



Proyecto de Fortalecimiento del Modelo de Vigilancia y Control - Resultados Fase I

JULIO DE 2020



Proyecto de Fortalecimiento del Modelo de Vigilancia y Control

Resultados Fase I



Karen Cecilia Abudinen Abuchaibe

Ministra de Tecnologías de la Información y las Comunicaciones



Iván Antonio Mantilla Gaviria

Viceministro de Conectividad y Digitalización



Gloria Liliana Calderón Cruz

Directora de Vigilancia y Control



Asesores

Liliana Giral Penagos

Natalia Serrano Ferrer

Valentina Roca Aguilera



PROYECTO DE FORTALECIMIENTO DEL MODELO DE VIGILANCIA Y CONTROL RESULTADOS FASE I

● Contenido

1.	OBJETIVO Y ALCANCE.....	5
2.	INTRODUCCIÓN.....	6
3.	ENFOQUE METODOLÓGICO	7
3.1.	FASE DE LEVANTAMIENTO Y ARQUITECTURA AS-IS.....	10
3.2.	FASE DE PROCESAMIENTO Y ARQUITECTURA TO-BE	10
3.3.	FASE DE ANÁLISIS DE BRECHA Y PLAN DE ACCIÓN	11
4.	ESTADO ACTUAL (AS - IS) DEL MODELO DE VIGILANCIA Y CONTROL.....	12
4.1.	Dominio Estrategia	12
4.2.	Dominio negocio	13
4.3.	Dominio Información	16
4.4.	Dominio Sistemas de Información.....	18
4.5.	Dominio Servicios Tecnológicos	22
4.6.	Resumen resultados estado actual	25
5.	ARQUITECTURA OBJETIVO (TO-BE)	26
5.1.	DOMINIO ESTRATEGIA	27
5.2.	DOMINIO NEGOCIO.....	30
5.3.	DOMINIO DE INFORMACIÓN.....	39
5.4.	DOMINIO SISTEMAS DE INFORMACIÓN	45
5.5.	DOMINIO DE SERVICIOS TECNOLÓGICOS	49
6.	ANÁLISIS DE BRECHAS Y PLAN DE ACCIÓN.....	50
6.1.	PORTAFOLIO DE PROYECTOS Y PLAN DE ACCIÓN	51
7.	CONCLUSIONES	57
8.	BIBLIOGRAFÍA.....	59

Ilustraciones

Ilustración 1. Metamodelo.....	8
Ilustración 2. Cadena de Valor de Vigilancia y Control AS-IS	14
Ilustración 3. Madurez de los pilares de la información actual	17
Ilustración 4. Diagrama de sistemas de información Vs. procedimientos.....	18
Ilustración 5. Sistemas de información alineados a los procesos MinTIC	19
Ilustración 6. Sistemas de información que interactúan o son fuente de información en el proceso de Vigilancia y Control	23
Ilustración 7. Ambientes de pruebas.....	24
Ilustración 8. Relación entre planes, normatividad y modelo de Vigilancia y Control	28
Ilustración 9. Ciclo de mejora continua del modelo de Inspección, Vigilancia y Control propuesto.....	30





Ilustración 10. Cadena de valor Modelo de Inspección, Vigilancia y Control propuesto	31
Ilustración 11. Canales de comunicación vs. procesos.....	36
Ilustración 12. Diagrama del modelo de entidades de datos.....	40
Ilustración 13. Madurez de los pilares de la información deseada.....	44
Ilustración 14. Arquitectura centrada en datos.....	46
Ilustración 15. Procedimientos vs servicios de negocio vs sistemas de información.....	47
Ilustración 16. Ejemplo de uso del ESB WS02.....	48
Ilustración 17. Programas y proyectos del plan de acción	52
Ilustración 18. Criterios de priorización	52
Ilustración 19. Resultados proyectos.....	53
Ilustración 20. Hoja de ruta esencial	54
Ilustración 21. Hoja de ruta prioritaria.....	55
Ilustración 22. Hoja de ruta importante	55

Tablas

Tabla 1. Descripción de los dominios - Arquitectura Empresarial	7
Tabla 2. Componentes del metamodelo	10
Tabla 3. Descripción Sistemas de información	21
Tabla 4. Partes interesadas de Modelo propuesto.....	35
Tabla 5. Procedimientos nuevo modelo	38
Tabla 6. Catálogo de entidades maestras	41
Tabla 7. Catálogo de Entidades de Información Interoperables.....	43
Tabla 8. Mapa de ruta - áreas involucradas.....	56

Resumen: El foro económico mundial ha definido la cuarta revolución industrial (4RI) como la acelerada introducción de la tecnología en los diferentes ámbitos de la vida de las personas (WEF, 2016). La transformación digital es una característica de la 4RI, ya que es un proceso de explotación de tecnologías digitales que tiene la capacidad de crear nuevas formas de hacer las cosas en todos los sectores económicos. Con la expedición del CONPES 3975 de 2019 se plantea como línea de acción mejorar el desempeño de la política de gobierno digital, para abordar la adopción y explotación de la transformación digital en el sector público.

El presente documento describe un proyecto que se puede enmarcar dentro de esta línea de acción. Como parte del sector público, el MINTIC ha decidido llevar a cabo un ejercicio de arquitectura empresarial sobre el modelo de inspección, vigilancia y control actual con el fin plantear una propuesta de modelo más eficiente a partir de la automatización y del análisis de grandes volúmenes de datos (Big Data). Con lo anterior, en el documento se explica el proyecto y se presentan los resultados de la primera fase.

Es importante mencionar que el presente documento fue elaborado con base en los resultados del contrato de consultoría 837 de 2019 suscrito con la Unión Temporal Bisa Grow.





