	Plan de revisión y seguimiento a la implementación del MSPI	Documento con el plan de seguimiento, revisión y auditoria del MSPI (Revisado y aprobado por la dirección).
SUPERVISAR / MONITORIZA	• [MEA01] Supervisar Evaluar, valorar Rendimiento y Conformidad • [MEA02] Supervisar		• Documento con el plan de ejecución de las auditorías al igual que las revisiones independientes al MSPI (Revisado y aprobado por la

Tabla 11. Continuación

R	Evaluar, valorar El Sistema de Control Interno • [MEA03] Supervisar Evaluar y valorar La conformidad con requisitos externos • [DSS01] Gestionar las operaciones • [DSS02] Gestionar las peticiones y los incidentes del servicio • [DSS03] Gestionar los problemas • [DSS04] Gestionar la continuidad • [DSS05] Gestionar los servicios de	EVAL. DESEMPEÑO MEJORA CONTINUA	Plan de Ejecución de Auditorias Plan de mejora continua	dirección). Anexos: • Documento con el resultado de la ejecución del plan de auditorías. • Documento con las observaciones, no conformidades menores y mayores identificadas durante la ejecución de las auditorias. • Documento con los hallazgos y evidencias sobre la efectividad de los controles implementados, así como de las desviaciones identificadas. • Documento con el plan de mejoramiento del MSPI. • Documento con el plan de comunicación de resultados.

Tabla 11. Continuación

	seguridad • [DSS06] Gestionar los Controles de los procesos del Negocio • [APO13] Gestionar la Seguridad

Fuente. Autor del proyecto

4.6.4 Métricas de los procesos del Modelo propuesto. Con el fin de poder medir el desempeño de los procesos y del modelo de Gobernanza propuesto, es necesario contar con unas variables que serán usadas como métricas, las cuales se relacionan a continuación y se discriminan por procesos:

Tabla 12
Descripción, metas y métricas del modelo propuesto. Proceso APO01

APO01: Gestionar el Marco de Gestión de TI	**Descripción del proceso**: Aclarar y mantener el gobierno de la misión y la visión corporativa de TI. Implementar y mantener mecanismos y autoridades para la gestión de la información y el uso de TI en la empresa para apoyar los objetivos de gobierno en consonancia con las políticas y los principios rectores.
Meta del Proceso	**Métricas Relacionadas**
1. Se ha definido y se mantiene un conjunto eficaz de políticas.	• Porcentaje de políticas, estándares y otros elementos catalizadores activos documentados y actualizados. • Fecha de las últimas actualizaciones del marco de trabajo y de los elementos catalizadores. • Número de exposiciones a riesgos debidas a la inadecuación del diseño del entorno de control
2. Todos tienen conocimiento de las políticas y de cómo deberían implementarse.	• Número de empleados que asistieron a sesiones de formación o de sensibilización. • Porcentaje de proveedores indirectos con contratos en los que se definen requisitos de control.

Fuente. (ISACA, 2012)

Tabla 13
Descripción, metas y métricas del modelo propuesto. Proceso APO02

APO02: Gestionar la Estrategia	**Descripción del proceso**: Proporcionar una visión holística del negocio actual y del entorno de TI, la dirección futura, y las iniciativas necesarias para migrar al entorno deseado. Aprovechar los bloques y componentes de la estructura empresarial, incluyendo los servicios externalizados y las capacidades relacionadas que permitan una respuesta ágil, confiable y eficiente a los objetivos estratégicos.
Meta del Proceso	**Métricas Relacionadas**
1. Todos los aspectos de la estrategia de TI están alineados con la estrategia del negocio.	• Porcentaje de objetivos en la estrategia de TI que soportan la estrategia de negocio. • Porcentaje de los objetivos del negocio considerados en la estrategia de TI
2. La estrategia de TI es coste-efectiva, apropiada, realista, factible, enfocada al negocio y equilibrada.	• Porcentaje de iniciativas en la estrategia de TI autofinanciadas (los beneficios superan los costes). • Tendencias en el retorno de inversión (ROI) de las iniciativas incluidas en la estrategia de TI. • Encuesta sobre el nivel de satisfacción de las partes interesadas sobre las estrategias de TI
3. Se pueden derivar objetivos a corto plazo claros, concretos, y trazables de iniciativas a largo plazo específicas, y se pueden traducir, por tanto, en planes operativos.	• Porcentaje de proyectos en la cartera de proyectos de TI que pueden ser directamente trazables con la estrategia de TI.
4. TI es un generador de valor para el negocio.	• Porcentaje de los objetivos estratégicos empresariales obtenidos como resultado de iniciativas estratégicas de TI. • Número de nuevas oportunidades de negocio generadas como resultado directo de los desarrollos de TI. • Porcentaje de proyectos/iniciativas de TI respaldados directamente por los propietarios del negocio.
5. Existe conciencia de la estrategia de TI y una clara asignación de responsabilidades para su entrega.	• Consecución de resultados estratégicos de TI medibles como parte de los objetivos de desempeño del personal. • Frecuencia de actualizaciones del plan de comunicación de la estrategia de TI. • Porcentaje de iniciativas estratégicas con asignación de responsabilidades.

Fuente. (ISACA, 2012)

Tabla 14
Descripción, metas y métricas del modelo propuesto. Proceso APO03

APO03: Gestionar la Arquitectura Empresarial	**Descripción del proceso**: Establecer una arquitectura común compuesta por los procesos de negocio, la información, los datos, las aplicaciones y las capas de la arquitectura tecnológica de manera eficaz y eficiente para la realización de las estrategias de la empresa y de TI mediante la creación de modelos clave y prácticas que describan las líneas de partida y las arquitecturas objetivo. Definir los requisitos para la taxonomía, las normas, las directrices, los procedimientos, las plantillas y las herramientas y proporcionar un vínculo para estos componentes. Mejorar la adecuación, aumentar la agilidad, mejorar la calidad de la información y generar ahorros de costes potenciales mediante iniciativas tales como la reutilización de bloques de componentes para los procesos de construcción.
Meta del Proceso	**Métricas Relacionadas**
1. La arquitectura y los estándares son eficaces apoyando a la empresa.	• Número de excepciones solicitadas y concedidas en los estándares de la arquitectura básica. • Nivel de realimentación sobre la arquitectura por parte del cliente. • Beneficios aportados por el proyecto que pueden ser trazados a la implicación de la arquitectura (por ejemplo, reducción de costes debido a la reutilización).
2. La cartera de servicios de la arquitectura de empresa soporta el cambio empresarial ágil.	• Porcentaje de proyectos que usan los servicios de la arquitectura de empresa. • Nivel de realimentación sobre la arquitectura por parte del cliente
3. Existen dominios apropiados y actualizados y/o arquitecturas federadas que proveen información fiable de la arquitectura.	• Fecha de la última actualización en el dominio y/o arquitecturas federadas. • Número de deficiencias detectadas en los modelos a lo largo de los dominios de empresa, información, datos, aplicaciones y arquitectura de tecnología. • Nivel de realimentación del cliente de la arquitectura en relación a la calidad de la información proporcionada.
4. Se utiliza un marco de arquitectura de empresa y una metodología común, así como un repositorio de arquitectura integrado, con el fin de permitir la reutilización de eficiencias dentro de la empresa.	• Porcentaje de proyectos que utilizan el marco de trabajo y la metodología para reutilizar componentes ya definidos. • Número de personas formadas en la metodología y en el manejo del conjunto de herramientas. • Número de excepciones concedidas en los estándares de la arquitectura básica.

Fuente. (ISACA, 2012)

Tabla 15

Descripción, metas y métricas del modelo propuesto. Proceso APO04

APO04: Gestionar la Innovación	**Descripción del proceso**: Mantener un conocimiento de la tecnología de la información y las tendencias relacionadas con el servicio, identificar las oportunidades de innovación y planificar la manera de beneficiarse de la innovación en relación con las necesidades del negocio. Analizar cuáles son las oportunidades para la innovación empresarial o qué mejora puede crearse con las nuevas tecnologías, servicios o innovaciones empresariales facilitadas por TI, así como a través de las tecnologías ya existentes y por la innovación en procesos empresariales y de TI. Influir en la planificación estratégica y en las decisiones de la arquitectura de empresa
Meta del Proceso	**Métricas Relacionadas**
1. El valor de empresa es creado mediante la cualificación y puesta en escena de los avances e innovaciones tecnológicas más apropiadas, los métodos y las soluciones TI utilizadas.	• Penetración en el mercado o competitividad debido a la innovación. • Percepciones de las partes interesadas y realimentación sobre la innovación en TI.
2. Los objetivos de la empresa se cumplen por la mejora de los beneficios de la calidad y/o la reducción de costes como resultado de la identificación e implementación de soluciones innovadoras.	• Porcentaje de las iniciativas implementadas que dieron los beneficios previstos. • Porcentaje de las iniciativas implementadas con un vínculo claro a los objetivos de la empresa.
3. La innovación se permite y se promueve y forma parte de la cultura de la empresa.	• Introducción de objetivos de innovación o relacionados con tecnologías emergentes en las metas de rendimiento para personal relevante. • Opinión y encuestas de partes interesadas.

Fuente. (ISACA, 2012)

Tabla 16

Descripción, metas y métricas del modelo propuesto. Proceso APO05.

Tabla 16. Continuación

APO05: Gestionar el Portafolio	**Descripción del proceso**: Ejecutar el conjunto de direcciones estratégicas para la inversión alineada con la visión de la arquitectura empresarial, las características deseadas de inversión, los portafolios de servicios relacionados, considerar las diferentes categorías de inversión y recursos y las restricciones de financiación. Evaluar, priorizar y equilibrar programas y servicios, gestionar la demanda con los recursos y restricciones de fondos, basados en

	su alineamiento con los objetivos estratégicos, así como en su valor y riesgo corporativo. Mover los programas seleccionados al portafolio de servicios activos listos para ser ejecutados. Supervisar el rendimiento global del portafolio de servicios y programas, proponiendo ajustes si fuesen necesarios en respuesta al rendimiento de programas y servicios o al cambio en las prioridades corporativas.
Meta del Proceso	**Métricas Relacionadas**
1. Se ha definido una mezcla apropiada de inversión alineada con la estrategia corporativa.	• Porcentaje de inversiones TI que tienen trazabilidad con la estrategia de la compañía. • Grado hasta el que la dirección corporativa está satisfecha con la contribución de TI a la estrategia empresarial.
2. Fuentes de fondos de inversión identificados y están disponibles.	• Relación entre fondos asignados y fondos usados. • Relación entre fondos disponibles y fondos asignados
3. Casos de negocio de programa evaluados y priorizados antes de que se asignen los fondos.	• Porcentaje de unidades de negocio involucradas en la evaluación y priorización de procesos
4. Existe una vista precisa y comprensiva del rendimiento de las inversiones del portafolio.	• Nivel de satisfacción con los informes de supervisión del portafolio
5. Los cambios en el programa de inversiones se reflejan en los portafolios relevantes de servicios, activos y recursos de TI.	• Porcentaje de cambios del programa de inversiones reflejados en los portafolios relevantes de TI.
6. Los beneficios han sido generados debido a los beneficios de la monitorización.	• Porcentaje de inversiones en los que los beneficios producidos han sido medidos y comparados con el caso de negocio.

Fuente. (ISACA, 2012)

Tabla 17

Descripción, metas y métricas del modelo propuesto. Proceso APO06.

APO06: Gestionar el presupuesto y los costes	**Descripción del proceso:** Gestionar las actividades financieras relacionadas con las TI tanto en el negocio como en las funciones de TI, abarcando presupuesto, coste y gestión del beneficio, y la priorización del gasto mediante el uso de prácticas presupuestarias formales y un sistema justo y equitativo de reparto de costes a la empresa. Consultar a las partes interesadas para identificar y controlar los costes totales y los beneficios en el contexto de los planes estratégicos y tácticos de TI, e iniciar

Tabla 17. Continuación

	acciones correctivas cuando sea necesario.
Meta del Proceso	**Métricas Relacionadas**
1. Un presupuesto de TI transparente y completo que refleja adecuadamente los gastos planificados.	• Número de cambios en el presupuesto debido a omisiones y errores. • Número de desviaciones entre las categorías presupuestarias previstas y reales
2. La asignación de recursos de TI para las iniciativas de TI se prioriza basándose en necesidades de la empresa.	• Porcentaje de la alineación de los recursos de TI con iniciativas de alta prioridad. • Número de problemas de asignación de recursos escalados.
3. Los costes de los servicios se asignan de manera equitativa.	• Porcentaje de costes generales de TI que se han asignado de acuerdo con los modelos de costes acordados.
4. Los presupuestos pueden ser comparados con precisión con los costes reales.	• Porcentaje de variación entre los presupuestos, previsiones y los costes reales.

Fuente. (ISACA, 2012)

Tabla 18

Descripción, metas y métricas del modelo propuesto. Proceso APO07.

APO07: Gestionar los Recursos Humanos	**Descripción del proceso**: Proporcionar un enfoque estructurado para garantizar una óptima estructuración, ubicación, capacidades de decisión y habilidades de los recursos humanos. Esto incluye la comunicación de las funciones y responsabilidades definidas, la formación y planes de desarrollo personal y las expectativas de desempeño, con el apoyo de gente competente y motivada.
Meta del Proceso	**Métricas Relacionadas**
1. La estructura organizacional y las relaciones de TI son flexibles y dan respuesta ágil.	• Número de definiciones de servicio y catálogos de servicio. • Nivel de satisfacción de los ejecutivos con la toma de decisiones de la gerencia. • Número de decisiones que no pudieron resolverse dentro de las estructuras de gestión y se escalaron a las estructuras de gobierno
4. Los recursos humanos son gestionados eficaz y eficientemente.	• Porcentaje de rotación del personal. • Duración media de las vacantes. • Porcentaje de puestos de TI vacantes.

Fuente. (ISACA, 2012)

Tabla 19
Descripción, metas y métricas del modelo propuesto. Proceso APO08.

APO08: Gestionar las Relaciones	**Descripción del proceso:** Gestionar las relaciones entre el negocio y TI de modo formal y transparente, enfocándolas hacia el objetivo común de obtener resultados empresariales exitosos apoyando los objetivos estratégicos y dentro de las restricciones del presupuesto y los riesgos tolerables. Basar la relación en la confianza mutua, usando términos entendibles, lenguaje común y voluntad de asumir la propiedad y responsabilidad en las decisiones claves.
Meta del Proceso	**Métricas Relacionadas**
1. Las estrategias, planes y requisitos de negocio están bien entendidos, documentados y aprobados.	• Porcentaje de servicios TI alineados con los requisitos del negocio.
2. Existencia de buenas relaciones entre la empresa y las TI.	• Resultados de las encuestas de satisfacción de los usuarios y del personal de TI.
3. Las partes interesadas del negocio son conscientes de las oportunidades posibilitadas por la TI.	• Encuesta del nivel de concienciación tecnológica de las partes interesadas de negocio. • Ratio de oportunidades tecnológicas incluidas en las propuestas de inversión.

Fuente. (ISACA, 2012)

Tabla 20 *Descripción, metas y métricas del modelo propuesto. Proceso APO09.*

APO09: Gestionar los Acuerdos de Servicios	**Descripción del proceso**: Alinear los servicios basados en TI y los niveles de servicio con las necesidades y expectativas de la empresa, incluyendo identificación, especificación, diseño, publicación, acuerdo y supervisión de los servicios TI, niveles de servicio e indicadores de rendimiento.
Meta del Proceso	**Métricas Relacionadas**
1. La empresa puede usar de modo efectivo los servicios TI tal como se han definido en el catálogo.	• Número de procesos de negocio con acuerdos de servicio sin definir.
2. Los acuerdos de servicio reflejan las capacidades y necesidades de la TI.	• Porcentaje de servicio TI activos cubiertos por acuerdos de servicio. • Porcentaje de clientes satisfechos porque el servicio cumple los niveles acordados.
3. Los servicios TI rinden como está estipulado en los acuerdos de servicio.	• Número y severidad de incumplimientos del servicio. • Porcentaje de servicios monitorizados para cumplir los acuerdos. • Porcentaje de servicios que alcanzan su objetivo.

Fuente. (ISACA, 2012)

Tabla 21
Descripción, metas y métricas del modelo propuesto. Proceso APO10.

APO10: Gestionar los Proveedores	**Descripción del proceso**: Administrar todos los servicios de TI prestados por todo tipo de proveedores para satisfacer las necesidades del negocio, incluyendo la selección de los proveedores, la gestión de las relaciones, la gestión de los contratos y la revisión y supervisión del desempeño, para una eficacia y cumplimiento adecuados.
Meta del Proceso	**Métricas Relacionadas**
1. Los proveedores rinden según lo acordado.	• Porcentaje de proveedores que cumplen con los requisitos acordados. • Número de infracciones de servicio causadas por los proveedores.
2. El riesgo de los proveedores se evalúa y trata adecuadamente.	• Número de eventos de riesgo que conducen a incidentes del servicio. • Frecuencia de las reuniones con suministradores sobre la gestión de riesgos. • Porcentaje de los incidentes relacionados con el riesgo resuelto adecuadamente (en tiempo y coste).
3. Las relaciones con los proveedores son eficaces.	• Numero de reuniones de revisión con proveedores. • Número de disputas formales con proveedores. • Porcentaje de disputas con proveedores resueltas adecuadamente y en un tiempo razonable.

Fuente. (ISACA, 2012)

Tabla 22
Descripción, metas y métricas del modelo propuesto. Proceso APO11.

APO11: Gestionar la Calidad	**Descripción del proceso**: Definir y comunicar los requisitos de calidad en todos los procesos, procedimientos y resultados relacionados de la organización, incluyendo controles, vigilancia constante y el uso de prácticas probadas y estándares de mejora continua y esfuerzos de eficiencia.
Meta del Proceso	**Métricas Relacionadas**
1. Las partes interesadas están satisfechas con la calidad de los servicios y las soluciones.	• Promedio de satisfacción de las partes interesadas con las soluciones y servicios. • Porcentaje de partes interesadas satisfechos con la calidad de TI. • Número de servicios con un plan de gestión de la calidad formal.

Tabla 22. Continuación

2. Los resultados de los proyectos y de los servicios entregados son predecibles.	• Porcentaje de proyectos revisados que cumplen con las metas y objetivos de calidad. • Porcentaje de soluciones y servicios entregados con una certificación formal. • Número de defectos sin descubrir antes de la puesta en producción.
3. Los requisitos de calidad están implementados en todos los procesos.	• Número de procesos con un requisito de calidad definido. • Número de procesos con un informe de evaluación formal de la calidad. • Número de ANSs que incluyen criterios de aceptación de calidad.

Fuente. (ISACA, 2012)

Tabla 23

Descripción, metas y métricas del modelo propuesto. Proceso APO12.

APO12: Gestionar el Riesgo	**Descripción del proceso**: Identificar, evaluar y reducir los riesgos relacionados con TI de forma continua, dentro de niveles de tolerancia establecidos por la dirección ejecutiva de La empresa.
Meta del Proceso	**Métricas Relacionadas**
1. El riesgo relacionado con TI está identificado, analizado, gestionado y reportado.	• Grado de visibilidad y reconocimiento en el entorno actual. • Número de eventos de pérdida con características clave, capturados en • Repositorios. • Porcentaje de auditorías, eventos y tendencias capturados en repositorios.
2. Existe un perfil de riesgo actual y completo.	• Porcentaje de procesos de negocio claves incluidos en el perfil de riesgo • Completitud de atributos y valores en el perfil de riesgo
3. Todas las acciones de gestión para los riesgos significativos están gestionadas y bajo control.	• Porcentaje de propuestas de gestión de riesgos rechazadas debido a una falta de consideración sobre algún riesgo relacionado. • Número de incidentes significativos no identificados e incluidos en el portafolio de gestión de riesgos.
4. Las acciones de gestión de riesgos están efectivamente implementadas.	• Porcentaje de planes de acción para riesgos de TI ejecutados de la forma que fueron diseñados. • Número de medidas que no reducen el riesgo residual.

Fuente. (ISACA, 2012)

Tabla 24
Descripción, metas y métricas del modelo propuesto. Proceso APO13.

APO13: Gestionar la Seguridad	**Descripción del proceso**: Definir, operar y supervisar un sistema para la gestión de la seguridad de la información.
Meta del Proceso	**Métricas Relacionadas**
1. Está en marcha un sistema que considera y trata efectivamente los requerimientos de seguridad de la información de la empresa.	• Número de roles de seguridad claves claramente definidos. • Número de incidentes relacionados con la seguridad.
2. Se ha establecido, aceptado y comunicado por toda la empresa un plan de seguridad.	• Nivel de satisfacción de las partes interesadas con el plan de seguridad de toda la empresa. • Número de soluciones de seguridad que se desvían del plan. • Número de soluciones de seguridad que se desvían de la arquitectura de la empresa.
3. Las soluciones de seguridad de la información están implementadas y operadas de forma consistente en toda la empresa.	• Número de servicios con alineamiento confirmado al plan de seguridad. • Número de incidentes de seguridad causados por la no observancia del plan de seguridad. • Número de soluciones desarrolladas con alineamiento confirmado al plan de seguridad.

Fuente. (ISACA, 2012)

Tabla 25.
Descripción, metas y métricas del modelo propuesto. Proceso BAI01.

BAI01: Gestionar los programas y proyectos	**Descripción del proceso**: Gestionar todos los programas y proyectos del portafolio de inversiones de forma coordinada y en línea con la estrategia corporativa. Iniciar, planificar, controlar y ejecutar programas y proyectos y cerrarlos con una revisión post-implementación.
Meta del Proceso	**Métricas Relacionadas**
1. Las partes interesadas relevantes están comprometidas con los programas y los proyectos.	• Porcentaje de partes interesadas efectivamente comprometidas. • Nivel de satisfacción con la involucración de las partes interesadas.
2. El alcance y los resultados de los programas y proyectos son viables y están alineados con los objetivos.	• Porcentaje de grupos de interés que aprueban las necesidades de la empresa, el alcance, los resultados esperados y el nivel de riesgo del proyecto. • Porcentaje de proyectos emprendidos sin casos de negocio aprobados.
3. Los planes de programas y proyectos tienen probabilidades de lograr los	• Porcentaje de actividades alineadas al alcance y a los resultados esperados.

Tabla 25. Continuación

resultados esperados.	• Porcentaje de programas activos emprendidos sin mapas de valor de programa actualizados y válidos.
4. Las actividades de los programas y proyectos se ejecutan de acuerdo a los planes.	• Frecuencia de revisiones de estado. • Porcentaje de desviaciones del plan de referencia. • Porcentaje de partes interesadas que firman las revisiones de cambio de estado (stage-gate) de los programas activos
5. Existen suficientes recursos de los programas y proyectos para realizar las actividades de acuerdo a los planes.	• Número de incidentes con recursos (por ejemplo, habilidades, capacidad).
6. Los beneficios esperados de los programas y proyectos son obtenidos y aceptados.	• Porcentaje de beneficios esperados que se han alcanzado. • Porcentaje de resultados aceptados al primer intento. • Nivel de satisfacción expresada por las partes interesadas en las revisiones de cierre de proyectos.

Fuente. (ISACA, 2012)

Tabla 26

Descripción, metas y métricas del modelo propuesto. Proceso BAI02.

BAI02: Gestionar la Definición de los requisitos	**Descripción del proceso**: Identificar soluciones y analizar requerimientos antes de la adquisición o creación para asegurar que estén en línea con los requerimientos estratégicos de la organización y que cubren los procesos de negocios, aplicaciones, información/datos, infraestructura y servicios. Coordinar con las partes interesadas afectadas la revisión de las opciones viables, incluyendo costes y beneficios relacionados, análisis de riesgo y aprobación de los requerimientos y soluciones propuestas.
Meta del Proceso	**Métricas Relacionadas**
1. Los requerimientos funcionales y técnicos del negocio reflejan las necesidades y expectativas de la organización.	• Porcentaje de requerimientos repetidos debido a la no alineación entre las necesidades y expectativas de la organización. • Nivel de satisfacción de las partes interesadas con los requerimientos.
2. La solución propuesta satisface los requerimientos funcionales, técnicos y de cumplimiento del negocio.	• Porcentaje de requerimientos satisfechos por la solución propuesta.

Tabla 26. Continuación

3. El riesgo asociado con los requerimientos ha sido tomado en cuenta en la solución propuesta.	• Números de incidentes no identificados como riesgo. • Porcentaje de riesgos no mitigado exitosamente.
4. Los requerimientos y soluciones propuestas cumplen con los objetivos del caso de negocio (valor esperado y costes probables).	• Porcentaje de los objetivos del caso de negocio alcanzados por la solución propuesta. • Porcentaje de partes interesadas que no aprueban la solución con relación al caso de negocio.

Fuente. (ISACA, 2012)

Tabla 27

Descripción, metas y métricas del modelo propuesto. Proceso BAI03.

BAI03: Gestionar la Identificación y Construcción de Soluciones	**Descripción del proceso**: Establecer y mantener soluciones identificadas en línea con los requerimientos de la empresa que abarcan el diseño, desarrollo, compras/contratación Y asociación con proveedores/fabricantes. Gestionar la configuración, preparación de pruebas, realización de pruebas, gestión de requerimientos y mantenimiento de procesos de negocio, aplicaciones, datos/información, infraestructura y servicios.
Meta del Proceso	**Métricas Relacionadas**
1. El diseño de la solución, incluyendo los componentes relevantes, debe cumplir con las necesidades de la empresa, alineándose con estándares y tratando todos los riesgos identificados.	• Número de rediseños realizados debido a discordancias con los requerimientos. • Tiempo para aprobar que el entregable de diseño ha cumplido los requerimientos.
2. La solución conforme al diseño, es acorde a las normas organizativas y cuenta con controles, seguridad y 'auditabilidad' apropiadas.	• Número de excepciones al diseño observadas durante la fase de revisión
3. La solución es de una calidad aceptable y ha sido probada convenientemente.	• Número de errores encontrados durante las pruebas. • Tiempo y esfuerzo para completar las pruebas.
4. Los cambios aprobados de los requerimientos están correctamente incorporadas a la solución.	• Número de cambios aprobados y registrados que generan nuevos errores.
5. Las actividades de mantenimiento cumplen satisfactoriamente con las necesidades tecnológicas y de negocio.	• Número de solicitudes de mantenimiento no atendidas.

Fuente. (ISACA, 2012)

Tabla 28

Descripción, metas y métricas del modelo propuesto. Proceso BAI04.

BAI04: Gestionar la Disponibilidad y la capacidad	**Descripción del proceso**: Equilibrar las necesidades actuales y futuras de disponibilidad, rendimiento y capacidad con una provisión de servicio efectiva en costes. Incluye la evaluación de las capacidades actuales, la previsión de necesidades futuras basadas en los requerimientos del negocio, el análisis del impacto en el negocio y la evaluación del riesgo para planificar e implementar acciones para alcanzar los requerimientos identificados.
Meta del Proceso	**Métricas Relacionadas**
1. El plan de disponibilidad anticipa la expectativa del negocio en cuanto a requerimientos críticos de capacidad.	• Número de actualizaciones de capacidad, rendimiento o disponibilidad no planificada.
2. Cumplimiento de requerimientos de capacidad, rendimiento y disponibilidad.	• Número de picos de transacciones donde se excede la meta de rendimiento. • Número de incidentes de disponibilidad. • Número de eventos donde la capacidad ha excedido los límites planificados.
3. Cuestiones de disponibilidad, rendimiento y capacidad identificados y resueltos de manera rutinaria.	• Número y porcentaje de cuestiones de disponibilidad, rendimiento y capacidad no resueltos.

Fuente. (ISACA, 2012)

Tabla 29

Descripción, metas y métricas del modelo propuesto. Proceso BAI05.

BAI05: Gestionar la Introducción del Cambio organizativo.	**Descripción del proceso**: Maximizar la probabilidad de la implementación exitosa en toda la empresa del cambio organizativo de forma rápida y con riesgo reducido, cubriendo el ciclo de vida completo del cambio y todos las partes interesadas del negocio y de TI.
Meta del Proceso	Métricas Relacionadas
1. El deseo de cambio de las partes interesadas ha sido entendido.	• Nivel de deseo de cambio de las partes interesadas. • Nivel de involucración de la alta dirección.
2. El equipo de implementación es competente y está habilitado para conducir el cambio.	• Índices de satisfacción de las partes interesadas afectadas con el equipo de implementación. • Numero de habilidades identificadas o cuestiones de capacidad.
3. El cambio deseado es comprendido y aceptado por las partes interesadas.	• Comentarios de las partes interesadas sobre el nivel de comprensión. • Número de preguntas recibidas.

Tabla 29. Continuación

4. Los que juegan algún papel están facultados para entregar el cambio.	• Porcentaje de los que juegan algún papel con una autoridad asignada adecuada. • Comentarios de los que juegan algún papel acerca del nivel de facultamiento.
5. Todos los que juegan algún papel están habilitados para operar, utilizar y mantener el cambio.	• Porcentaje de los que juegan algún papel debidamente formados. • Autoevaluación de capacidades relevantes por parte de los que juegan algún papel. • Nivel de satisfacción de los que juegan algún papel operando, utilizando y manteniendo el cambio.
6. El cambio está integrado y sostenido.	• Porcentaje de usuarios adecuadamente formados en el cambio. • Nivel de satisfacción de los usuarios con la adopción del cambio.

Fuente. (ISACA, 2012)

Tabla 30

Descripción, metas y métricas del modelo propuesto. Proceso BAI06.

BAI06: Gestionar los Cambios	**Descripción del proceso**: Gestione todos los cambios de una forma controlada, incluyendo cambios estándar y de mantenimiento de emergencia en relación con los procesos de negocio, aplicaciones e infraestructura. Esto incluye normas y procedimientos de cambio, análisis de impacto, priorización y autorización, cambios de emergencia, seguimiento, reporte, cierre y documentación.
Meta del Proceso	**Métricas Relacionadas**
1. Los cambios autorizados son realizados de acuerdo a sus cronogramas respectivos y con errores mínimos.	• Cantidad de trabajo rehecho debido a cambios fallidos. • Reducción en el tiempo y esfuerzo necesarios para aplicar los cambios. • Número y antigüedad de peticiones de cambio en cartera.
2. Las evaluaciones de impacto revelan el efecto de los cambios sobre todos los componentes afectados.	• Porcentaje de cambios sin éxito debidos a evaluaciones de impacto inadecuadas.
3. Todos los cambios de emergencia son revisados y autorizados una vez hecho el cambio.	• Porcentaje sobre el total de cambios que corresponde a cambios de emergencia. • Número de cambios de emergencia no autorizados una vez hecho el cambio.
4. Las principales partes interesadas están informadas sobre todos los aspectos del cambio.	• Ratios de satisfacción de las partes interesadas con las comunicaciones de los cambios.

Fuente. (ISACA, 2012)

Tabla 31

Descripción, metas y métricas del modelo propuesto. Proceso BAI07.

BAI07: Gestionar la aceptación al cambio y la transición	**Descripción del proceso**: Aceptar formalmente y hacer operativas las nuevas soluciones, incluyendo la planificación de la implementación, la conversión de los datos y los sistemas, las pruebas de aceptación, la comunicación, la preparación del lanzamiento, el paso a producción de procesos de negocio o servicios TI nuevos o modificados, el soporte temprano en producción y una revisión post-implementación.
Meta del Proceso	**Métricas Relacionadas**
1. Las pruebas de aceptación consiguen la aprobación de las partes interesadas y tienen en cuenta todos los aspectos de los planes de implementación y conversión.	• Porcentaje de partes interesadas satisfechas con la completitud del proceso de pruebas.
2. Los lanzamientos están listos para su paso a producción contando con la buena disposición y el soporte de las partes interesadas.	• Número y porcentaje de lanzamientos que no están listos para lanzamiento en los plazos previstos.
3. Los lanzamientos pasan a producción satisfactoriamente, son estables y cumplen con las expectativas.	• Número o porcentaje de lanzamientos que no consiguen ser estables en un periodo de tiempo aceptable. • Porcentaje de lanzamientos que causan períodos de inactividad.
4. Las lecciones aprendidas contribuyen a futuros lanzamientos.	• Número y porcentaje de análisis de causa raíz completados.

Fuente. (ISACA, 2012)

Tabla 32

Descripción, metas y métricas del modelo propuesto. Proceso BAI08.