1. OBJETIVO Y ALCANCE

El proyecto de Fortalecimiento del Modelo de Vigilancia y Control se estructuró en dos fases. La primera de ellas consistió en realizar el Diagnóstico del Modelo de Vigilancia y Control actual, mediante el enfoque de arquitectura empresarial, para el análisis y procesamiento de la información que dicho modelo genera a través de los procesos, procedimientos, bases de datos, sistemas de información, matrices de obligaciones, cargas de trabajo, formatos y demás fuentes de consulta que tenga la Dirección de Vigilancia y Control del Ministerio TIC, en relación con los servicios de comunicaciones móviles, no móviles, radiodifusión sonora, servicios postales y de televisión (AS IS); así como establecer recomendaciones dirigidas al fortalecimiento y modernización de dicho modelo bajo el mismo enfoque (TO BE). La segunda fase del proyecto contempla la ejecución de todos los proyectos requeridos para llegar al estado deseado (TO BE) del Modelo de Inspección, Vigilancia y Control.

El objetivo de este documento es presentar al lector los resultados de la fase I del proyecto, es decir, el estado actual y deseado del modelo de Vigilancia y Control desde la perspectiva de Arquitectura Empresarial. De igual forma, se realiza un análisis de las brechas existentes para llegar del estado actual al deseado. Con el fin de cerrar estas brechas, se proponen una serie de programas y proyectos, con un plan de acción identificando la duración de cada uno y la relación entre ellos.

Este documento corresponde al informe final con base en el diagnóstico, las recomendaciones y la propuesta de un nuevo modelo de inspección, vigilancia y control. Se presentan los resultados principales, la metodología empleada para el desarrollo del proyecto, una breve descripción del diagnóstico del estado actual del modelo de vigilancia y control de MinTIC, una breve descripción de la propuesta del estado objetivo de dicho modelo y, finalmente, el análisis de brechas entre el estado actual y el estado deseado, la propuesta de portafolio de proyectos para el cierre de brechas y el mapa de ruta propuesto para la instauración del nuevo modelo de inspección, vigilancia y control.

El diagnóstico se desarrolló basado en un enfoque de arquitectura empresarial, para lo cual se siguieron los lineamientos de los siguientes documentos:

- Marco de referencia de arquitectura empresarial de MinTIC¹.
- Modelo Integrado de Planeación y Gestión MIPG².
- Marco de interoperabilidad MinTIC³.
- Gobierno Digital MinTIC⁴.
- Marco de trabajo de arquitectura empresarial de Open Group TOGAF®⁵.

¹ Marco de referencia MinTIC <https://www.mintic.gov.co/arquiturati/630/w3-propertyvalue-8118.html>

² Modelo Integrado de Planeación y Gestión <https://www.funcionpublica.gov.co/web/mipg>

³ Marco de interoperabilidad <https://www.mintic.gov.co/arquiturati/630/w3-propertyvalue-8117.html>

⁴ Gobierno digital https://estrategia.gobiernoenlinea.gov.co/623/articles-81473_recurso_1.pdf

⁵ Arquitectura Empresarial TOGAF <https://pubs.opengroup.org/architecture/toqaf9-doc/arch/index.html>





2. INTRODUCCIÓN

La convergencia de los servicios TIC viene acompañada de la necesidad de modernizar el ejercicio de Inspección, Vigilancia y Control que adelanta el Ministerio TIC sobre los prestadores de servicios de telecomunicaciones y servicios postales, para contribuir a la mejora en la calidad de los servicios ofrecidos a los ciudadanos. Es así, que en cumplimiento de los compromisos del Plan TIC 2018 – 2022, la Dirección de Vigilancia y Control diseñó en 2019 el proyecto de Fortalecimiento al Modelo de Vigilancia y Control, a través del cual se busca migrar el modelo actual a uno que, mediante el uso de herramientas tecnológicas y la explotación de grandes volúmenes de datos permita realizar el ejercicio de inspección y vigilancia de forma predictiva y preventiva.

Con lo anterior en mente, la Dirección de Vigilancia y Control del Ministerio TIC adelantó el proceso de selección a través de concurso de méritos abierto, para contratar un consultor que realizara el Diagnóstico del Modelo de Vigilancia bajo un enfoque de Arquitectura Empresarial. En este orden, en diciembre de 2019 la Unión Temporal BISA GROW conformada por las empresas BISA Corporation Ltda y Grow Data SAS resultó adjudicataria para la ejecución del mencionado proyecto por valor de \$823.336.800.

Así las cosas, mediante el contrato de consultoría No. 837 de 2019, la Unión Temporal BISA Grow ejecutó el diagnóstico al modelo de vigilancia y control, el cual tuvo lugar del 11 diciembre de 2019 al 30 de marzo, con prórroga hasta el 31 de mayo de 2020.

El mencionado diagnóstico se enmarcó dentro de los lineamientos de Arquitectura Empresarial del MinTIC (Comunicaciones, 2019) y el Marco de Arquitectura Empresarial del TOGAF, partiendo con la identificación de la arquitectura actual del MRAE (AS-IS) del Modelo de Vigilancia y Control desde los dominios de Estrategia, Negocio, Información, Sistemas de Información y Servicios Tecnológicos, planteamiento de la arquitectura objetivo MRAE (TO-BE), a través de la cual se procesa la información obtenida en la etapa de levantamiento de información y se plantea el estado deseado a la luz de las necesidades identificadas por la Dirección de Vigilancia y Control; y el análisis de brechas del MRAE y mapa de ruta o plan de acción, que por su parte establece la línea de acción a través de la cual deben desarrollarse los proyectos con las iniciativas que resulten del correspondiente análisis para el cierre de brechas.

Con base en lo anterior, el presente documento, expone el marco metodológico aplicado para la realización del Diagnóstico, así como los principales resultados obtenidos del análisis de estado actual del Modelo de Vigilancia y Control en los aspectos de Estrategia, Negocio, Información, Sistemas de Información y Servicios Tecnológicos descritos en la sección 4. Así mismo, en la sección 5 se presenta las opciones de mejora en estos aspectos, para lograr un nuevo Modelo de Inspección, Vigilancia y Control. Por último, la sección 6 tratará las brechas identificadas entre el estado del actual del Modelo (AS-IS) y el deseado (TO-BE) y expondrá los proyectos necesarios que deberán desarrollarse al interior de la Entidad para lograr el objetivo de contar con un Modelo de Inspección, Vigilancia y Control preventivo y predictivo basado en el análisis de grandes volúmenes de datos (Big Data).