BAI08: Gestionar el Conocimiento	**Descripción del proceso**: Mantener la disponibilidad de conocimiento relevante, actual, validado y fiable para dar soporte a todas las actividades de los procesos y facilitar la toma de decisiones. Planificar la identificación, recopilación, organización, mantenimiento, uso y retirada de conocimiento.
Meta del Proceso	**Métricas Relacionadas**
1. Las fuentes de información son identificadas y clasificadas.	• Porcentaje cubierto de categorías de información. • Volumen de información clasificado. • Porcentaje de información categorizada que ha sido validada.
2. El conocimiento es utilizado y compartido.	• Porcentaje de conocimiento disponible utilizado realmente. • Número de usuarios formados en el uso y compartición de conocimiento.
3. La compartición de conocimiento está integrada en la cultura de la empresa.	• Nivel de satisfacción de los usuarios. • Porcentaje del repositorio de conocimiento utilizado.
3. La compartición de conocimiento está integrada en la cultura de la empresa.	• Frecuencia de actualización.

Fuente. (ISACA, 2012)

Tabla 33

Descripción, metas y métricas del modelo propuesto. Proceso BAI09.

BAI09: Gestionar los Activos	**Descripción del proceso:** Gestionar los activos de TI a través de su ciclo de vida para asegurar que su uso aporta valor a un coste óptimo, que se mantendrán en funcionamiento (acorde a los objetivos), que están justificados y protegidos físicamente, y que los activos que son fundamentales para apoyar la capacidad del servicio son fiables y están disponibles. Administrar las licencias de software para asegurar que se adquiere el número óptimo, se mantienen y despliegan en relación con el uso necesario para el negocio y que el software instalado cumple con los acuerdos de licencia.
Meta del Proceso	**Métricas Relacionadas**
1. Las licencias cumplen y están alineadas con las necesidades del negocio. 2. Los activos se mantienen en condiciones óptimas.	• Porcentaje de licencias usadas respecto a licencias pagadas. • Número de activos no utilizados. • Comparativa de costes. • Número de activos obsoletos.

Fuente. (ISACA, 2012)

Tabla 34

Descripción, metas y métricas del modelo propuesto. Proceso BAI10.

BAI10: Gestionar la Configuración	**Descripción del proceso**: Definir y mantener las definiciones y relaciones entre los principales recursos y capacidades necesarios para la prestación de los servicios proporcionados por TI, incluyendo la recopilación de información de configuración, el establecimiento de líneas de referencia, la verificación y auditoría de la información de configuración y la actualización del repositorio de configuración.
Meta del Proceso	**Métricas Relacionadas**
1. El repositorio de configuración es correcto, completo y está actualizado.	• Número de desviaciones ente el repositorio de configuración y la configuración real. • Número de discrepancias relativas a información de configuración incompleta o inexistente.

Fuente. (ISACA, 2012)

Tabla 35

Descripción, metas y métricas del modelo propuesto. Proceso MEA01.

MEA01: Supervisar Evaluar, Valorar Rendimiento y la Conformidad	**Descripción del proceso**: Recolectar, validar y evaluar métricas y objetivos de negocio, de TI y de procesos. Supervisar que los procesos se están realizando acorde al rendimiento acordado y conforme a los objetivos y métricas y se proporcionan informes de forma sistemática y

Tabla 35. Continuación

	planificada.
Meta del Proceso	**Métricas Relacionadas**
1. Objetivos y métricas aprobadas por las partes interesadas.	• Porcentaje de informes de rendimiento entregados en plazo. • Porcentaje de objetivos y métricas aprobadas por las partes interesadas.
2. Procesos medidos acorde a las métricas y objetivos acordados.	• Porcentaje de procesos con objetivos y métricas definidas.
3. La monitorización, evaluación y generación de información es efectiva y operativa.	• Porcentaje de procesos con efectividad de objetivos y métricas revisadas y mejoradas. • Porcentaje de procesos críticos supervisados.
4. Objetivos y métricas integradas dentro de los sistemas de supervisión de la empresa.	• Porcentaje de objetivos y métricas alineadas al sistema de supervisión de la empresa.
5. Los informes acerca del rendimiento y conformidad de los procesos es útil y a tiempo.	• Porcentaje de informes de rendimiento entregados en plazo.

Fuente. (ISACA, 2012)

Tabla 36

Descripción, metas y métricas del modelo propuesto. Proceso MEA02

MEA02: Supervisar Evaluar, valorar el Sistema de Control Interno.	**Descripción del proceso**: Supervisar y evaluar de forma continua el entorno de control, incluyendo tanto autoevaluaciones como revisiones externas independientes. Facilitar a la Dirección la identificación de deficiencias e ineficiencias en el control y el inicio de acciones de mejora. Planificar, organizar y mantener normas para la evaluación del control interno y las actividades de aseguramiento.
Meta del Proceso	**Métricas Relacionadas**
1. Los procesos, recursos e información cumplen con los requisitos del sistema de control interno de la empresa.	• Porcentaje de procesos con la seguridad de que las salidas cumplen el objetivo dentro de los márgenes de tolerancia. • Porcentaje de procesos con la seguridad de que son conformes con las metas de control interno.
2. Todas las iniciativas de aseguramiento se planean y ejecutan de forma efectiva.	• Porcentaje de iniciativas de aseguramiento que siguen a programas de aseguramiento aprobados y los estándares de planificación
3. Se proporciona aseguramiento independiente de que el sistema de control interno es operativo y efectivo.	• Porcentaje de procesos bajo revisión independiente.
4. El control interno está establecido y las	• Número de debilidades identificadas en

Tabla 36. Continuación

deficiencias son identificadas y comunicadas.	los informes externos de certificación y cualificación. • Número de brechas mayores en el control interno. • Tiempo transcurrido entre la ocurrencia de la deficiencia del control interno y su comunicación.

Fuente. (ISACA, 2012)

Tabla 37

Descripción, metas y métricas del modelo propuesto. Proceso DSS01

MEA03: Supervisar Evaluar y Valorar la Conformidad con Requisitos Externos	**Descripción del proceso**: Evaluar el cumplimiento de requisitos regulatorios y contractuales tanto en los procesos de TI como en los procesos de negocio dependientes de las tecnologías de la información. Obtener garantías de que se han identificado, se cumple con los requisitos y se ha integrado el cumplimiento de TI en el cumplimiento de la empresa general.
Meta del Proceso	**Métricas Relacionadas**
1. La totalidad de los requisitos externos de cumplimiento se han identificado.	• Tiempo medio transcurrido entre la identificación de los problemas de incumplimiento y su resolución. • Frecuencia de revisiones de cumplimiento.
2. Tratar adecuadamente los requisitos externos de cumplimiento.	• Número anual de incidentes críticos por incumplimiento. • Porcentaje de propietarios de procesos que hayan confirmado por escrito el cumplimiento de requisitos externos.

Fuente. (ISACA, 2012)

Tabla 38

Descripción, metas y métricas del modelo propuesto. Proceso MEA0.

DSS01: Gestionar Operaciones	**Descripción del proceso**: Coordinar y ejecutar las actividades y los procedimientos operativos requeridos para entregar servicios de TI tanto internos como externalizados, incluyendo la ejecución de procedimientos operativos estándar predefinidos y las actividades de monitorización requeridas.
Meta del Proceso	**Métricas Relacionadas**
1. Las actividades operativas se realizan según lo requerido y programado.	• Número de procedimientos operativos no estándar ejecutados. • Número de incidentes causados por problemas operativos.

Tabla 38. Continuación

2. Las operaciones son monitorizadas, medidas, reportadas y remediadas.	• Tasa de eventos comparada con el número de incidentes. • Porcentaje de tipos de eventos operativos críticos cubiertos por sistemas de detección automática.

Fuente. (ISACA, 2012)

Tabla 39

Descripción, metas y métricas del modelo propuesto. Proceso DSS03

DSS02: Gestionar Peticiones e Incidente de servicio.	**Descripción del proceso**: Proveer una respuesta oportuna y efectiva a las peticiones de usuario y la resolución de todo tipo de incidentes. Recuperar el servicio normal; registrar y completar las peticiones de usuario; y registrar, investigar, diagnosticar, escalar y resolver incidentes.
Meta del Proceso	**Métricas Relacionadas**
1. Los servicios relacionados con TI están disponibles para ser utilizados.	• Número y porcentaje de incidentes que causan interrupción en los procesos críticos de negocio. • Tiempo promedio entre incidentes de acuerdo con el servicio facilitado por TI.
2. Los incidentes son resueltos según los niveles de servicio acordados.	• Porcentaje de incidentes resueltos dentro de un periodo acordado/aceptable.
3. Las peticiones de servicio son resueltas según los niveles de servicio acordados y la satisfacción del usuario.	• Nivel de satisfacción del usuario con la resolución de las peticiones de servicio. • Tiempo promedio transcurrido para el tratamiento de cada tipo de petición de servicio.

Fuente. (ISACA, 2012)

Tabla 40

Descripción, metas y métricas del modelo propuesto. Proceso DSS02

DSS03: Gestionar Problemas	**Descripción del proceso**: Identificar y clasificar problemas y sus causas raíz y proporcionar resolución en tiempo para prevenir incidentes recurrentes. Proporcionar recomendaciones de mejora.
Meta del Proceso	**Métricas Relacionadas**
1. Garantizar que los problemas relativos a TI son resueltos de forma que no vuelven a suceder.	• Descenso del número de incidentes recurrentes causados por problemas no resueltos. • Porcentaje de incidentes graves para los que se han registrado problemas. • Porcentaje de soluciones temporales definidos para problemas abiertos.

Tabla 40. Continuación

	• Porcentaje de problemas registrados como parte de una gestión de problemas proactiva. • Número de problemas para los que se ha encontrado una solución satisfactoria que apunta a causas raíz.

Fuente. (ISACA, 2012)

Tabla 41

Descripción, metas y métricas del modelo propuesto. Proceso DSS04

DSS04: Gestionar la continuidad	**Descripción del proceso**: Establecer y mantener un plan para permitir al negocio y a TI responder a incidentes e interrupciones de servicio para la operación continua de los procesos críticos para el negocio y los servicios TI requeridos y mantener la disponibilidad de la información a un nivel aceptable para la empresa.
Meta del Proceso	**Métricas Relacionadas**
1. La información crítica para el negocio está disponible para el negocio en línea con los niveles de servicio mínimos requeridos.	• Porcentaje de servicios TI que cumplen los requisitos de tiempos de funcionamiento. • Porcentaje de restauraciones satisfactorias y en tiempo de copias alternativas o de respaldo. • Porcentaje de medios de respaldo transferidos y almacenados de forma segura.
2. Los servicios críticos tienen suficiente resiliencia.	• Número de sistemas críticos para el negocio no cubiertos por el plan.
3. Las pruebas de continuidad del servicio han verificado la efectividad del plan.	• Número de ejercicios y pruebas que han conseguido los objetivos de recuperación. • Frecuencia de las pruebas.
4. Un plan de continuidad actualizado refleja los requisitos de negocio actuales.	• Porcentaje de mejoras acordadas que han sido reflejadas en el plan. • Porcentaje de asuntos identificados que se han incluido satisfactoriamente en el plan.
5. Las partes interesadas internas y externas han sido formadas en el plan de continuidad.	• Porcentaje de interesados internos y externos que han recibido formación. • Porcentaje de asuntos identificados que se han tratado subsecuentemente en los materiales de formación.

Fuente. (ISACA, 2012)

Tabla 42
Descripción, metas y métricas del modelo propuesto. Proceso DSS05

DSS05: Gestionar Servicios de Seguridad	**Descripción del proceso**: Proteger la información de la empresa para mantener aceptable el nivel de riesgo de seguridad de la información de acuerdo con la política de seguridad. Establecer y mantener los roles de seguridad y privilegios de acceso de la información y realizar la supervisión de la seguridad.
Meta del Proceso	**Métricas Relacionadas**
1. La seguridad de las redes y las comunicaciones cumple con las necesidades del negocio.	• Número de vulnerabilidades descubiertas • Número de rupturas (breaches) de cortafuegos.
2. La información procesada, almacenada y transmitida en los dispositivos de usuario final está protegida.	• Porcentaje de individuos que reciben formación de concienciación relativa al uso de dispositivos de usuario final. • Número de incidentes que impliquen dispositivos de usuario final. • Número de dispositivos de usuario final no autorizados detectados en la red o en el entorno.
3. Todos los usuarios están identificados de manera única y tienen derechos de acceso de acuerdo con sus roles en el negocio.	• Promedio de tiempo entre los cambios y actualizaciones de cuentas. • Número de cuentas (con respecto al número de usuarios/empleados autorizados).
4. Se han implantado medidas físicas para proteger la información de accesos no autorizados, daños e interferencias mientras es procesada, almacenada o transmitida.	• Porcentaje de pruebas periódicas de los dispositivos de seguridad del entorno. • Clasificación media para las evaluaciones de seguridad física. • Número de incidentes relacionados con seguridad física.
5. La información electrónica tiene las medidas de seguridad apropiadas mientras está almacenada, transmitida o destruida.	• Número de incidentes relacionados con accesos no autorizados a la información.

Fuente. (ISACA, 2012)

Tabla 43
Descripción, metas y métricas del modelo propuesto. Proceso DSS06

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

Tabla 43. Continuación

	requisitos de control de la información y gestionar y operar los controles adecuados para asegurar que la información y su procesamiento satisfacen estos requerimientos.
Meta del Proceso	**Métricas Relacionadas**
1. La cobertura y efectividad de los controles clave para cumplir con los requerimientos de negocio para el procesamiento de la información es completa.	• Porcentaje completado de inventario de procesos críticos y controles clave. • Porcentaje de controles clave cubiertos con los planes de pruebas. • Número de incidentes y evidencias del informe de auditoría indicando fallos de los controles clave.
2. El inventario de roles, responsabilidades y derechos de acceso está alineado con las necesidades autorizadas de negocio.	• Porcentaje de roles de proceso de negocio con derechos de acceso y niveles de autorización asignados. • Porcentaje de roles de proceso de negocio con una separación clara de tareas. • Número de incidentes y evidencias de auditoría debido a acceso o violación de segregación de funciones.
3. Las transacciones de negocio son retenidas completamente y según se requiera en registros	• Porcentaje de completitud de registros de transacciones rastreables. • Número de incidentes donde el historial de transacciones no pueda ser recuperado

Fuente. (ISACA, 2012)

4.6.5 Modelo de Madurez. El modelo de madurez a utilizar es el propuesto por el estándar internacional ISO/IEC 15504 – denominado Determinación de la Capacidad de Mejora del Proceso de Software (Software Process Improvement Capability Determination). El cual establece los criterios de evaluación a través de seis (6) niveles de capacidad.

Niveles de Capacidad

Nivel 0: Proceso Incompleto. En este nivel la organización no cuenta con una implementación efectiva de los procesos y carencia del logro de los objetivos.

Nivel 1: Proceso Realizado. En este nivel la organización cuenta con la existencia de procesos definidos, pero su cumplimiento se realiza cuando es necesario, estos carecen de planificación y seguimiento.

Nivel 2: Proceso gestionado. En este nivel la organización cuenta procesos implementados con productos evidenciables de acuerdo a la planificación. El proceso es supervisado y ajustado a estándares y especificaciones prestablecidas.

Nivel 3: Proceso establecido. En este nivel la organización cuenta con procesos con una implementación planificada, monitoreada y ajustada. Los cuales se realizan y gestionan de acuerdo al procedimiento documentado y estandarizado.

Nivel 4: Proceso predecible. En este nivel la organización cuenta con procesos establecidos, con métricas e indicadores que permiten conocer su capacidad y predecir el comportamiento.

Nivel 5: Proceso optimizado. En este nivel la organización cuenta con procesos predecibles con un mejoramiento continuo que contribuye al cumplimiento de los objetivos actuales y futuros del negocio.

Atributos del Proceso. ISO/IEC 15504-2, basa el nivel de capacidad de acuerdo a una serie de atributos de los procesos y cada uno de estos aplica un proceso de capacidad específico como se

ilustra en la figura 25. Los atributos permiten determinar si el proceso ha obtenido un nivel de capacidad concreta (ISACA, 2013).

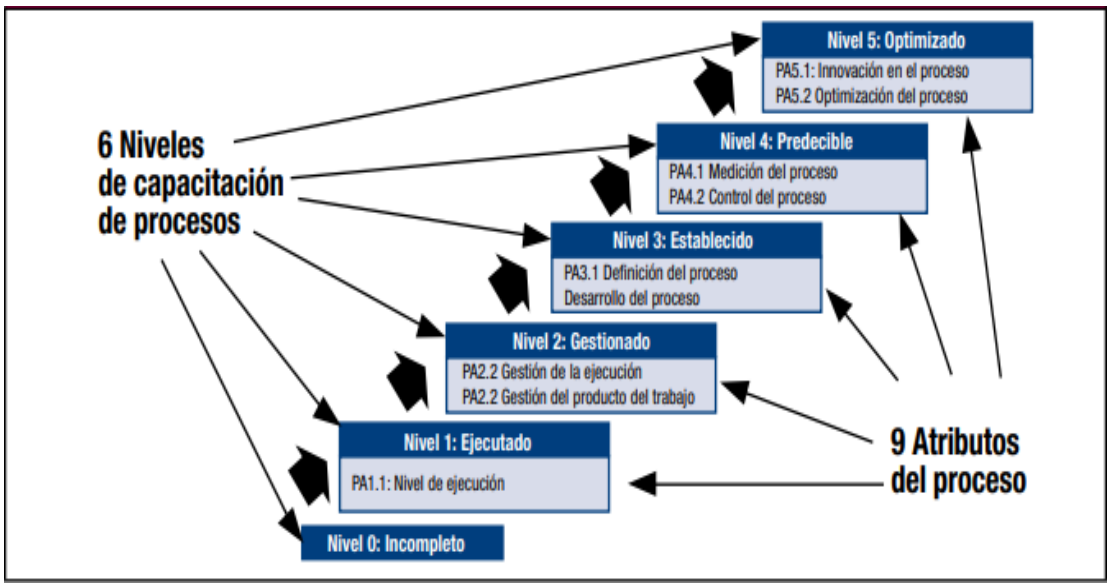

Figura 25. **(ISACA, 2013)**.
Fuente. Atributos de procesos de ISO/IEC 15504.

4.6.6 Plan de Implementación. La implementación del Modelo de Gobierno TI como apoyo al MSPI para las entidades del estado colombiano, inicia con la creación del entorno apropiado para la aplicación del modelo, lo cual permite que la iniciativa esté asegurada por parte los stakeholders.

La guía base de implementación para el modelo propuesto, es la planteada por el IT Governance Institute, ITgobernance implementation (Governance Institute); en la cual se establecen siete (7) fases:

Fase 1: Obtener el compromiso de la alta dirección. El objetivo de esta fase es obtener el aval y apoyo de la alta dirección de la organización para la implementación del Modelo de Gobierno TI como apoyo al MSPI. Así como difusión entre los stakeholders (Partes Interesadas).

Actividades:

- Presentación del modelo a la alta dirección de la organización
- Socialización del alcance del proyecto.
- Difusión a las partes interesadas.

Entregables:

- Documento de apoyo y compromiso en la implementación del modelo, firmado y aprobado por la alta dirección.

Fase 2: Determinar el estado actual. El objetivo de esta fase es identificar a través de un diagnóstico de capacidad las fortalezas, debilidades y riesgos de los procesos de TI, con respecto a sus requerimientos y su respectiva alineación con las necesidades de la organización.

Actividades:

- Aplicación del diagnóstico de evaluación de capacidad a los procesos de TI en la organización.
- Validar el resultado obtenido.
- Presentación de resultados del estado actual de TI en la organización.

Entregables:

- Análisis de resultados del estado de capacidad de los procesos de TI en la organización.

Fase 3. Establecer el estado futuro deseado. Determinar los requerimientos del proceso para lograr un nivel de capacidad optimizado, que permitan satisfacer los objetivos actuales y proyectados del negocio.

Actividades:

- Analizar los requerimientos del estado de capacidad del nivel optimizado para los procesos de TI en la organización.

Entregables:

- Caracterización del nivel de capacidad de TI optimizado en la organización.

Fase 4. Identificar las brechas. De acuerdo con el diagnóstico realizado en las dos fases anteriores, a través de las cuales se obtiene el nivel de capacidad actual y el deseado para los procesos de TI en la organización, se realiza la identificación de brechas a cerrar para dar continuidad a la implementación del modelo.

Actividades:

- Identificación de las brechas existentes entre el estado de capacidad actual y el deseado.
- Identificación de posibles causas, amenazas, riesgos y restricción que dificultarían el cierre de las brechas en mención.

- Identificar fortalezas, oportunidades de mejora y beneficios que facilitarían el cierre de las brechas.

Entregables:

- Documentación de las brechas existentes.
- Documento con las acciones requeridas para el cierre de las brechas.

Fase 5. Definir el plan de Implementación. El objetivo de esta fase es determinar el plan o programa de implementación a seguir para el logro de los objetivos propuestos.

Actividades:

- Determinar de acuerdo a las brechas detectadas, cuáles de estas serán cerradas y cuales por el alcance de sus requerimientos solo quedarán planteadas para su implementación en un futuro.
- Identificar en el modelo propuesto cuales son los controles necesarios para el cierre de las brechas propuestas para obtener el logro de los objetivos.
- Definir las actividades de control como proyectos, y establecer para cada uno de estos los responsables, metas, recursos y cronograma.
- Establecer el orden de ejecución de cada uno de los proyectos.

Actividades:

- Documento con las brechas a cerrar y las que quedaran planteadas.
- Actividades de control requeridas para el cumplimiento de los objetivos propuestos.
- Documentación de los proyectos a implementar, responsables, recursos y metas entre otros.
- Cronograma de implementación.

Fase 6. Desarrollar el Plan de Implementación. En esta fase de inicia el desarrollo de implementación establecido en la fase anterior.

Actividades:

- Desarrollo de cada proyecto, de acuerdo al orden establecido en la fase cinco (5).
- Gestión del talento humano, recursos físicos y financieros, requeridos para llevar a cabo la implementación de cada uno de los proyectos.
- Realizar las actividades requeridas en cada uno de los proyectos para dar cumplimiento al cronograma en el tiempo establecido.
- Realizar las pruebas de cumplimento a la finalización de cada proyecto para realizar el cierre respectivo del mismo.
- Socializar con las partes interesadas el cierre del proyecto.

Entregables:

- Lista de requerimiento de recursos para la ejecución de cada uno de los proyectos.

- Documentación de las pruebas realizadas y los resultados obtenidos a cada una de las actividades implementadas.
- Documento de conformidad del cierre formal del proyecto, con la aprobación de sus responsables.

Fase 7. Monitorear y controlar el desempeño de la implementación. Establecer un programa de revisión periódica a cada uno de los proyectos, que permita la validación de cumplimiento de los objetivos propuestos.

Actividades:

- Establecer mecanismos que permitan realizar la validación de los proyectos implementados y cumplimiento de los objetivos propuestos.
- Definir responsables para el monitoreo de cada uno de los proyectos implementados.
- Realizar el reporte de monitoreo a los responsables, para la toma de decisiones de acuerdo a los resultados obtenidos.

Entregables:

- Documentación de los procesos de validación y monitoreo del cumplimiento de los objetivos de los proyectos implementados.
- Informe con los resultados obtenidos en el monitoreo.

4.7 Validación de la propuesta

4.7.1 Metodología de Validación. Para validar la coherencia y la efectividad de la propuesta del modelo de gobernanza de TI para las entidades del estado, como apoyo al cumplimiento del componente de Seguridad y Privacidad de la Información en el marco de la Política de Gobierno Digital, se fundamentará en la opinión de una muestra de "Expertos".

Siguiendo los criterios del grupo de autores que han aplicado el método Delphi en sus investigaciones (Reguant-Álvarez & Torrado-Fonseca, 2016) y (Rodriguez Garcia & Garcia, 2017), se estableció la secuencia metodológica a seguir, compuesta de tres fases fundamentales: Preparatoria, consulta y consenso.

Fase Preparatoria

Selección de expertos. De acuerdo con el objetivo de la investigación, el método a desarrollar el Delfhi, que en concordancia con los referentes teóricos de (Oñate, Ramos y Díaz, 1998; Bravo y Arrieta, 2005; Cruz, 2006; Blasco y López, 2010), la muestra se conforma por un grupo coordinador y un grupo de expertos.

El grupo coordinador se conformó a partir del Director del proyecto a evaluar, Doctor en Ingenieria de Seguridad de la Información y Master en Seguridad Informática y la directora de la Maestría de Gobierno de TI de la Universidad Francisco de Paula Santander – UFPSO. Seleccionados de acuerdo con las características establecidas para este grupo por Calabuig y Crespo (2009) en su investigación, donde los integrantes deben cumplir con competencias como:

investigadores académicos, docentes, profesionales con experiencia relacionada con el tema a valorar y gran facilidad de intercomunicación al trabajar conjuntamente en otros estudios.

El grupo de coordinación realiza la selección del grupo de expertos, en concordancia con los criterios de selección expuestos por Landeta (1999), indica que se requiere de un mínimo de siete expertos, un máximo de 30. Okoli y Pawlowski (2004), opinan que en la literatura se recomienda entre 10 y 18, para lo cual Yáñez y Cuadra (2008), señalan que este rango del número de expertos es razonable.

Como criterio fundamental para realizar la selección del panel de expertos se seleccionó un grupo de profesionales con alguno de los siguientes perfiles:

- Experiencia en el área de Implementación de MSPI den entidades del estado colombiano.
- Docencia en Gobierno de TI
- Estudios superiores de postgrado en áreas relacionadas o afines al Gobierno de TI.
- Experiencia Profesional relacionada a Gobierno TI, Seguridad, Control Interno y Auditoria TI.

Preparación del instrumento: Se realizan dos cuestionarios. El primer formulario permite determinar los posibles candidatos a expertos seleccionados de acuerdo al perfil establecido, asi como tambien conocer su disposición a participar. El segundo forulario la valoración del modelo propuesto.

Decisión de la vía de consulta: Se realiza por medio correo electronico.

Fase de consulta. Se realiza la primera versión del cuestionario y se sometió a valoración por parte del grupo coordinador de expertos, se realizan las acotaciones necesarias al formulario en una segunda ronda, y se realiza la validación por el grupo de expertos seleccionados con la finalidad de obtener los criterios cuantitativos.

El envío y la recepción del formulario se realizó por correo electrónico en el cual se anexa un resumen ejecutivo del proyecto y el instrumento para su valoración.

4.7.2 Resultados de Validación a Expertos. El formulario N° 1, se envió el 9 de agosto con fecha límite de respuesta hasta el 30 de agosto de 2019. El formulario N° 2, se envió el 22 de septiembre con fecha límite de respuesta hasta el 10 de octubre de 2019.

Tamaño de la muestra. El formulario N° 1, inicialmente se envió a un total de treinta y cuatro (34) enlaces de Gobierno Digital para el Departamento de Norte de santander, de los cuales solo se recibio respuesta de dos (2) encuestados, quienes manifestaron formalmente no tener actualmente ningún vínculo con las alcaldía relacionada. Ante esta negativa se procedió a expandir la muestra un grupo de nueve (9) profesionales que hacen parte de entidades del orden nacional como: MinTIC, Alcaldías, Ejercito Nacional y Docentes de Universidaes, expertos en areas como seguridad de la Informacion, privacidad de la Informacion, Sistemas de Gestion de Seguridad de la Informacion, Gobierno de tenologias de la Informacion y adicional a ello cuenta con experfiencia en la adopcion del MSPI .

Contenido del Cuestionario. Las preguntas del formulario N°1, esta relacioanda con datos demógraficos, formación academica, areas de experiencia profesional, participación en

fases de implementación o auditoria del MSPI, cargo y entidad para la cual presta sus servicios profesionales. Adicional se consulta sobre una auto valoración del grado de conocimiento sobre el tema, asi como el grado de influencia de fuentes relacionadas (Ver Anexo 3). Estas preguntas permiten realizar la valoración del coeficiente de competencia de cada uno de los candidatos a expertos.

Determinación del coeficiente de competencia de los experto. De los posibles nueve (9) expertos seleccionados a consultar, siete (7) dieron respuesta, y aunque en la literatura no se encuetra definido un número para el desarrollo de la validación por el metodo de Delphi, Landeta (2002) por su parte indica que con un minimo de siete (7) expertos se puede determinar la factibilidad del proyecto.

Para establecer la variable en mención se pidió que valoraran el grado de conocimiero en el area del proyecto, marcando con una "X", en una escala de 1 a 10, de manera creciente. Los resultados obtenidos en este item son los siguientes:

Tabla *44*
Autovaloración de expertos

Experto	Grado de Conocimiento									
	1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**
EXP 1								X		
EXP 2									X	
EXP 3										X
EXP 4										X
EXP 5										X
EXP 6									X	
EXP 7									X	

Fuente. Autor del proyecto

Apartir del coeficiente de competencia de expertos, se procede a realizar el calculo de la variable del coeficiente de conocimiento o información kc, donde la valoración dada por el experto en la escala de 0 a 10 se multiplica por 0,1.

Tabla *45*
Coeficiente de Conocimiento o información kc

Experto	Grado de Conocimiento	kc
EXP 1	8	0.8
EXP 2	9	0.9
EXP 3	10	1
EXP 4	10	1
EXP 5	10	1
EXP 6	9	0.9
EXP 7	9	0.9

Fuente. Autor del proyecto

Posteriormente se procede con la evaluación del coeficiente de argumentación de los criterios del experto, el cual se obtiene como resultado de puntos a partir de la tabla patrón relacionada a continuación.

Tabla *46*
Grado de influencia en cada fuente

Experto	Grado de Conocimiento	Grado de Influencia en cada Fuente					
		F1	F2	F3	F4	F5	F6
EXP 1	8	M	A	A	M	A	A
EXP 2	9	M	M	A	B	B	A
EXP 3	10	A	A	A	A	A	A
EXP 4	10	A	A	A	A	A	A
EXP 5	10	A	A	M	A	A	A
EXP 6	9	A	M	A	A	M	A
EXP 7	9	A	M	A	A	A	A

Fuente. Autor del proyecto, con base en (Rodríguez García & García, 2017).

Para realizar el calculo del coeficiente de argumentación se realiza a partir de la siguiete tabla patron.

Tabla *47*
Patrón para el coeficiente de Argumentación del experto

FUENTES DE ARGUMENTACIÓN	Alto	Medio	Bajo
Análisis teórico realizado por usted	0,3	0,2	0,1
Su experiencia obtenida	0,5	0,4	0,2
Trabajo de autores nacionales	0,05	0,05	0,05
Trabajos de autores extranjeros	0,05	0,05	0,05
Su propio conocimiento del estado del problema en el extranjero	0,05	0,05	0,05
Su intuición	0,05	0,05	0,05

Fuente. Autor del proyecto, con base en (Rodríguez García & García, 2017).

Apartir de la tabla patrón y la autovaloración realizada por cada una de los expertos, se realiza el calculo coeficiente de argumentación ka.

Tabla *48 Coeficiente de argumentación*

Experto	Grado de Influencia en cada Fuente						ka
	F1	F2	F3	F4	F5	F6	
EXP 1	0.2	0.5	0.05	0.05	0.05	0.05	0.9
EXP 2	0.2	0.4	0.05	0.05	0.05	0.05	0.8
EXP 3	0.3	0.5	0.05	0.05	0.05	0.05	1
EXP 4	0.3	0.5	0.05	0.05	0.05	0.05	1
EXP 5	0.3	0.5	0.05	0.05	0.05	0.05	1
EXP 6	0.3	0.4	0.05	0.05	0.05	0.05	0.9
EXP 7	0.3	0.4	0.05	0.05	0.05	0.05	0.9

Fuente. Autor del proyecto

Tabla *49 Coeficiente de competencia K*

Experto	Kc	Grado de Influencia en cada Fuente						ka	K
		F1	F2	F3	F4	F5	F6		
EXP 1	0.8	0.2	0.5	0.05	0.05	0.05	0.05	0.9	0.85
EXP 2	0.9	0.2	0.4	0.05	0.05	0.05	0.05	0.8	0.85
EXP 3	1	0.3	0.5	0.05	0.05	0.05	0.05	1	1
EXP 4	1	0.3	0.5	0.05	0.05	0.05	0.05	1	1
EXP 5	1	0.3	0.5	0.05	0.05	0.05	0.05	1	1
EXP 6	0.9	0.3	0.4	0.05	0.05	0.05	0.05	0.9	0.9
EXP 7	0.9	0.3	0.4	0.05	0.05	0.05	0.05	0.9	0.9

Fuente. Autor del proyecto

El código de interpretación para el coeficiente de competencias es:

Si $0.8 < K < 1$, coeficiente de competencia del experto alto.