3. ENFOQUE METODOLÓGICO

Para el desarrollo del Diagnóstico del Modelo de Vigilancia y Control se estableció como punto de partida los lineamientos del Marco de Referencia de Arquitectura Empresarial definidos por el Ministerio TIC a través de diferentes instrumentos como el MAE.G.GEN.01 - Documento Maestro del Modelo de Arquitectura Empresarial, instrumento que establece la estructura conceptual, define los lineamientos, incorpora las mejores prácticas y marca la ruta de implementación de proyectos al interior de las entidades públicas, G.GEN.03 Guía General de un Proceso de Arquitectura Empresarial, los lineamientos del Marco de Interoperabilidad para el Gobierno Digital y Metodología de Arquitectura Empresarial del marco de referencia TOGAF.

El desarrollo del Diagnóstico al Modelo de Vigilancia y Control bajo el enfoque de Arquitectura Empresarial (TOGAF) comprendió la evaluación y análisis integral de los componentes (dominios) de estrategia, negocio, información, sistemas de información y tecnología, mediante el levantamiento de información y planteamiento de la Arquitectura Actual (AS-IS), propuesta de Arquitectura Objetivo (TO-BE) y Análisis de Brechas y mapa de ruta que establece acciones para pasar de la arquitectura actual a la deseada.

Dominio	Alcance
Estrategia y gobierno	<ul style="list-style-type: none">Comprende la evaluación y el análisis de la interacción del Modelo de Vigilancia y Control actual con el Plan Nacional de Desarrollo, Plan Estratégico Institucional, Plan Estratégico de Tecnologías de la Información, Leyes, Decretos y Resoluciones.
Arquitectura de negocio	<ul style="list-style-type: none">Responsable de la comprensión de la cadena valor, los procesos, procedimientos, las áreas o unidades organizacionales, las personas y su organigrama.
Arquitectura de información	<ul style="list-style-type: none">Responsable de la comprensión de los datos, la información y el conocimiento producido a través del ejercicio de vigilancia y control.
Arquitectura de sistemas de información	<ul style="list-style-type: none">Responsable de la comprensión de los sistemas de información, aplicaciones y software.
Arquitectura de tecnología	<ul style="list-style-type: none">Responsable de la comprensión de los centros de datos y el hardware que se encuentra en el centro de datos, como los servidores, almacenamientos, UPS⁶, dispositivos de redes, dispositivos de seguridad, entre otros.

Tabla 1. Descripción de los dominios - Arquitectura Empresarial

Fuente: MinTIC – UT Bisa Grow, 2020.

Alineado con lo anterior, el ejercicio de Arquitectura Empresarial viene acompañado del Metamodelo, que corresponde a la definición de los componentes que intervienen en el proceso de vigilancia y control y cómo éstos gráficamente se interrelacionan.

⁶ *Uninterruptible Power Supply.*

La siguiente ilustración representa el Metamodelo implementado para el desarrollo del Diagnóstico del Modelo de Vigilancia y Control:

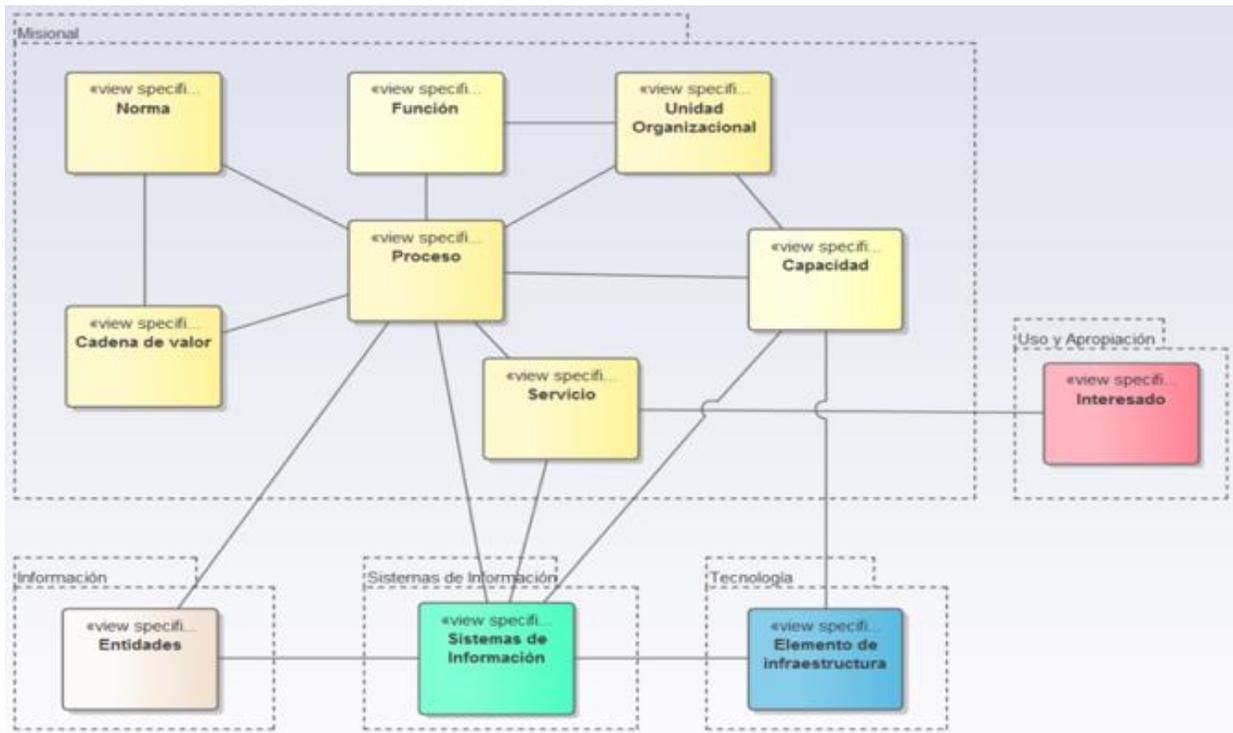


Ilustración 1. Metamodelo
Fuente: UT Bisa Grow, 2020.