Si $0.5 < K < 0{,}8$, coeficiente de competencia del experto medio

Si $K < 0.5$, coeficiente de competencia del experto bajo.

De acuerdo con los resultados obtenidos en la variable K, evidenciados en la tabla 49, permite determinar que el nivel del coeficiente de competencia de los expertos seleccionados es Alto.

Valoración de expertos para la propuesta. De acuerdo con la validación del coeficiente de competencia de los candiatos, se seleccionarón los siete expertos y se procede a realizar el formulario N° 2, el cual esta compuesto por 11 preguntas con respuesta de selección unica, que permiten medir el grado de factibilidad de modelo. Adicional se establecen dos preguntas con respuesta abierta, relacionada una, a las fases y/o componentes que el experto considera que deben ser incluidos o eliminados de la propuesta y una seguna pregunta, si considera que el nombre de alguno de los ítems de la propuesta, debe ser cambiado.

Descripción del contenido de las preguntas del formulario N° 2. El formulario inicia con un capitulo de identificación del experto, cuyas respuestas son opcionales por razones de confidencialidad. Sólo se describen a quienes autorizarón que su nonbre figure en la tesis. Acontinuación en la tabla 50 se relacionan los nombres y entidades donde prestan servicios profesionales los expertos que autorizaron que sus datos aparecieran en la tesis. En la tabla 51 el cargo, nivel educativo, experiencia en el area asi como en investigación.

Tabla *50*
Identificación de Expertos

Ref	Nombre y Apellidos	Entidad
EXP 1	María del Pilar Niño Campo	Alcaldía Mayor de Bogotá
EXP 2	Yesica Tatiana Vanegas	Alcaldía de Neiva
EXP 3	Andres Días Molina	MINTIC
EXP 4	Senén Niño Gil	MINTIC
EXP 5	Erika Tatiana Quintero Quintero	MINTIC
EXP 6		
EXP 7	Torcoroma Velazques Pérez	UFPSO

Fuente. Autor del proyecto

Tabla *51*
Identificación de Expertos - Experiencia

Ref	Cargo	Nivel Educativo	Experiencia en el área (años)	Experiencia en la docencia y/o en la investigación (años)
EXP 1	Profesional Especializado	Magister	5	1
EXP 2	Ingeniero de Sistemas	Profesional	4	0
EXP 3	Asesor – CISO	Especialista	11	3
EXP 4	Consultor en Seguridad de la Información	Especialista	8	0

Tabla 51. Continuación

EXP 5	Contratista de seguridad de la Información	Magister	9	0
EXP 6	Investigador	Magister	10	5
EXP 7	Directora Maestria GTI	Doctor	3	20

Fuente. Autor del proyecto

El contenido de las preguntas se encuentra descriptas en la table 47 y las opciones de respuesta son las siguientes:

- MR: Muy relevante
- BR: Bastante relevante
- R: Relevante
- PR: Poco relevante
- ND: Nada relevante

Tabla *52*
Frecuencia Absoluta

Pregunta	MR	BR	R	PR	NR	TOTAL
1. ¿Considera relevante la aseveración de que el gobierno de TI integra e institucionaliza las buenas prácticas para garantizar que la TI en las entidades públicas soporten los objetivos del negocio?	5	2	0	0	0	7
2. ¿Considera que la adopción de un modelo de Gobernanza de TI para las entidades del estado, mejora la eficacia de la implementación del modelo de seguridad y privacidad de la información propuesto dentro del marco de la estrategia de Gobierno Digital?.	5	1	1	0	0	8

Tabla 52. Continuación

3. ¿Considera que el patrón de gobierno de TI diseñado, se adapta al Modelo de Seguridad y Privacidad de la Información (MSPI) de MinTIC en Colombia?	0	6	1	0	0	7
4. ¿Comparte la idea de que las características particulares consideradas en el modelo de Gobernanza de TI; les facilita a las entidades del estado colombiano cumplir con la implementación y gestión del Programa de Seguridad y Privacidad de la Información propuesto por MINTIC y mejorar la eficacia en su adopción?	3	3	1	0	0	7
5. ¿Considera que la Propuesta de Modelo de Gobernanza de TI para las entidades del estado, como apoyo al cumplimiento del componente de Seguridad y Privacidad de la Información, puede añadir valor y si se sigue e implementa facilita a las entidades del estado colombiano el cumplimiento del Decreto 1008 de 2018?	2	4	1	0	0	7
6. ¿Considera que el modelo propuesto, posee los elementos estructurales (Dominios, niveles, metas de TI y fases del MSPI) de un modelo de gobierno de TI?	4	2	1	0	0	7
7. ¿Existe coherencia entre los elementos estructurales (Dominios, niveles, metas de TI y fases del MSPI) del modelo propuesto?	4	3	0	0	0	7
8. ¿Hay correspondencia entre el modelo diseñado y la definición de un modelo de Gobernanza de TI?	2	5	0	0	0	7
9. Existe claridad en el contenido de cada elemento del modelo.	4	3	0	0	0	7
10. ¿Existe correspondencia entre los elementos estructurales del modelo, sus objetivos y sus características?	5	2	0	0	0	7
11. ¿Considera que la adopción del modelo de Gobernanza propuesto, facilita la dirección y el control del Sistema de Gestión de Seguridad de la Información MSPI?	1	5	0	1	0	7

Fuente. Autor del proyecto, con base en (Rodríguez García & García, 2017).

Tabla *53*
Frecuencia Absoluta Acumulada

Pregunta	MR	BR	R	PR	NR	TOTAL
1. ¿Considera relevante la aseveración de que el gobierno de TI integra e institucionaliza las buenas prácticas para garantizar que la TI en las entidades públicas soporten los objetivos del negocio?	5	7	7	7	7	33
2. ¿Considera que la adopción de un modelo de Gobernanza de TI para las entidades del estado, mejora la eficacia de la implementación del modelo de seguridad y privacidad de la información propuesto dentro del marco de la estrategia de Gobierno Digital?.	5	6	7	7	7	32
3. ¿Considera que el patrón de gobierno de TI diseñado, se adapta al Modelo de Seguridad y Privacidad de la Información (MSPI) de MinTIC en Colombia?	0	6	7	7	7	27
4. ¿Comparte la idea de que las características particulares consideradas en el modelo de Gobernanza de TI; les facilita a las entidades del estado colombiano cumplir con la implementación y gestión del Programa de Seguridad y Privacidad de la Información propuesto por MINTIC y mejorar la eficacia en su adopción?	3	6	7	7	7	30
5. ¿Considera que la Propuesta de Modelo de Gobernanza de TI para las entidades del estado, como apoyo al cumplimiento del componente de Seguridad y Privacidad de la Información, puede añadir valor y si se sigue e implementa facilita a las entidades del estado colombiano el cumplimiento del Decreto 1008 de 2018?	2	6	7	7	7	29
6. ¿Considera que el modelo propuesto, posee los elementos estructurales (Dominios, niveles, metas de TI y fases del MSPI) de un modelo de gobierno de TI?	4	6	7	7	7	31
7. ¿Existe coherencia entre los elementos estructurales (Dominios, niveles, metas de TI y fases del MSPI) del modelo propuesto?	4	7	7	7	7	32

Tabla 53. Continuación

8. ¿Hay correspondencia entre el modelo diseñado y la definición de un modelo de Gobernanza de TI?	2	7	7	7	7	30
9. Existe claridad en el contenido de cada elemento del modelo.	4	7	7	7	7	32
10. ¿Existe correspondencia entre los elementos estructurales del modelo, sus objetivos y sus características?	5	7	7	7	7	33
11. ¿Considera que la adopción del modelo de Gobernanza propuesto, facilita la dirección y el control del Sistema de Gestión de Seguridad de la Información MSPI?	1	6	6	7	7	27

Fuente. Autor del proyecto, con base en (Rodríguez García & García, 2017).

Tabla *54*

Frecuencia Relativa Acumulada

Pregunta	MR	BR	R	PR	NR
1. ¿Considera relevante la aseveración de que el gobierno de TI integra e institucionaliza las buenas prácticas para garantizar que la TI en las entidades públicas soporten los objetivos del negocio?	0,714285714	1	1	1	1
2. ¿Considera que la adopción de un modelo de Gobernanza de TI para las entidades del estado, mejora la eficacia de la implementación del modelo de seguridad y privacidad de la información propuesto dentro del marco de la estrategia de Gobierno Digital?.	0,714285714	0,8571429	1	1	1
3. ¿Considera que el patrón de gobierno de TI diseñado, se adapta al Modelo de Seguridad y Privacidad de la Información (MSPI) de MinTIC en Colombia?	0	0,8571429	1	1	1
4. ¿Comparte la idea de que las características particulares consideradas en el modelo de Gobernanza de TI; les facilita a las entidades del estado colombiano cumplir con la implementación y gestión del Programa de Seguridad y Privacidad de la Información propuesto por MINTIC y mejorar la eficacia en su adopción?	0,428571429	0,8571429	1	1	1

Tabla 54. Continuación

5. ¿Considera que la Propuesta de Modelo de Gobernanza de TI para las entidades del estado, como apoyo al cumplimiento del componente de Seguridad y Privacidad de la Información, puede añadir valor y si se sigue e implementa facilita a las entidades del estado colombiano el cumplimiento del Decreto 1008 de 2018?	0,285714286	0,8571429	1	1	1
6. ¿Considera que el modelo propuesto, posee los elementos estructurales (Dominios, niveles, metas de TI y fases del MSPI) de un modelo de gobierno de TI?	0,571428571	0,8571429	1	1	1
7. ¿Existe coherencia entre los elementos estructurales (Dominios, niveles, metas de TI y fases del MSPI) del modelo propuesto?	0,571428571	1	1	1	1
8. ¿Hay correspondencia entre el modelo diseñado y la definición de un modelo de Gobernanza de TI?	0,285714286	1	1	1	1
9. Existe claridad en el contenido de cada elemento del modelo.	0,571428571	1	1	1	1
10. ¿Existe correspondencia entre los elementos estructurales del modelo, sus objetivos y sus características?	0,714285714	1	1	1	1
11. ¿Considera que la adopción del modelo de Gobernanza propuesto, facilita la dirección y el control del Sistema de Gestión de Seguridad de la Información MSPI?	0,142857143	0,8571429	0,8571429	1	1

Fuente. Autor del proyecto, con base en (Rodríguez García & García, 2017).

Despues de realizar la construcción de la tabla de frecuencias relativas, se procede a buscar la imagen de cada uno de los valores, por la inversa de la curva normal. De igual manera se optiene los puntos de corte, los cuales dan como resultado al dividir la suma de cada una de las columnas entre su promedio como se videncia en la siguiente tabla 55.

Tabla

55 Imagen de las frecuencias acumulativas relativas

Pregunta	MR	BR	R	PR	Suma	Promedio	N-P
1. ¿Considera relevante la aseveración de que el gobierno de TI integra e institucionaliza las buenas prácticas para garantizar que la TI en las entidades públicas soporten los objetivos del negocio?	0.57	3.5	3.5	3.5	11.07	2.7675	-0.6348
2. ¿Considera que la adopción de un modelo de Gobernanza de TI para las entidades del estado, mejora la eficacia de la implementación del modelo de seguridad y privacidad de la información propuesto dentro del marco de la estrategia de Gobierno Digital?.	0.57	1.07	3.5	3.5	8.64	2.16	-0.0273
3. ¿Considera que el patrón de gobierno de TI diseñado, se adapta al Modelo de Seguridad y Privacidad de la Información (MSPI) de MinTIC en Colombia?	-3.5	1.07	3.5	3.5	4.57	1.1425	0.9902
4. ¿Comparte la idea de que las características particulares consideradas en el modelo de Gobernanza de TI; les facilita a las entidades del estado colombiano cumplir con la implementación y gestión del Programa de Seguridad y Privacidad de la Información propuesto por MINTIC y mejorar la eficacia en su adopción?	-1.19	1.07	3.5	3.5	6.88	1.72	0.4127
5. ¿Considera que la Propuesta de Modelo de Gobernanza de TI para las entidades del estado, como apoyo al cumplimiento del componente de Seguridad y Privacidad de la Información, puede añadir valor y si se sigue e implementa facilita a las entidades del estado colombiano el cumplimiento del Decreto 1008 de 2018?	-0.57	1.07	3.5	3.5	7.5	1.875	0.2577

Tabla 54. Continuación

6. ¿Considera que el modelo propuesto, posee los elementos estructurales (Dominios, niveles, metas de TI y fases del MSPI) de un modelo de gobierno de TI.	0.18	1.07	3.5	3.5	8.25	2.0625	0.0702
7. ¿Existe coherencia entre los elementos estructurales (Dominios, niveles, metas de TI y fases del MSPI) del modelo propuesto?	0.18	3.5	3.5	3.5	10.68	2.67	-0.5373
8. ¿Hay correspondencia entre el modelo diseñado y la definición de un modelo de Gobernanza de TI?.	-0.57	3.5	3.5	3.5	9.93	2.4825	-0.3498
9. Existe claridad en el contenido de cada elemento del modelo.	0.18	3.5	3.5	3.5	10.68	2.67	-0.5373
10. ¿Existe correspondencia entre los elementos estructurales del modelo, sus objetivos y sus características?	0.57	3.5	3.5	3.5	11.07	2.7675	-0.6348
11. ¿Considera que la adopción del modelo de Gobernanza propuesto, facilita la dirección y el control del Sistema de Gestión de Seguridad de la Información MSPI?	-1.07	1.07	1.07	3.5	4.57	1.1425	0.9902
Suma	-4.65	23.92	36.07	38.5	93.84	23.46	
PUNTOS DE CORTE(Promedio Columna)	-0.4227	2.1745	3.2791	3.5		N (PROMEDIO GENERAL)	

Fuente. Autor del proyecto, con base en (Rodríguez García & García, 2017).

La variable N es el resultado de la división la sumatoria de las sumas entre el producto de la cantidad de pasos (número de preguntas) por la cantidad de categoria (número de respuestas):

N= 93.84/11*4= 2.1327

P= Valor promedio

N-P: Promedio otorgado por los expertos a cada pregunta.

Interpretación de resultados. Los puntos de corte permiten establecer la categoria o grado de adecación de cada uno de los interrogantes, de acuerdo a la opinión del grupo de expertos. Ver tabla 57.

Tabla *56*
Grado de categoría o adecuación de cada pregunta

MR	BR	R	PR	NR
-0.4227	2.1745	3.2791	3.5	

Fuente. Propia, con base en (Rodríguez García & García, 2017).

Tabla *57*
Análisis de resultados

Pregunta	MR	BR	R	PR
1. ¿Considera relevante la aseveración de que el gobierno de TI integra e institucionaliza las buenas prácticas para garantizar que la TI en las entidades públicas soporten los objetivos del negocio?	X			
2. ¿Considera que la adopción de un modelo de Gobernanza de TI para las entidades del estado, mejora la eficacia de la implementación del modelo de seguridad y privacidad de la información propuesto dentro del marco de la estrategia de Gobierno Digital?.		X		
3. ¿Considera que el patrón de gobierno de TI diseñado, se adapta al Modelo de Seguridad y Privacidad de la Información (MSPI) de MinTIC en Colombia?		X		
4. ¿Comparte la idea de que las características particulares consideradas en el modelo de Gobernanza de TI; les facilita a las entidades del estado colombiano cumplir con la implementación y gestión del Programa de Seguridad y Privacidad de la Información propuesto por MINTIC y mejorar la eficacia en su adopción?		X		
5. ¿Considera que la Propuesta de Modelo de Gobernanza de TI para las entidades del estado, como apoyo al cumplimiento del componente de Seguridad y Privacidad de la Información, puede añadir valor y si se sigue e implementa facilita a las entidades del estado colombiano el cumplimiento del Decreto 1008 de 2018?		X		

Tabla 57. Continuación

6. ¿Considera que el modelo propuesto, posee los elementos estructurales (Dominios, niveles, metas de TI y fases del MSPI) de un modelo de gobierno de TI?.		X
7. ¿Existe coherencia entre los elementos estructurales (Dominios, niveles, metas de TI y fases del MSPI) del modelo propuesto?	X	
8. ¿Hay correspondencia entre el modelo diseñado y la definición de un modelo de Gobernanza de TI?.		X
9. Existe claridad en el contenido de cada elemento del modelo.	X	
10. ¿Existe correspondencia entre los elementos estructurales del modelo, sus objetivos y sus características?	X	
11. ¿Considera que la adopción del modelo de Gobernanza propuesto, facilita la dirección y el control del Sistema de Gestión de Seguridad de la Información MSPI?		X

Fuente. Autor del proyecto, con base en (Rodríguez García & García, 2017).

Como se puede observar en la tabla 5, en el analisis de resultados, el grupo de expertos coinciden en señalar, como muy relevante, aspectos del modelo propuesto como:

- La aseveración de que el gobierno de TI integra e institucionaliza las buenas prácticas para garantizar que la TI en las entidades públicas soporten los objetivos del negocio.
- La existencia coherencia entre los elementos estructurales (Dominios, niveles, metas de TI y fases del MSPI) del modelo propuesto.
- La existencia de claridad en el contenido de cada elemento del modelo.
- La existencia de correspondencia entre los elementos estructurales del modelo, sus objetivos y sus características.

Asi como tambien coinciden en señalar como bastante relevante, considerar que:

- La adopción de un modelo de Gobernanza de TI para las entidades del estado, mejora la eficacia de la implementación del modelo de seguridad y privacidad de la información propuesto dentro del marco de la estrategia de Gobierno Digital.
- El patrón de gobierno de TI diseñado, se adapta al Modelo de Seguridad y Privacidad de la Información (MSPI) de MinTIC en Colombia. Así como también comparte la idea de que las características particulares consideradas en el modelo de Gobernanza de TI; les facilita a las entidades del estado colombiano cumplir con la implementación y gestión del Programa de Seguridad y Privacidad de la Información propuesto por MINTIC y mejorar la eficacia en su adopción.
- La Propuesta de Modelo de Gobernanza de TI para las entidades del estado, como apoyo al cumplimiento del componente de Seguridad y Privacidad de la Información, puede añadir valor y si se sigue e implementa facilita a las entidades del estado colombiano el cumplimiento del Decreto 1008 de 2018.
- El modelo propuesto, posee los elementos estructurales (Dominios, niveles, metas de TI y fases del MSPI) de un modelo de gobierno de TI.
- La existencia de correspondencia entre el modelo diseñado y la definición de un modelo de Gobernanza de TI.
- La adopción del modelo de Gobernanza propuesto, facilita la dirección y el control del Sistema de Gestión de Seguridad de la Información MSPI.

Los resulados descriptos en la tabla en la tabla 57, permiten deducir que el modelo de gobernanza de TI propuesto para las entidades del estado, como apoyo al cumplimiento del componente de Seguridad y Privacidad de la Información en el marco de la Política de Gobierno Digital, es bastante relevante para el 63.64 % de las consideraciones valoradas y el 36.36% restante como muy relevante, sin encontrarse ningún aspecto con valoración relevante, poco o nada relevante.

Capítulo 5. Conclusiones y trabajo futuro

El resultado de esta investigación propone un Modelo de Gobernanza de TI dirigido a las entidades del estado Colombiano que tiene como objetivo apoyar el cumplimiento del componente de Seguridad y Privacidad de la información definido dentro de la política de gobierno digital, facilitando no solo la adopción del MSPI, sino también la evaluación, dirección y monitorización del nuevo Sistema de Gestión de Seguridad de la Información y su componente de Privacidad, alineando las tecnologías de la información con los objetivos de la entidad facilitando el cumplimiento de los lineamientos del estado a la vez que genera valor.

El diseño del Modelo de Gobierno propuesto requirió de una revisión del estado del arte de los diferentes modelos de Gobierno de TI existentes y del Modelo de Seguridad y Privacidad propuesto por el estado Colombiano, junto con una investigación referente al estado actual de adopción del MSPI por parte de los entes territoriales de nuestra Nación.

Como resultado pudo evidenciarse que debido al desconocimiento, falta de formación en cuanto a la gestión de la seguridad de la información muy pocas entidades del estado Colombiano en el departamento Norte de Santander tienen adelantada la adopción del MSPI, exponiéndose al incumplimiento de las políticas de Gobierno digital definidas en el decreto 1008 del 14 de Junio del 2018.

La validez del Modelo propuesto fue fundamentada en la opinión de un conjunto de expertos en seguridad de la Información, privacidad de la Información, Sistemas de Gestión de Seguridad de la Información, Gobierno de tecnologías de la Información y que además conocen

muy bien y cuentan con experiencia como consultores y líderes de proyecto en la adopción del MSPI exigido por el Gobierno Colombiano. A quienes se les socializo el Modelo de Gobierno propuesto y se les envió una copia documental del mismo para su revisión.

Contribuciones del proyecto. Este proyecto de investigación muestra una revisión completa del Modelo de Seguridad y privacidad de la Información incluyendo los entregables esperados por el estado, como también del requerimiento necesarios para la Adopción del MSPI.

Otra contribución relevante de esta propuesta, es el diseño de un novedoso Modelo en el que se alinean las fases del MSPI, con los lineamientos requeridos para implementar el Gobierno de Tecnologías de la información orientado principalmente a facilitar la dirección y el control, garantizando el cumplimiento de las políticas de Gobierno Digital encaminadas a la implementación de un Sistema de Gestión de Seguridad y Privacidad de la información.

Líneas de trabajo futuro. A medida que se realizaba el proyecto de investigación, pudo evidenciarse varias oportunidades de mejora y actividades complementarias de la solución propuesta que mejorarían el Modelo propuesto pero que por limitaciones temporales, se proponen como líneas de trabajo futuro. Ellas son las siguientes:

- Definir unos indicadores de desempeño PKI para el Modelo.
- Construir unos diagramas de despliegue de los componentes del Modelo.
- Construir unos instrumentos para apoyar la adopción del Modelo de Gobierno propuesto.
- Construir un producto de Software con un tablero de control que facilite la Monitorización, la dirección y el Control del Modelo de Gobierno propuesto.

- Revisar periódicamente las actualizaciones de la legislación del estado colombiano, los marcos de gobierno de TI y del MSPI, de manera que permita mantener un modelo de Gobierno de TI, acorde con las necesidades y tendencias de la organización.
- Evaluar la adaptabilidad del modelo propuesto, de manera que se pueda aplicar a cualquier organización, independiente del estado o sector.

Referencias

Andres J, Medina C, Edinson J and Garcia M 2011 Modelo De Integración Entre Meci Y Un Marco De Referencia Para Gobierno De Ti Aplicado A Entidades Territoriales Municipales En Colombia (Santiago de Cali: Universidad Icesi)

Aguilar Alonso I, Carrillo Verdún J, Tovar Caro E 2017 Description of the structure of the IT demand management process framework Int. J. Inf. Manage. 37 1461–73

Al Qassimia, N., & Rusu, L. (7 - 9 de Octubre de 2015). IT Governance in a Public Organization in a Developing Country: A Case Study of a Governmental Organization. ScienceDirect, 7. Obtenido de https://core.ac.uk/download/pdf/82196685.pdf

Ballester, M. (2010). Gobierno de las TIC ISO/38500. Journal Online, 4. Obtenido de https://www.isaca.org/Journal/archives/2010/Volume-1/Documents/jpdf1001-online-gobierno.pdf

Brandis K, Dzombeta S and Haufe K 2014 Towards a framework for governance architecture anagement in cloud environments: A semantic perspective Futur. Gener. Comput. Syst. 32 274–81.

Carlos J, Silva N, Fernandez L 1151 Manual para la implementación de la Estrategia de Gobierno en Línea (Colombia: Gobierno digital).

Cerqueira, L., & Denner dos, C. (2017). Un estudio acerca de la influencia de los mecanismos no operacionales en la efectividad de lagobernanza de tecnología de la información pública. SCielo, 52(3), pp.256-267. doi:http://dx.doi.org/10.1016/j.rausp.2017.05.005.

Chen Y C, Wu J H 2011 IT management capability and its impact on the performance of a CIO Inf. Manag. 48 145–56.

Congreso de la República 1998 Ley 489 sobre la organización y funcionamiento de las entidades

del orden nacional (Colombia: Congreso de la República)

Congreso de la República 2011 Ley 1437 código de procedimiento administrativo y de lo contencioso administrativo (Colombia: Congreso de la República)

Congreso de la República 2012 Ley estatutaria 1581 (Colombia: Congreso de la República).

Congreso de la República 2014 Ley 1712 de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones (Colombia: Congreso de la República).

Congreso de la República 2017 Decreto 1499 del cual se modifica el Decreto 1083 de 2015, Decreto Único Reglamentario del Sector Función Pública, en lo relacionado con el Sistema de Gestión establecido en el artículo 133 de la Ley 1753 de 2015 (Colombia: Congreso de la República)

Espinoza Aguirre C, Pillo Guanoluisa D 2018 IT governance model for public institutions with a focus on higher education (Cáceres:13a Conferencia Ibérica sobre Sistemas y Tecnologías de la Información (CISTI))

Fernández, M. A. (2009). Análisis, Planificación y Gobierno de las Tecnologías de la Información en las Universidades. Madrid España: Universidad de Almería.

Findeter. (2018). PLAN DE SEGURIDAD Y PRIVACIDAD DE LA.

Gómez, G. E. (2015). Gobernanza Corporativa de la Tecnología de la Información (T.I). Leganés,: Universidad Carlos III de Madrid.

Governance Institute 2007 It Governance Using Cobit ® And Val It Tm : Student Book, 2 Nd Edition t o h ig h e r e d u c a t io n (United States of America: Governance Institute)

Governance Institute. (s.f.). IT governance implementation guide using COBIT and Val IT. USA.

ISACA. (2012). COBIT 5 - Un marco de negocio para el gobierno y la estión de las TI de la empresa. Estados Unidos: Isaca.

ISACA. (2012). COBIT 5: Procesos Catalizadores.

ISACA. (2013). Guía de Auto-Evaluación: Usando COBIT 5. EE.UU.

ISO / IEC. (2015). ISO / IEC 38500: 2015. Obtenido de https://www.iso.org/standard/62816.html.

IT Governance Institute. (2009). ITGI TM Facilita la Adopción de IS0/IEC 38500:2008. EEUU: ITGI.

Kim Y J, Lee J M, Koo C, Nam K 2013 The role of governance effectiveness in explaining IT outsourcing performance Int. J. Inf. Manage. 33 850–60.

Lozano, L. (2015). Gobierno de TI, realidades sobre una década de prácticas en Colombia. Revista de Sistemas, 97.

Matias, M. (26 de Marzo de 2017). COBIT. Obtenido de http://cobitmmatiasc.blogspot.com/2017/03/dominios-y-procesos-de-cobit.html.

Mendoza Silva L, Vega Gallegos G 2018 Evaluación De La Capacidad De Detección Y Respuesta A Riesgos De Ciberseguridad, Caso De La Empresa Sisc (Colombia: Universidad del pacifico)

Mintic (2016). Modelo de Seguridad y Privacidad de la Información (Colombia: Ministerio de Tecnologías de la Información y las Comunicaciones).

MinTIC. (2016). Guía Metodológica de Pruebas de Efectividad. Seguridad y Privacidad de la Información, 28. Obtenido de https://www.mintic.gov.co/gestionti/615/articles-5482_G1_Metodologia_pruebas_efectividad.pdf.

MinTIC. (2018). MANUAL DE GOBIERNO DIGITAL. Bogotá.

Ocampo Garcias D 2011 Modelo de Seguridad de la Información para las Entidades Públicas del Estado Colombiano (Colombia:Universidad piloto de Colombia)

Rahimi F, Møller C, Hvam L 2016 Business process management and IT management: The missing integration Int. J. Inf. Manage. 36 142–54

Reguant-Álvarez, M., & Torrado-Fonseca, M. (2016). El método Delphi . REIRE,Revista d'Innovació i Recerca en Educació, 87-102.

Rodriguez Garcia & Garcia. (2017). El método Delphi para el procesamiento de los resultados de encuestas a expertos o usuarios en estudios de mercado y en la investigación educacional. Universidad Simón Bolivar.

Santiago Chinchilla E, Sánchez Allende J 2017 Riesgo de ciberseguridad en las empresa Tecnol. y Desarro.

UNE-ISO/IEC 38500. (Abril de 2013). Gobernanza corporativa de la Tecnología de la Información (TI). Mdrid, España: AENOR.

Useche Samudio C 2016 Metodología para la Medición de la Efectividad de los Indicadores de Gestión del Modelo de Seguridad y Privacidad de la Información (Bogotá: Escuela Colombiana de ingeniería Julio Garavito).

Vargas Alvarado S M 2017 Modelo De Gobierno De Ti Como Apoyo A Los Procesos Administrativos Caso Universidad De Los Llano (Manizales: Universidad Nacional de Colombia)

Verhoef C 2007 Quantifying the effects of IT-governance rules Sci Comput Program. 67 247–77

Apéndices

Apéndice A. Decreto 1078 de 2015

DECRETO 1078 DEL 26 DE MAYO DE 2015	
"TITULO 9 – POLÍTICAS Y LINEAMIENTOS DE TECNOLOGIAS DE LA INFORMACIÓN	
CAPÍTULO 1 - ESTRATEGÍA DE GOBIERNO EN LÍNEA	
SECCIÓN 1 - OBJETO, ÁMBITO DE APLICACIÓN, DEFINICIONES, PRINCIPIOS Y FUNDAMENTOS	
Artículo 2.2.9.1.1.1. Objeto	Definir los lineamientos, instrumentos y plazos de la estrategia de Gobierno en Línea para garantizar el máximo aprovechamiento de las Tecnologías de la Información y las Comunicaciones, con el fin de contribuir con la construcción de un Estado abierto, más eficiente, más transparente y más participativo y que preste mejores servicios con la colaboración de toda la sociedad. (Decreto 2573 de 2014, art.1)
Artículo 2.2.9.1.1.2. Ámbito de aplicación.	Serán sujetos obligados de las disposiciones contenidas en el presente capítulo las entidades que conforman la Administración Pública en los términos del artículo 39 de la Ley 489 de 1998 y los particulares que cumplen funciones administrativas. Parágrafo. La implementación de la estrategia de Gobierno en Línea en las Ramas Legislativa y Judicial, en los órganos de control, en los autónomos e independientes y demás organismos del Estado, se realizará bajo un esquema de coordinación y colaboración armónica en aplicación de los principios señalados en el artículo 209 de la Constitución Política. (Decreto 2573 de 2014, art. 2)
Artículo 2.2.9.1.1.3. Definiciones.	Para la interpretación del presente capítulo, las expresiones aquí utilizadas deben ser entendidas con el significado que a continuación se indica: ARQUITECTURA EMPRESARIAL: Es una práctica estratégica que consiste en analizar integralmente las entidades desde diferentes perspectivas o dimensiones, con el propósito de obtener, evaluar y diagnosticar su estado actual y establecer la transformación necesaria. El objetivo es generar valor a través de las Tecnologías de la Información para que se ayude a materializar la visión de la entidad. MARCO DE REFERENCIA DE ARQUITECTURA EMPRESARIAL PARA LA GESTIÓN DE TECNOLOGÍAS DE LA INFORMACIÓN: Es un modelo de referencia puesto a disposición de las instituciones del Estado colombiano para ser utilizado como orientador estratégico de las arquitecturas empresariales, tanto sectoriales como institucionales. El Marco establece la estructura conceptual, define lineamientos, incorpora mejores prácticas y orienta la implementación para lograr una administración pública más eficiente, coordinada y transparente, a través del fortalecimiento de la gestión de las Tecnologías de la Información. (Decreto 2573 de 2014, art. 3)
Artículo 2.2.9.1.1.4. Principios y fundamentos de la Estrategia de Gobierno en línea.	La Estrategia de Gobierno en línea se desarrollará conforme a los principios del debido proceso, igualdad, imparcialidad, buena fe, moralidad, participación, responsabilidad, transparencia, publicidad, coordinación, eficacia, economía y celeridad consagrados en los artículos 209 de la Constitución Política, 3 de la Ley 489 de 1998 y 3 de la Ley 1437 de 2011. Así mismo, serán fundamentos de la Estrategia los siguientes: Excelencia en el servicio al ciudadano: Propender por el fin superior de fortalecer la relación de los ciudadanos con el Estado a partir de la adecuada atención y provisión de los servicios, buscando la optimización en el uso de los recursos,