El metamodelo está compuesto por 12 componentes agrupados por dominio, los cuales se relacionan entre sí, permitiendo asociar las características de cada uno con el análisis arquitectónico. A continuación, se hace una breve descripción de cada componente.

No.	Componentes del metamodelo	Descripción del Componente
1	Estrategia	Estado o condición que la entidad quiere lograr o sostener a través de los medios adecuados para impulsar el fortalecimiento institucional para la gestión efectiva de la Dirección de Vigilancia y Control del MinTIC, establecidos en su Plan Estratégico Institucional y el PETI. Define los fines principales para avanzar hacia el cumplimiento de la visión institucional.
2	Normatividad	Leyes, decretos, políticas o reglamentos que rigen conductas y procedimientos según los criterios y lineamientos establecidos desde la constitución y su ordenamiento jurídico para desarrollar la misionalidad dentro de la Dirección de Vigilancia y Control del MinTIC.



3	Capacidad	Son las habilidades para ejecutar un curso de acción especificado para alcanzar metas y objetivos estratégicos. Una capacidad no es una función de negocio, pero es un concepto que debe estar desarrollado en otros objetos, en particular actores que cumplen roles, funciones de negocio, procesos de negocio, productos, servicios de negocio, servicios de aplicación, componentes de aplicaciones e infraestructura.
4	Unidad organizacional	Representa cualquier asociación reconocida de gente en el contexto de la Dirección de Vigilancia y Control del MinTIC, que tiene unos objetivos de negocio y que participa en procesos del negocio de la entidad. Son las unidades, áreas misionales o de apoyo, grupos de trabajo que hacen parte de la estructura organizacional de la Dirección de Vigilancia y Control del MinTIC.
5	Función	Es una perspectiva que define el comportamiento y responsabilidad de una unidad organizacional respondiendo al "qué" hace o de qué es responsable dentro del modelo de inspección vigilancia y control.
6	Servicio	Un servicio representa una vista externa de lo que una organización o unidad organizacional ofrece a sus clientes. Un servicio es realizado/soportado por procesos. Un servicio puede ser ejecutado por una función o directamente por un servicio de aplicación; sin embargo, lo correcto es modelarlo para que sea ejecutado desde un proceso. De ser necesario se pueden descomponer los servicios en componentes más pequeños para darle mayor precisión a su flujo.
7	Proceso	Los procesos también son otra perspectiva (al igual que las funciones) que definen el comportamiento, pero en este caso especificando el "cómo" (cómo es hecho el trabajo). Los procesos son contenedores que encapsulan la lógica de la operación del negocio en la forma de subprocesos, actividades, roles, entradas, salidas, aplicaciones, recursos necesarios.
8	Cadena de Valor	La cadena de valor es un modelo que permite describir las actividades de una organización para generar valor al cliente final y a la misma institución. Es hecha operativa por los procesos del negocio.
9	Entidades de datos	Es un agrupamiento de datos que representa un elemento del negocio, como persona, cédula, nombre, apellido, estado civil.
10	Sistemas de información	Sistemas de información es una unidad autónoma de funcionalidad. Los servicios pueden ser combinados con otros servicios de software para proporcionar la funcionalidad completa de una aplicación de mayor tamaño. Es un servicio que provee datos, información o conocimiento para ser consumidos por componentes de software, aplicaciones internas o sistemas de información externos. Puede agregar otros servicios de aplicación.
11	Elementos de Infraestructura	Representa un objeto o componente del mundo real con existencia independiente que sirve como base para procesar, almacenar o transportar información o un servicio de información. Por ejemplo, un switch, un





		hardware de comunicaciones, un firewall físico, un arreglo de discos, un servidor con procesador, memoria, disco e interfaz de comunicación.
12	Interesado	Grupo de individuos u organizaciones que pueden afectar o verse afectados por el ejercicio de la arquitectura empresarial.

Tabla 2. Componentes del metamodelo

Fuente: UT Bisa Grow, 2020.

Explicado lo anterior, a continuación, se detalla la metodología adelantada en cada una de las etapas de la fase I del proyecto: Diagnóstico al Modelo de Vigilancia y Control.

3.1. FASE DE LEVANTAMIENTO Y ARQUITECTURA AS-IS

Fase cuyo propósito fue establecer el estado actual del Modelo de Vigilancia y Control desde la perspectiva de estrategia, negocio, información, sistemas información y servicios tecnológicos. Para cumplir este propósito se realizaron los siguientes pasos:

Paso 1: Diseño:

- Diseño de los componentes del metamodelo (elemento que proporciona metodología y directrices para establecer la arquitectura del modelo de Vigilancia y Control).
- Diseño de los artefactos: Catálogos y Matrices.
- Diseño de las vistas: Facilitan la visualización de la arquitectura en los diferentes dominios.

Paso 2: Levantamiento de información:

Esta fase correspondió a la realización de mesas de trabajo con todos los entes que al interior de la Entidad intervienen en el ejercicio de vigilancia y control, así como la recolección de la documentación y evidencias del proceso proporcionadas por la Dirección de Vigilancia y Control y la oficina de TI.

Paso 3: Elaboración de la arquitectura actual:

Se desarrolló la documentación de arquitectura empresarial para cada uno de los dominios de estrategia, negocio, sistemas de información, información y tecnología.

3.2. FASE DE PROCESAMIENTO Y ARQUITECTURA TO-BE

El propósito de esta fase fue presentar el estado deseado del Modelo de Inspección, Vigilancia y Control desde los cinco aspectos de arquitectura empresarial.

Paso 1: Diseño:

- Selección de los marcos de referencia para los dominios de estrategia, negocio, sistemas de información, información y tecnología.





- Selección las vistas para presentar los dominios de estrategia, negocio, sistemas de información, información y tecnología.

Paso 2: Elaboración de la arquitectura objetivo:

- Elaborar la arquitectura objetivo de acuerdo con las vistas seleccionadas y los marcos de referencia.

3.3. FASE DE ANÁLISIS DE BRECHA Y PLAN DE ACCIÓN

Partiendo de los resultados obtenidos en la fase de levantamiento de información (AS- IS) y del planteamiento del estado deseado (TO – BE), esta fase proporciona las brechas existentes entre un estado y el otro y plantea las acciones que, al interior de la Entidad, la Dirección de Vigilancia y Control y la Oficina de TI deberán ejecutarse para alcanzar la meta propuesta.

Las actividades que se desarrollaron en esta fase correspondieron a:

- Análisis de brecha entre las arquitecturas empresariales AS-IS y las TO-BE en todos los dominios a partir de lo que no se tiene y se identificó como oportunidad de mejora, a través de bloques de arquitectura.
- Desarrollo del portafolio de proyectos para cerrar las brechas y definición de la priorización de los proyectos mediante el mapa de ruta o plan de acción para la instauración del nuevo Modelo de Inspección, Vigilancia y Control.





4. ESTADO ACTUAL (AS - IS) DEL MODELO DE VIGILANCIA Y CONTROL

En aras de identificar las acciones necesarias para migrar a un modelo más eficiente basado en la automatización y en el análisis de grandes volúmenes de datos (Big Data) resulta necesario contar con un punto de partida. El estado actual del modelo de inspección, vigilancia y control (AS IS) permite contar con el escenario inicial que dé luces sobre los requerimientos para migrar al estado deseado (TO BE) de dicho modelo. Para contar con la fotografía actual del modelo en los diferentes dominios, fue necesario realizar una etapa de levantamiento de información a través de entrevistas, investigación de la documentación y de los sistemas de información, entre otros.

De esta etapa es importante resaltar que el modelo actual no depende únicamente de la Dirección de Vigilancia y Control (DVC). Existen otras dependencias del MinTIC que juegan un rol muy relevante para que todo el proceso de inspección, vigilancia y control (IVC) pueda llevarse a cabo. En algunos casos las otras áreas proveen las fuentes de información a la DVC (por ejemplo, la Dirección de Industria, que administra el sistema en que se registran los prestadores de servicios), mientras en otros casos requieren de información por parte de la DVC con el fin de adelantar sus procesos (por ejemplo, el área de cartera para cobrar las sanciones impuestas a los prestadores de servicios de telecomunicaciones y servicios postales).

En la presente sección se exponen los resultados principales de este ejercicio de levantamiento de información, haciendo énfasis sobre las características más relevantes que tiene el modelo actual de vigilancia y control en los dominios de estrategia, negocio, información, sistemas de información y servicios tecnológicos.

4.1. Dominio Estrategia

En este dominio se describieron los aspectos relacionados con los planes estratégicos y la normatividad asociada al modelo de vigilancia y control. De igual forma, se identificaron los servicios institucionales relacionados, los diferentes planes de gobierno involucrados, los sectores, disposiciones de la OCDE y su alineación con el modelo actual.

La normatividad más relevante que se analizó dentro de este dominio se menciona a continuación:

- ✓ Ley 1955 de 2019, Plan Nacional de Desarrollo 2018-2022;
- ✓ Política de Gobierno Digital (Consultada a través del documento Manual de Gobierno Digital. Ministerio de Tecnologías de la Información y comunicaciones. Versión 5. agosto de 2018);
- ✓ Plan TIC 2018-2022;
- ✓ Plan Estratégico de TI (PETI) del MinTIC 2019-2023;
- ✓ Decreto 1078 de 2015, Decreto Único Reglamentario del Sector TIC.
- ✓ Ley 1978 de 2019, por la cual se moderniza el sector de las Tecnologías de la Información y las Comunicaciones (TIC), se distribuyen competencias, se crea un regulador único y se dictan otras disposiciones;
- ✓ Decreto 1414 de 2017 de MinTIC, por el cual se modifica la estructura del MinTIC y se dictan otras disposiciones y;





- ✓ Resolución 415 de 2010, por la cual se expide el Reglamento de Radiodifusión Sonora y se dictan otras disposiciones.

Respecto a los planes, se analizó la relación entre Vigilancia y Control frente a la Estrategia de Gobierno Digital (Emanada de la Política de Gobierno Digital), el Plan Nacional de Desarrollo 2018-2022, el Plan TIC 2018-2022 y el Plan Estratégico de Tecnologías de la Información (PETI) del Ministerio de Tecnologías de la Información y Comunicaciones.

Posteriormente, se procedió a analizar la madurez respecto a las directrices en materia de Gobierno Digital e Inspección, Vigilancia y Control dictaminadas por la Organización para la Cooperación y el Desarrollo Económicos (OCDE), y la identificación de los servicios del MinTIC relacionados con Vigilancia y Control. También se llevó a cabo un análisis comparativo con modelos de inspección, vigilancia y control en 10 países, a través de la metodología DOFA.

Finalmente, a través de los análisis realizados en las matrices de alineación entre el modelo de Vigilancia y Control (Cadena de Valor y carta descriptiva), contra la normatividad y planes, se identificó que las matrices de obligaciones requieren un seguimiento permanente de la legislación, regulación y jurisprudencia que se genera continuamente en materia de Inspección, Vigilancia y Control del Sector y Servicios TIC y Postales. A su vez, estas matrices se actualizan manualmente sin involucrar elementos tecnológicos.