	teniendo en cuenta el modelo de Gestión Pública Eficiente al Servicio del Ciudadano y los principios orientadores de la Política Nacional de Eficiencia Administrativa al Servicio del Ciudadano. Apertura y reutilización de datos públicos: Abrir los datos públicos para impulsar la participación, el control social y la generación de valor agregado. Estandarización: Facilitar la evolución de la gestión de TI del Estado colombiano hacia un modelo estandarizado que aplica el marco de referencia de arquitectura empresarial para la gestión de TI. Interoperabilidad: Fortalecer el intercambio de información entre entidades y sectores. Neutralidad tecnológica: Garantizar la libre adopción de Tecnologías, teniendo en cuenta recomendaciones, conceptos y normativas de los organismos internacionales competentes e idóneos en la materia, que permitan fomentar la eficiente prestación de servicios, emplear contenidos y aplicaciones que usen Tecnologías de la Información y las Comunicaciones, así como garantizar la libre y leal competencia, y que su adopción sea armónica con el desarrollo ambiental sostenible. Innovación: Desarrollar nuevas formas de usar las Tecnologías de la Información y las Comunicaciones para producir cambios que ganen nuevo y mayor valor público. Colaboración: Implementar soluciones específicas para problemas públicos, mediante el estímulo y aprovechamiento del interés y conocimiento de la sociedad, al igual que un esfuerzo conjunto dentro de las propias entidades públicas y sus servidores. (Decreto 2573 de 2014, art. 4)
SECCIÓN 2 – COMPONENTES, INSTRUMENTOS Y RESPONSABLES	
Artículo 2.2.9.1.2.1. Componentes.	Los fundamentos de la Estrategia serán desarrollados a través de 4 componentes que facilitarán la masificación de la oferta y la demanda del Gobierno en Línea. 1. TIC para Servicios. Comprende la provisión de trámites y servicios a través de medios electrónicos, enfocados a dar solución a las principales necesidades y demandas de los ciudadanos y empresas, en condiciones de calidad, facilidad de uso y mejoramiento continuo. 2. TIC para el Gobierno abierto. Comprende las actividades encaminadas a fomentar la construcción de un Estado más transparente, participativo y colaborativo involucrando a los diferentes actores en los asuntos públicos mediante el uso de las Tecnologías de la Información y las Comunicaciones. 3. TIC para la Gestión. Comprende la planeación y gestión tecnológica, la mejora de procesos internos y el intercambio de información. Igualmente, la gestión y aprovechamiento de la información para el análisis, toma de decisiones y el mejoramiento permanente, con un enfoque integral para una respuesta articulada de gobierno y para hacer más eficaz la gestión administrativa entre instituciones de Gobierno. 4. Seguridad y privacidad de la Información. Comprende las acciones transversales a los demás componentes enunciados, tendientes a proteger la información y los sistemas de información, del acceso, uso, divulgación, interrupción o destrucción no autorizada. Parágrafo. TIC para el gobierno abierto comprende algunos de los aspectos que hacen parte de Alianza para el Gobierno Abierto, pero no los cobija en su totalidad. (Decreto 2573 de 2014, art.5)
Artículo 2.2.9.1.2.2. Instrumentos	Instrumentos. Los instrumentos para la implementación de la estrategia de Gobierno en línea serán los siguientes: Manual de Gobierno en Línea. Define las acciones que corresponde ejecutar a las entidades del orden nacional y territorial respectivamente. Marco de referencia de arquitectura empresarial para la gestión de Tecnologías

	de la Información. Establece los aspectos que los sujetos obligados deberán adoptar para dar cumplimiento a las acciones definidas en el Manual de Gobierno en Línea. Parágrafo 1. Los instrumentos podrán ser actualizados periódicamente cuando así lo determine el Ministerio de las Tecnologías de la Información y Comunicaciones. Parágrafo 2. La estrategia de Gobierno en Línea será liderada por el Ministerio de Tecnologías de la Información y Comunicaciones y articulada con las demás entidades cuando se relacionen con las funciones misionales que tengan a su cargo. (Decreto 2573 de 2014, art. 6)
Artículo 2.2.9.1.2.3. Responsable de coordinar la implementación de la Estrategia de Gobierno en línea en los sujetos obligados.	El representante legal de cada sujeto obligado, será el responsable de coordinar, hacer seguimiento y verificación de la implementación y desarrollo de la Estrategia de Gobierno en línea. (Decreto 2573 de 2014, art.7)
Artículo 2.2.9.1.2.4. Responsable de orientar la implementación de la Estrategia de Gobierno en línea.	En las entidades del orden nacional, el Comité Institucional de Desarrollo Administrativo de que trata el artículo 6 del Decreto 2482 de 2012, o las normas que lo modifiquen o sustituyan, será la instancia orientadora de la implementación de la Estrategia de Gobierno en línea al interior de cada entidad. Los sujetos obligados deberán incluir la estrategia de Gobierno en línea de forma transversal dentro de sus planes estratégicos sectoriales e institucionales, y anualmente dentro de los planes de acción de acuerdo con el Modelo Integrado de Planeación y Gestión de qué trata el Decreto 2482 de 2012 o las normas que lo modifiquen o sustituyan. En estos documentos se deben definir las actividades, responsables, metas y recursos presupuestares que les permitan dar cumplimiento a los lineamientos que se establecen. En las entidades del orden territorial y demás sujetos obligados, la instancia orientadora de la implementación de la Estrategia de Gobierno en línea será el Consejo de Gobierno o en su defecto el Comité Directivo o la instancia que haga sus veces. En caso que no existan estas instancias en el sujeto obligado, será la instancia o dependencia de mayor nivel jerárquico de la entidad. En las materias relacionadas con trámites adelantados por medios electrónicos. La instancia orientadora deberá articularse con el Comité Anti trámites o con el responsable de esta materia al interior de los sujetos obligados. (Decreto 2573 de 2014, art. 8)
SECCIÓN 3 – MEDICIÓN, MONITOREO Y PLAZOS	
Artículo 2.2.9.1.3.1. Medición y Monitoreo.	El Ministerio de Tecnologías de la Información y las Comunicaciones, a través de la Dirección de Gobierno en Línea y dela Dirección de Estándares y Arquitectura de Tecnologías de la Información, diseñará el modelo de monitoreo que permita medir el avance en las acciones definidas en el Manual de Gobierno en Línea que corresponda cumplir a los sujetos obligados, los cuales deberán suministrar la información que le sea requerida. En el caso de las entidades y organismos de la Rama Ejecutiva del Poder Público del Orden Nacional, la información será suministrada en el Formulario Único de Reporte de Avance en la Gestión (FURAG) o el que haga sus veces, de acuerdo con lo señalado en el Decreto 2482 de 2012, o las normas que lo modifiquen o sustituyan. (Decreto 2573 de 2014, art. 9)

Artículo 2.2.9.1.3.2.	Los sujetos obligados deberán implementar las actividades establecidas en el Manual de Gobierne en línea dentro de los siguientes plazos:

1. Sujetos obligados del Orden Nacional

COMPONENTE/ AÑO	2015	2016	2017	2018	2019	2020
TIC para Servicios	90%	100%	Mantener	Mantener 100%	Mantener 100%	Mantener 100%
TIC para el Gobierno abierto	90%	100%	Mantener	Mantener 100%	Mantener 100%	Mantener 100%
TIC para la Gestión	25%	50%	80%	100%	Mantener 100%	Mantener 100%
Seguridad y privacidad de la Información	40%	60%	80%	100%	Mantener 100%	Mantener 100%

2. Sujetos obligados del Orden territorial.

2.1. A. Gobernaciones de categoría Especial y Primera; alcaldías de categoría Especial, y demás sujetos obligados de la Administración Pública en el mismo nivel.

B. Gobernaciones de categoría segunda, tercera y cuarta; alcaldías de categoría primera, segunda y tercera y demás sujetos obligados de la Administración Pública en el mismo nivel.

C. Alcaldías de categoría cuarta, quinta y sexta, y demás sujetos obligados la Administración Pública en el mismo nivel.

Para las entidades agrupadas en A, B y C los plazos serán los siguientes:

COMPONENTE/ AÑO	Entidades A (%)						Entidades B (%)						Entidades C (%)					
	2015	2016	2017	2018	2019	2020	2015	2016	2017	2018	2019	2020	2015	2016	2017	2018	2019	2020
TIC para Servicios	70	90	100	Mantener100	Mantener 100	Mantener 100	45	70	100	Mantener 100	Mantener 100	Mantener 100	40	55	70	100	Mantener 100	Mantener 100
TIC para el Gobierno abierto	80	95	100	Mantener100	Mantener 100	Mantener 100	65	80	100	Mantener 100	Mantener 100	Mantener 100	65	75	85	100	Mantener 100	Mantener 100
TIC para la Gestión	20	45	80	100	Mantener 100	Mantener 100	10	30	50	65	80	100	10	30	50	65	80	100
Seguridad y privacidad de la Información	35	50	80	100	Mantener 100	Mantener 100	10	30	50	65	80	100	10	30	50	65	80	100

Parágrafo. Las obligaciones a cargo de los sujetos obligados indicadas en la ley 1712 de 2014 que sean incorporadas en los componentes, contarán con los plazos de cumplimiento señalados en dicha ley.

(Decreto 2573 de 2014, art. 10)

SECCIÓN 4 – MAPA DE RUTA, SELLO DE LA EXCELENCIA GOBIERNO EN LÍNEA EN COLOMBIA Y PLAZOS

Artículo 2.2.9.1.4.1. Mapa de ruta de Gobierno en línea.	El Ministerio de Tecnologías de la Información y la Comunicaciones, definirá un mapa de ruta que contendrá. 1. Servicios y trámites priorizados para ser dispuestos en línea. 2. Proyectos de mejoramiento para la gestión institucional e interinstitucional con el uso de medios electrónicos, que los sujetos obligados deberán implementar. 3. Las demás acciones que requieran priorizarse para masificar la oferta y la demanda de Gobierno en línea con base en lo señalado en los componentes de que trata el presente decreto.

<table>
<tr><td></td><td>Dicho mapa se publicará dentro de los seis (6) meses siguientes a la expedición del Decreto 2573 de 2014 y podrá ser actualizado periódicamente.
Parágrafo. La priorización de trámites y servicios que se incluyan en el mapa de ruta se hará en coordinación con el Departamento Administrativo de la Función Pública y el Departamento Nacional de Planeación, de acuerdo a sus competencias.
(Decreto 2573 de 2014, art. 11)</td></tr>
<tr><td>Artículo 2.2.9.1.4.2. Sello de excelencia Gobierno en Línea en Colombia</td><td>Los sujetos obligados deberán adoptar la marca o sello de excelencia Gobierno en Línea en Colombia en los niveles y plazos señalados en el artículo 2.2.9.1.4.3., de conformidad con el modelo de certificación y el mapa de ruta que defina el Ministerio de las Tecnologías de la Información y las Comunicaciones a través de la Estrategia de Gobierno en Línea.

Dicho modelo permitirá acreditar la alta calidad de los productos y servicios de los sujetos obligados, de manera que su cumplimiento les otorgue el derecho al uso de la marca correspondiente.

(Decreto 2573 de 2014, art. 12)</td></tr>
<tr><td>Artículo 2.2.9.1.4.3. Plazos para adoptar la marca o sello de excelencia Gobierno el Línea en Colombia.</td><td>Los sujetos obligados deberán adaptar la marca correspondiente en los siguientes plazos:</td></tr>
</table>

1. Sujetos obligados del Orden Nacional

CERTIFICACIONES / AÑO	2015	2016	2017	2018	2019	2020
TIC para Servicios		Nivel 1 según mapa de ruta	Nivel 2 según mapa de ruta	Nivel 3 según mapa de ruta	Mantener según el mapa de ruta	Mantener según el mapa de ruta
TIC para el Gobierno abierto		Nivel 1 según mapa de ruta	Nivel 2 según mapa de ruta	Nivel 3 según mapa de ruta	Mantener según el mapa de ruta	Mantener según el mapa de ruta
TIC para la Gestión			Nivel 1 según mapa de ruta	Nivel 2 según mapa de ruta	Nivel 3 según mapa de ruta	Mantener según el mapa de ruta

2. Sujetos obligados en el orden territorial.

2.1. Entidades A. Para Gobernaciones de categoría Especial y Primera; alcaldías de categoría Especial y demás sujetos obligados de la Administración Pública en el mismo nivel.

2.2. Entidades B. Para Gobernaciones de categoría segunda, tercera y cuarta; alcaldías de categoría primera, segunda y tercera, demás sujetos obligados de la Administración Pública en el mismo nivel.

2.3. Entidades C. Para Alcaldías de categoría cuarta, quinta y sexta y demás sujetos obligados de la Administración Pública en el mismo nivel.

Para las entidades agrupadas en A, B y C los plazos serán los siguientes:

CERTIFICACIONES / AÑO	Entidades A						Entidades B						Entidades C					
	2015	2016	2017	2018	2019	2020	2015	2016	2017	2018	2019	2020	2015	2016	2017	2018	2019	2020
TIC para Servicios		Nivel 1	Nivel 2	Nivel 3	Mantener Nivel	Mantener Nivel			Nivel 1	Nivel 2	Nivel 3	Mantener Nivel			Nivel 1	Nivel 2	Nivel 3	Mantener Nivel
TIC para el Gobierno abierto		Nivel 1	Nivel 2	Nivel 3	Mantener Nivel	Mantener Nivel			Nivel 1	Nivel 2	Nivel 3	Mantener Nivel			Nivel 1	Nivel 2	Nivel 3	Mantener Nivel
TIC para la Gestión			Nivel 1	Nivel 2	Nivel 3	Mantener Nivel				Nivel 1	Nivel 2	Nivel 3				Nivel 1	Nivel 2	Nivel 3

(Decreto 2573 de 2014, art. 13)

Apéndice B. Decreto 1008 de 2018

DECRETO 1008 DEL 14 DE JUNIO DE 2018	
“CAPÍTULO 1 – POLÍTICA DE GOBIERNO DIGITAL	
SECCIÓN 1 - OBJETO, ALCANCE, ÁMBITO DE APLICACIÓN Y PRINCIPIOS	
Artículo 2.2.9.1.1.1. Objeto	Establecer “lineamientos generales de la Política de Gobierno Digital para Colombia, antes estrategia de Gobierno en Línea, la cual desde ahora debe ser entendida como: el uso y aprovechamiento de las tecnologías de la información y las comunicaciones para consolidar un Estado y ciudadanos competitivos, proactivos, e innovadores, que generen valor público en un entorno de confianza digital (Decreto 1008, 2018)”.
Artículo 2.2.9.1.1.2. Ámbito de aplicación.	“Los sujetos obligados de las disposiciones contenidas en el presente capítulo serán las entidades que conforman la Administración Pública en los términos del artículo 39 de la Ley 489 de 1998 y los particulares que cumplen funciones administrativas” (Decreto 1008, 2018). “Parágrafo. La implementación de la Política de Gobierno Digital en las Ramas Legislativa y Judicial, en los órganos de control, en los autónomos e independientes y demás organismos del Estado, se realizará bajo un esquema de coordinación y colaboración armónica en aplicación de los principios señalados en los artículos 113 y 209 de la Constitución Política ” (Decreto 1008, 2018).
Artículo 2.2.9.1.1.3. Principios	La Política de Gobierno Digital se desarrollará conforme a los principios que rigen la función y los procedimientos administrativos consagrados en los artículos 209 de la Constitución Política, 3o de la Ley 489 de 1998, 3o de la Ley 1437 de 2011, 2o y 3o de la Ley 1712 de 2014, así como los que orientan el sector TIC establecidos en el artículo 2o de la Ley 1341 de 2009, y en particular los siguientes: Innovación: En virtud de este principio el Estado y los ciudadanos deben propender por la generación de valor público a través de la introducción de soluciones novedosas que hagan uso de TIC, para resolver problemáticas o necesidades identificadas. Competitividad: Según este principio el Estado y los ciudadanos deben contar con capacidades y cualidades idóneas para actuar de manera ágil y coordinada, optimizar la gestión pública y permitir la comunicación permanente a través del uso y aprovechamiento de las TIC. Proactividad: Con este principio se busca que el Estado y los ciudadanos trabajen de manera conjunta en el diseño de políticas, normas, proyectos y servicios, para tomar decisiones informadas que se anticipen a los acontecimientos, mitiguen riesgos y atiendan a las necesidades específicas de los usuarios, buscando el restablecimiento de los lazos de confianza a través del uso y aprovechamiento de las TIC. Seguridad de la Información: Este principio busca crear condiciones de uso confiable en el entorno digital, mediante un enfoque basado en la gestión de riesgos preservando la confidencialidad, integridad y disponibilidad de la información de las entidades del Estado, y de los servicios que prestan al ciudadano.
SECCIÓN 2 - ELEMENTOS DE LA POLÍTICA DE GOBIERNO DIGITAL	
Artículo 2.2.9.1.2.1.	La Política de Gobierno Digital será definida por el Ministerio de

Estructura.	Tecnologías de Información y las Comunicaciones y se desarrollará a través de componentes y habilitadores transversales que, acompañados de lineamientos y estándares, permitirán el logro de propósitos que generarán valor público en un entorno de confianza digital a partir del aprovechamiento de las TIC, conforme se describe a continuación: 1. Componentes de la Política de Gobierno Digital: Son las líneas de acción que orientan el desarrollo y la implementación de la Política de Gobierno Digital, a fin de lograr sus propósitos. Los componentes son: 1.1. TIC para el Estado: Tiene como objetivo mejorar el funcionamiento de las entidades públicas y su relación con otras entidades públicas, a través del uso de las Tecnologías de la Información y las Comunicaciones. 1.2. TIC para la Sociedad: Tiene como objetivo fortalecer la sociedad y su relación con el Estado en un entorno confiable que permita la apertura y el aprovechamiento de los datos públicos, la colaboración en el desarrollo de productos y servicios de valor público, el diseño conjunto de servicios, la participación ciudadana en el diseño de políticas y normas, y la identificación de soluciones a problemáticas de interés común. 2. Habilitadores Transversales de la Política de Gobierno Digital: Son los elementos fundamentales de Seguridad de la Información, Arquitectura y Servicios Ciudadanos Digitales, que permiten el desarrollo de los anteriores componentes y el logro de los propósitos de la Política de Gobierno Digital. 3. Lineamientos y estándares de la Política de Gobierno Digital: Son los requerimientos mínimos que todos los sujetos obligados deberán cumplir para el desarrollo de los componentes y habilitadores que permitirán lograr los propósitos de la Política de Gobierno Digital. 4. Propósitos de la Política de Gobierno Digital: Son los fines de la Política de Gobierno Digital, que se obtendrán a partir del desarrollo de los componentes y los habilitadores transversales, estos son: 4.1. Habilitar y mejorar la provisión de servicios digitales de confianza y calidad. 4.2. Lograr procesos internos, seguros y eficientes a través del fortalecimiento de las capacidades de gestión de tecnologías de información. 4.3. Tomar decisiones basadas en datos a partir del aumento, el uso y aprovechamiento de la información. 4.4. Empoderar a los ciudadanos a través de la consolidación de un Estado Abierto. 4.5. Impulsar el desarrollo de territorios y ciudades inteligentes para la solución de retos y problemáticas sociales a través del aprovechamiento de las TIC.
ARTÍCULO 2.2.9.1.2.2. MANUAL DE GOBIERNO DIGITAL.	Para la implementación de la Política de Gobierno Digital, las entidades públicas deberán aplicar el Manual de Gobierno Digital que define los lineamientos, estándares y acciones a ejecutar por parte de los sujetos

	obligados de esta Política de Gobierno Digital, el cual será elaborado y publicado por el Ministerio de Tecnologías de la Información y las Comunicaciones, en coordinación con el Departamento Nacional de Planeación. Parágrafo 1. El Manual podrá ser actualizado cuando así lo determine el Ministerio de las Tecnologías de la Información y Comunicaciones o cuando así lo recomiende el Consejo para la Gestión y Desempeño Institucional. Parágrafo 2. El Manual se articulará con los lineamientos que defina el Consejo Nacional de Política Económica y Social (Conpes) y se relacionen con los Componentes de la política de Gobierno Digital y se constituirá en herramienta metodológica del manual operativo del Modelo Integrado de Planeación y Gestión.
SECCIÓN 3 - INSTITUCIONALIDAD	
Artículo 2.2.9.1.3.1. Líder de la Política de Gobierno Digital.	El Ministerio de Tecnologías de la Información y las Comunicaciones, a través de la Dirección de Gobierno Digital o quien haga sus veces, liderará la Política de Gobierno Digital, en articulación con las demás entidades del Modelo Integrado de Planeación y Gestión cuando las temáticas o funciones misionales lo requieran.
Artículo 2.2.9.1.3.2. Responsable Institucional de la Política de Gobierno Digital.	El representante legal de cada sujeto obligado, será el responsable de coordinar, hacer seguimiento y verificación de la implementación de la Política de Gobierno Digital.
Artículo 2.2.9.1.3.3. Responsable de orientar la implementación de la Política de Gobierno Digital.	Los Comités Institucionales de Gestión y Desempeño de que trata el artículo 2.2.22.3.8 del Decreto número 1083 de 2015, serán los responsables de orientar la implementación de la política de Gobierno Digital, conforme a lo establecido en el Modelo Integrado de Planeación y Gestión.
Artículo 2.2.9.1.3.4. Responsable de liderar la implementación de la Política de Gobierno Digital.	El Director, Jefe de Oficina o Coordinador de Tecnologías y Sistemas de la Información y las Comunicaciones, o quien haga sus veces, de la respectiva entidad, tendrá la responsabilidad de liderar la implementación de la Política de Gobierno Digital. Las demás áreas de la respectiva entidad serán corresponsables de la implementación de la Política de Gobierno Digital en los temas de su competencia. El Director, Jefe de Oficina o Coordinador de Tecnologías y Sistemas de la Información y las Comunicaciones, o quien haga sus veces, hará parte del Comité Institucional de Gestión y Desempeño y responderá directamente al representante legal de la entidad, de acuerdo a lo establecido en el artículo 2.2.3.5.4. del Decreto Único Reglamentario de Función Pública 1083 de 2015.
SECCIÓN 4 - SEGUIMIENTO Y EVALUACIÓN	
Artículo 2.2.9.1.4.1. Seguimiento y Evaluación	El Ministerio de Tecnologías de la Información y las Comunicaciones, a través de la Dirección de Gobierno Digital, adelantará el seguimiento y evaluación de la Política de Gobierno Digital por medio de indicadores de cumplimiento e indicadores de resultado, de acuerdo con los criterios de evaluación y seguimiento definidos por el Consejo para la Gestión y Desempeño institucional. Así mismo, realizará mediciones de calidad a través del Sello de Excelencia de Gobierno Digital, sin perjuicio de las funciones asignadas al Departamento Nacional de Planeación. Para tal efecto, los sujetos obligados deberán suministrar la información que les sea requerida a través del Formulario Único de Reporte de Avance

	en la Gestión (FURAG) o el que haga sus veces, de acuerdo a lo señalado en el artículo 2.2.22.3.10 del Decreto número 1083 de 2015, Decreto Único Reglamentario de Función Pública. Parágrafo 1o. El modelo del sello de Excelencia de Gobierno en Línea adoptado por el Ministerio de Tecnologías de la Información y las Comunicaciones, pasará a denominarse modelo del Sello de Excelencia de Gobierno Digital, y a través de él, se evaluará la alta calidad de los productos y servicios digitales y capacidades de gestión de TI de los sujetos obligados. Parágrafo 2o. El seguimiento y la evaluación del avance de la Política de Gobierno Digital se realizarán con un enfoque de mejoramiento continuo, verificando que cada sujeto obligado presente resultados anuales mejores que en la vigencia anterior, de acuerdo con la segmentación de entidades definida en el artículo 2.2.9.1.4.2 del presente Decreto. Parágrafo 3o. El Ministerio de Tecnologías de la Información y las Comunicaciones podrá adelantar, bajo las directrices del Consejo para la Gestión y el Desempeño Institucional, estudios específicos para medir aspectos relacionados con la Política, para lo cual los sujetos obligados deberán suministrar la información que les sea requerida a través del FURAG.
Artículo 2.2.9.1.4.2. Segmentación de entidades	El Ministerio de Tecnologías de la Información y las Comunicaciones definirá, en el Manual de Gobierno Digital, la segmentación de los sujetos obligados de acuerdo a los criterios diferenciales de los territorios y de las entidades, para adelantar la orientación, implementación, seguimiento y evaluación de la política. El Ministerio de Tecnologías de la Información y las Comunicaciones propondrá la segmentación de entidades del orden territorial, y las actualizaciones que se requieran, para aprobación del Consejo para la Gestión y Desempeño Institucional, conforme a lo establecido en el artículo 2.2.22.3.11 del Decreto número 1083 de 2015.

Fuente: (Decreto 1008, 2018)

Apéndice C. Validación de Expertos – Cuestionario 1

ENCUESTA PARA DETERMINAR EL COEFICIENTE DE COMPETENCIA DEL EXPERTO

Nombres y apellidos:_____
Formación Académica: _____
Áreas De Experiencia Profesional tiempo (Meses): _____
Ha participado en alguna fase de Implementación o Auditoria del MSPI: _____
Cargo Actual:_____
Entidad: _____

Solicitamos a usted muy respetuosamente su colaboración como experto para ser consultado respecto al grado de factibilidad del MODELO DE GOBERNANZA DE TI PARA LAS ENTIDADES DEL ESTADO, COMO APOYO AL CUMPLIMIENTO DEL COMPONENTE DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN EN EL MARCO DE LA POLÍTICA DE GOBIERNO DIGITAL. Por tanto, se requiere determinar su coeficiente de competencia en este tema, para esto se requiere la respuesta de las siguientes preguntas de la forma más objetiva que le sea posible.

1.- Marque con una cruz (X), en la tabla siguiente, el valor que se corresponde con el grado de conocimientos que usted posee sobre el tema: "MODELO DE GOBERNANZA DE TI PARA LAS ENTIDADES DEL ESTADO, COMO APOYO AL CUMPLIMIENTO DEL COMPONENTE DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN EN EL MARCO DE LA POLÍTICA DE GOBIERNO DIGITAL". Teniendo en cuenta que según el conocimiento sobre el tema referido va creciendo desde 0 hasta 10.

1	2	3	4	5	6	7	8	9	10

2.- Realice una auto valoración del grado de influencia de cada una de las fuentes que le presentamos a continuación, según su conocimiento y criterio sobre: "MODELO DE GOBERNANZA DE TI PARA LAS ENTIDADES DEL ESTADO, COMO APOYO AL CUMPLIMIENTO DEL COMPONENTE DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN EN EL MARCO DE LA POLÍTICA DE GOBIERNO DIGITAL". Según la escala tipo Likert marque con una cruz (X), según corresponda, en A (alto), M (medio) o B (bajo).

FUENTES DE ARGUMENTACIÓN	**Grado de influencia de las fuentes en sus criterios**		
	A (alto)	**M** (medio)	**B** (bajo)
Análisis teórico realizado por usted			
Su experiencia obtenida			
Trabajo de autores nacionales			
Trabajos de autores extranjeros			
Su propio conocimiento del estado del problema en el extranjero			
Su intuición			

GRACIAS POR SU COLABORACIÓN… DIOS LES BENDIGA.

Apéndice D. Validación de Expertos – Cuestionario 2

VALIDACIÓN DE EXPERTOS

MODELO DE GOBERNANZA DE TI PARA LAS ENTIDADES DEL ESTADO, COMO APOYO AL CUMPLIMIENTO DEL COMPONENTE DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN EN EL MARCO DE LA POLÍTICA DE GOBIERNO DIGITAL

RECUERDE QUE LA INFORMACION SUMINISTRADA ES DE CARÁCTER CONFIDENCIAL. TODO EL MANEJO: APLICACIÓN, PROCESAMIENTO, ANALISIS E INFORMES ES CON FINES ACADEMICOS.

INFORMACION GENERAL

Nombre: _____ **Entidad:** _____

Ciudad: _____ **Cargo:** _____

NIVEL EDUCATIVO (Calificación profesional, grado científico o académico)

Profesor o Investigador		Magister	
Profesional o Licenciado		Doctor	
Especialista		Postdoctoral	

EXPERIENCIA (Favor calcular la experiencia en años)

Experiencia en el Cargo:

Experiencia docente y/o en la investigación:

En cumplimiento del requisito para optar el título de Magister en Gobierno de Tecnología de la Información se presenta la propuesta "MODELO DE GOBERNANZA DE TI PARA LAS ENTIDADES DEL ESTADO, COMO APOYO AL CUMPLIMIENTO DEL COMPONENTE DE SEGURIDAD Y PRIVACIDAD DE LA INFORMACIÓN EN EL MARCO DE LA POLÍTICA DE GOBIERNO DIGITAL", el cual se adjunta y colocamos a su consideración para su respectiva valoración.

Respetado colaborador. Lea atentamente cada uno de los criterios que se proponen e indique en la columna la calificación que en su opinión de experto corresponde a su criterio para evaluar el modelo de gobernanza en TI propuesto.

Muy Relevante	**MR**	Poco Relevante	**PR**
Bastante Relevante	**BR**	No Relevante	**NR**
Relevante	**R**		

ENUNCIADOS

MODELO DE ACTUACIÓN	**(Marque x en la opción que mejor refleje su opinión)**				
1. ¿Considera relevante la aseveración de que el gobierno de TI integra e institucionaliza las buenas prácticas para garantizar que la TI en las entidades públicas soporten los objetivos del negocio?	MR	BR	R	PR	NR
2. ¿Considera que la adopción de un modelo de Gobernanza de TI para las entidades del estado, mejora la eficacia de la implementación del modelo de seguridad y privacidad de la información propuesto dentro del marco de la estrategia de Gobierno Digital?.	MR	BR	R	PR	NR
3. ¿Considera que el patrón de gobierno de TI diseñado, se adapta al Modelo de Seguridad y Privacidad de la Información (MSPI) de MinTIC en Colombia?	MR	BR	R	PR	NR
4. ¿Comparte la idea de que las características particulares consideradas en el modelo de Gobernanza de TI; les facilita a las entidades del estado colombiano cumplir con la implementación y gestión del Programa de Seguridad y Privacidad de la Información propuesto por MINTIC y mejorar la eficacia en su adopción?	MR	BR	R	PR	NR
5. ¿Considera que la Propuesta de Modelo de Gobernanza de TI para las entidades del estado, como apoyo al cumplimiento del componente de Seguridad y Privacidad de la Información, puede añadir valor y si se sigue e implementa facilita a las entidades del estado colombiano el cumplimiento del Decreto 1008 de 2018?	MR	BR	R	PR	NR
6. ¿Considera que el modelo propuesto, posee los elementos estructurales (Dominios, niveles, metas de TI y fases del MSPI) de un modelo de gobierno de TI.	MR	BR	R	PR	NR
7. ¿Existe coherencia entre los elementos estructurales (Dominios, niveles, metas de TI y fases del MSPI) del modelo propuesto?	MR	BR	R	PR	NR

8. ¿Hay correspondencia entre el modelo diseñado y la definición de un modelo de Gobernanza de TI?.	MR	BR	R	PR	NR
9. Existe claridad en el contenido de cada elemento del modelo.	MR	BR	R	PR	NR
10. ¿Existe correspondencia entre los elementos estructurales del modelo, sus objetivos y sus características?	MR	BR	R	PR	NR
11. ¿Considera que la adopción del modelo de Gobernanza propuesto, facilita la dirección y el control del Sistema de Gestión de Seguridad de la Información MSPI?	MR	BR	R	PR	NR
Autoriza que su nombre aparezca como Jurado experto en la tesis	SI		NO		

GRACIAS POR SU PARTICIPACION