4.2. Dominio negocio

En este dominio se abordaron las características referentes a los componentes del Metamodelo de Arquitectura del dominio de negocio. Se contempló dentro del desarrollo del Modelo de Operación (análisis de la resolución 3160 de 2017 y sus posibles modificaciones), Procesos (Cadena de Valor, Carta descriptiva, Modelo de Vigilancia y Control, Procedimientos de Vigilancia Preventiva, Investigaciones, Investigaciones Materia de Abuso Sexual Infantil -MASI- y Decomisos por operación postal clandestina y carpeta de mejora de Vigilancia y Control de la cual se extrajeron los Indicadores y Métricas del Proceso), Estructura (Estructura de gobierno y recursos), y otros recursos clave (Capacidades institucionales identificadas a través del análisis del mapa de procesos de la entidad) requeridos para desarrollar adecuadamente el modelo actual. Como parte de este ejercicio se consultó la siguiente normativa que enmarca la operación del Modelo de Vigilancia y Control:

- Resolución No. 3160 de 2017 del MinTIC. Por la cual se establece la Política Pública de Vigilancia Preventiva
- Decreto 1414 de 2017 de MinTIC. Por la cual se modifica la estructura del Ministerio de Tecnologías de la Información y las Comunicaciones y se dictan otras disposiciones, en relación con las funciones.
- Resolución 3363 de 2017. Por la cual se delegan y asignan unas funciones al interior del Ministerio de Tecnologías de la Información y las Comunicaciones y derogan las Resoluciones N° 3452, 3454 y 3093 de 2015 y 1547 de 2016
- Resolución 3132 Por la cual se modifica y adopta el manual específico de funciones y de competencias laborales para los empleos de la planta de personal del Ministerio de Tecnologías de la Información y Comunicaciones





- Proyecto de Decreto “Por el cual se modifica la estructura del Ministerio de Tecnologías de la Información y las Comunicaciones, se determinan las funciones de sus dependencias y se dictan otras disposiciones”

Para desarrollar este dominio, se emplearon matrices de alineación y concordancia (artefactos de análisis). Esto permitió establecer qué hace, cómo opera y qué resultados produce el modelo de vigilancia y control y sus oportunidades de mejora a la luz del deber ser, es decir frente a la alineación estratégica y la obtención de resultados.

Adicionalmente, se realizó la aplicación de las herramientas de análisis y mejoramiento de procesos conocidas como Evaluación de Madurez de proceso, a través del Marco de Referencia de CMMI⁷, Evaluación de Valor agregado derivado de Lean Manufacturing, medición de cargas de trabajo y productividad a través de la Metodología de rediseño Institucional del Departamento Administrativo de la Función Pública y cumplimiento de requisitos para la documentación de procesos, emanada de la Norma Técnica ISO 9001:2015.

Los resultados permitieron diagnosticar la situación actual, estableciendo el nivel de madurez de los componentes analizados en 3 dimensiones (Medición del desempeño e indicadores, procesos, roles y responsabilidades), la eficiencia actual de los procedimientos de Vigilancia y Control (a través del cálculo del índice de valor agregado del proceso), las cargas de trabajo y productividad de los procedimientos de Vigilancia y Control (Evaluación del tiempo de trabajo, productividad y tiempos estándar de procesos).

El marco de referencia para desarrollar el análisis de este dominio es la cadena de valor del proceso de vigilancia y control, la cual se evidencia en la siguiente figura:

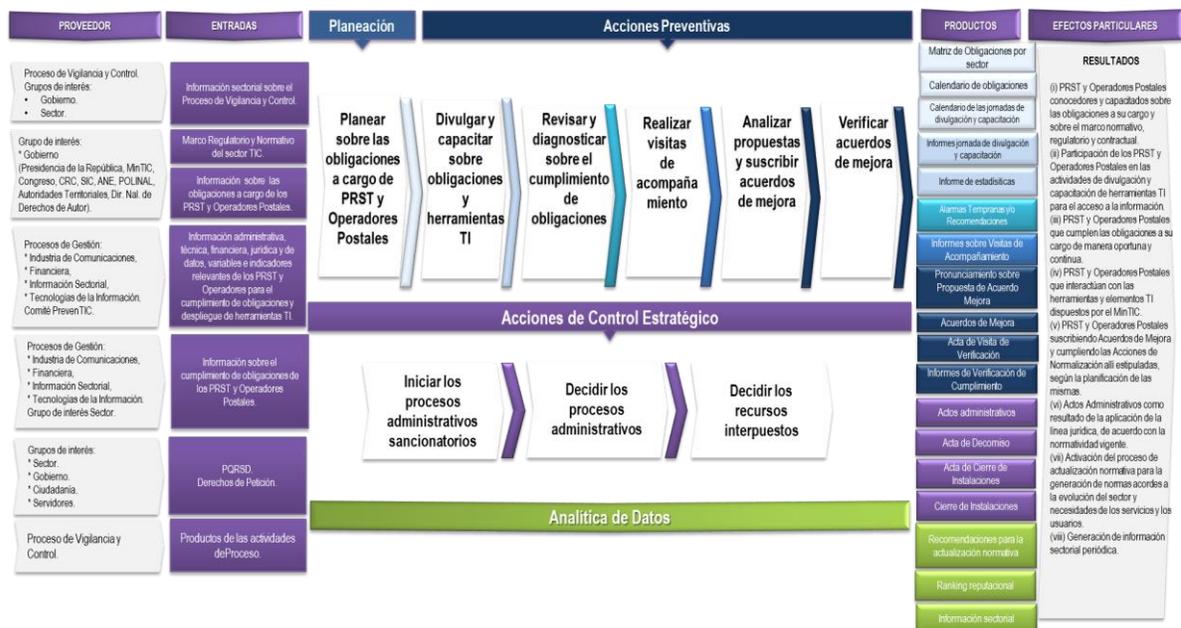


Ilustración 2. Cadena de Valor de Vigilancia y Control AS-IS

Fuente: VYC-TIC-CV-001 Cadena de Valor Proceso Vigilancia y Control. Versión 3. MinTIC

⁷ Capability Maturity Model Integration





Adicionalmente, se tienen en cuenta la carta descriptiva, que constituye un documento en el que se desarrolla cada uno de los aspectos de la cadena de valor y de los procedimientos con los que cuenta el proceso de vigilancia y control. Finalmente, un tercer elemento relevante que constituye un marco de referencia para entender el paso a paso de las labores de inspección, vigilancia y control que adelanta el MinTIC es el documento que describe el Modelo de Vigilancia y Control actual.

A partir del análisis realizado sobre este dominio, los principales resultados son:

- Se recomienda realizar una reingeniería al proceso actual de Vigilancia y Control, que modifique las acciones establecidas en la Resolución 3160 de 2017 y permita generar un mayor impacto en términos de efectividad del proceso.
- En el supuesto que se modifique la Resolución No. 3160 de 2017, se debe actualizar el Modelo de Vigilancia y Control para que se encuentre alineado con esta modificación. Los resultados en materia de cumplimiento de las acciones de mejora, las actividades definidas en la Resolución 3160 de 2017 que permiten la discrecionalidad en la determinación de sanciones y el reconocimiento diferencial o incentivos generado por el cumplimiento de las obligaciones legales y regulatorias, evidencian la necesidad de modificar el proceso de Vigilancia y Control actual.
- La documentación principal del proceso, la Cadena de Valor, la Carta descriptiva y el Modelo de Vigilancia y Control no están alineadas entre sí, toda vez que en la Carta Descriptiva se enuncian entradas, proveedores, actividades, salidas y clientes del proceso que no corresponden en su totalidad a lo definido en la Cadena de Valor de Vigilancia y Control, y la Carta Descriptiva.
- Al no evidenciarse actividades de Planeación y Analítica de Datos se generan inconsistencias frente las definiciones del deber ser del proceso definidas en la Cadena de Valor, Carta Descriptiva y Modelo de Vigilancia y Control.
- La documentación operativa del proceso⁸ no refleja en su totalidad la realidad de la operación desarrollada, toda vez que existen actividades que no generan valor. También fue posible identificar ausencia de documentación de actividades críticas para su desarrollo, ausencia de formatos y registros con información relevante para hacer seguimiento al desempeño del proceso, desarticulación entre las entradas y salidas, inexistencia de la secuencialidad e interacción entre los procedimientos y con procesos del ministerio en algunos casos. El alcance de los procedimientos no contempla el servicio de televisión. Finalmente, no se evidencia un enfoque de riesgos y de un modelo predictivo y preventivo de acuerdo con las mejores prácticas de otros países y recomendaciones de la OCDE.

Finalmente, uno de los resultados más importantes del levantamiento de información en los dominios de estrategia y negocio consiste en que se encuentran múltiples definiciones de sector TIC, servicios y obligaciones. Esto tiene un impacto sobre los sistemas de información, en tanto los diferentes sistemas se basan en diferentes definiciones, y esto dificulta la interoperabilidad entre ellos.

⁸ Los procedimientos de Investigaciones, Vigilancia Preventiva, Decomisos por Operación Postal Clandestina, Investigaciones Material de Abuso Sexual Infantil – MASI y sus respectivos formatos: Formato de responsabilidad acto de pruebas, Formato de responsabilidad apertura, Formato de responsabilidad recurso repo, Formato de responsabilidad sanción.





4.3. Dominio Información

En este dominio, primero se realizó un catálogo de entidades de información y, posteriormente, un análisis de la alineación de los sistemas y procesos actuales. De este análisis se encontró que existen múltiples repositorios de almacenamiento de información sin que entre ellos exista una interconexión. De igual forma se evidenció que no cuentan con diseños uniformes, con desarrollos incipientes para evaluar su calidad. Tampoco existe información suficiente sobre su estructura en algunos casos y se encontró que existe información del proceso de Vigilancia y Control que no se está almacenando en ningún repositorio. Esto supone retos en materia de seguridad de la información. A continuación, se resume el resultado del análisis de madurez de la información:

Metadatos: Nivel 2 Desarrollo: Ninguno de los sistemas contiene información incrustada como metadatos descriptivos dentro de los modelos de datos. Sin embargo, existen diagramas de entidad, relación y diccionario de datos de algunos sistemas. No hay un repositorio único de metadatos y tampoco hay indicadores sobre el estado de los metadatos.

Datos Maestros: Nivel 2 Desarrollo: existen un sin número de datos que deberían tener un repositorio maestro, ya que se utilizan en todo el proceso. Sin embargo, actualmente, se encuentran duplicados y con diferentes estructuras y datos en diferentes bases de datos. Por otra parte, tienen desplegado un MDM⁹ pero en este momento solo se aplica para un dato maestro. No hay indicadores sobre los datos maestros.

Datos Operacionales Estructurados: Nivel 3 Práctica: la mayoría de los datos se encuentran en repositorios estructurados, sin embargo, gran parte de los datos contiene falencias de optimización, como, por ejemplo: fallas en la mnemotecnia de los campos o las tablas, fallas en la asignación de tipo y tamaño de los campos, y fallas en la separación de los almacenamientos, lo que en algunos casos impide una obtención de datos eficiente. Finalmente, existe información de carácter estructurada que no está siendo almacenada y no existen indicadores sobre el uso o sobre los datos estructurados.

Datos Operacionales No Estructurados: Nivel 3 Práctica: existen repositorios de datos no estructurados en más de un proceso en almacenes diferentes. Algunos vinculan los datos de un repositorio estructurado con un archivo en un repositorio, otros, utilizan repositorios NoSQL para el almacenamiento. En estos dos tipos de procesos, se obtiene información de los datos no estructurados. Algunos archivos usados en el proceso no están siendo almacenados. No existe un repositorio único y no hay indicadores sobre los datos no estructurados.

Datos Analíticos: Nivel 1 Conciencia: tienen sistemas de reportes y presentación de indicadores, pero estos no se presentan automáticamente, la cantidad de indicadores no refleja la capacidad del proceso de generar información para la toma de decisiones y no existen indicadores sobre la información en sí misma.

Estos resultados se presentan de manera gráfica en la siguiente ilustración:

⁹ *Master Data Management*. Es la metodología que permite gestionar el conjunto de estos datos maestros de forma que no haya inconsistencias entre ellos.



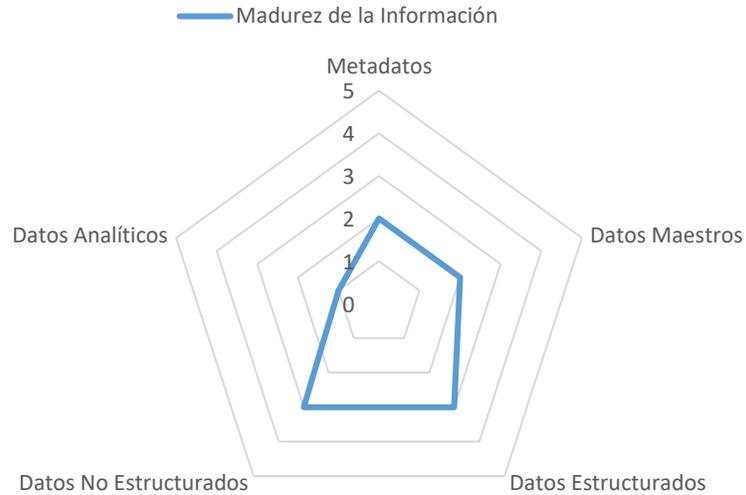


Ilustración 3. Madurez de los pilares de la información actual
Fuente: UT Bisa Grow, 2020.



4.4. Dominio Sistemas de Información

Para este dominio se elaboró un diagrama con los sistemas de información que actualmente soportan el modelo de Vigilancia y Control, donde se describen las actividades de la cadena de valor alineados a los procedimientos. También se presentan los procedimientos de los procesos de Vigilancia y Control alineados a los sistemas de información sobre los cuales se soportan. Los sistemas de información se encuentran pintados de color rosado. Las flechas indican qué procedimiento hace uso de un determinado sistema de información.

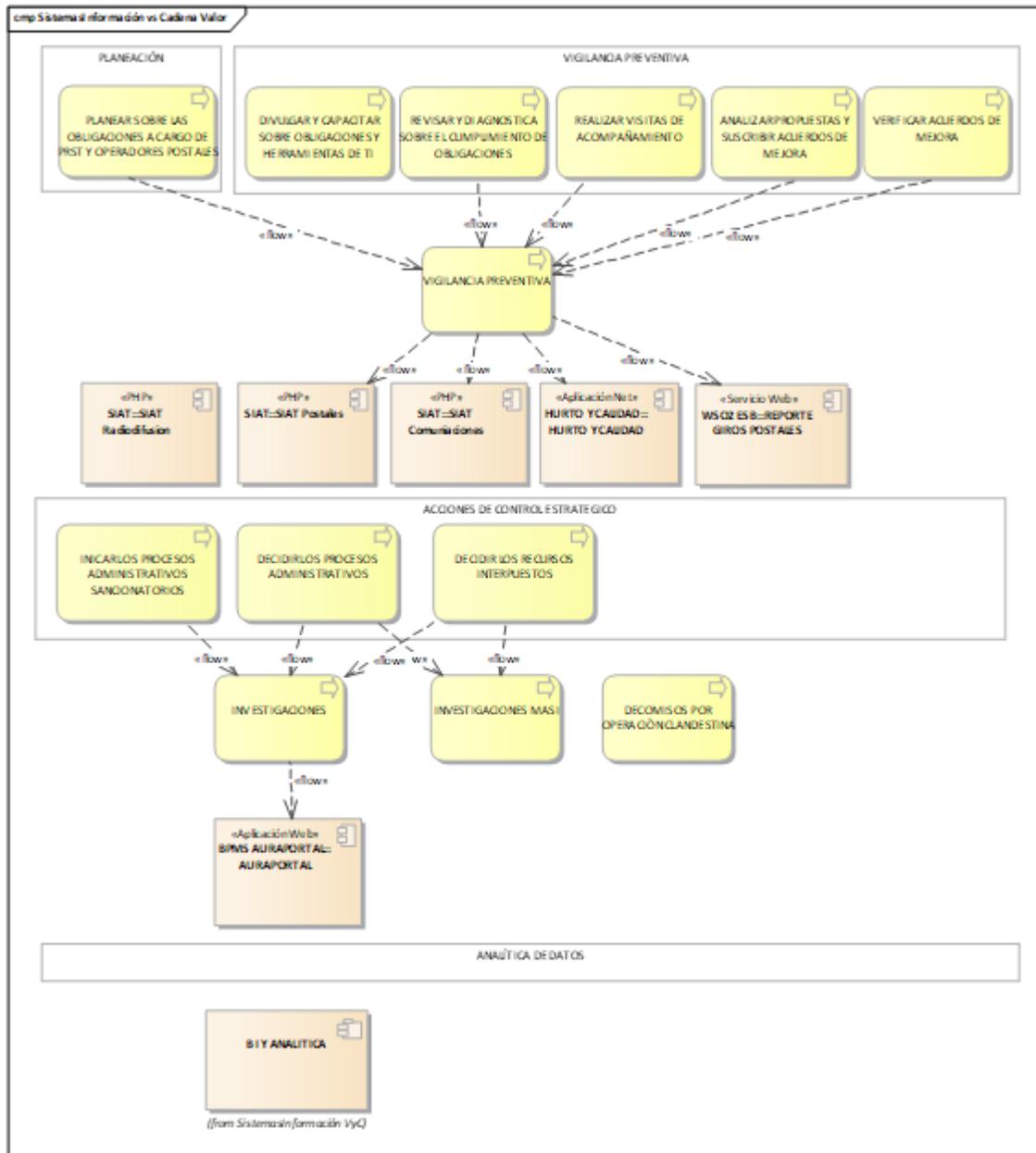


Ilustración 4. Diagrama de sistemas de información Vs. procedimientos.

Fuente: UT Bisa Grow, 2020.

De acuerdo con la ilustración anterior se identificó que:

- Los Sistemas de Información de Alertas Tempranas (SIAT) cumplen la funcionalidad de un repositorio de información y al alimentarse con información de las visitas en campo, generan alertas ex post y no ex ante.
- Los procedimientos de Investigaciones sobre Material de Abuso Sexual Infantil (MASI) y Decomisos no cuentan con soporte de ningún sistema de información.
- Existen herramientas de analítica e inteligencia de negocio, pero no se cuenta con un procedimiento que soporte actividades de analítica de datos en el Modelo Integrado de Gestión (MIG).

Se detectó durante la fase de levantamiento que los sistemas de información que soportan el proceso de vigilancia y control no son los únicos involucrados en el proceso. En efecto, se detectaron los siguientes sistemas de información que almacenan información relevante para el proceso de vigilancia y control, los cuales se exponen en la siguiente figura agrupados según los procesos del MIG de MinTIC:

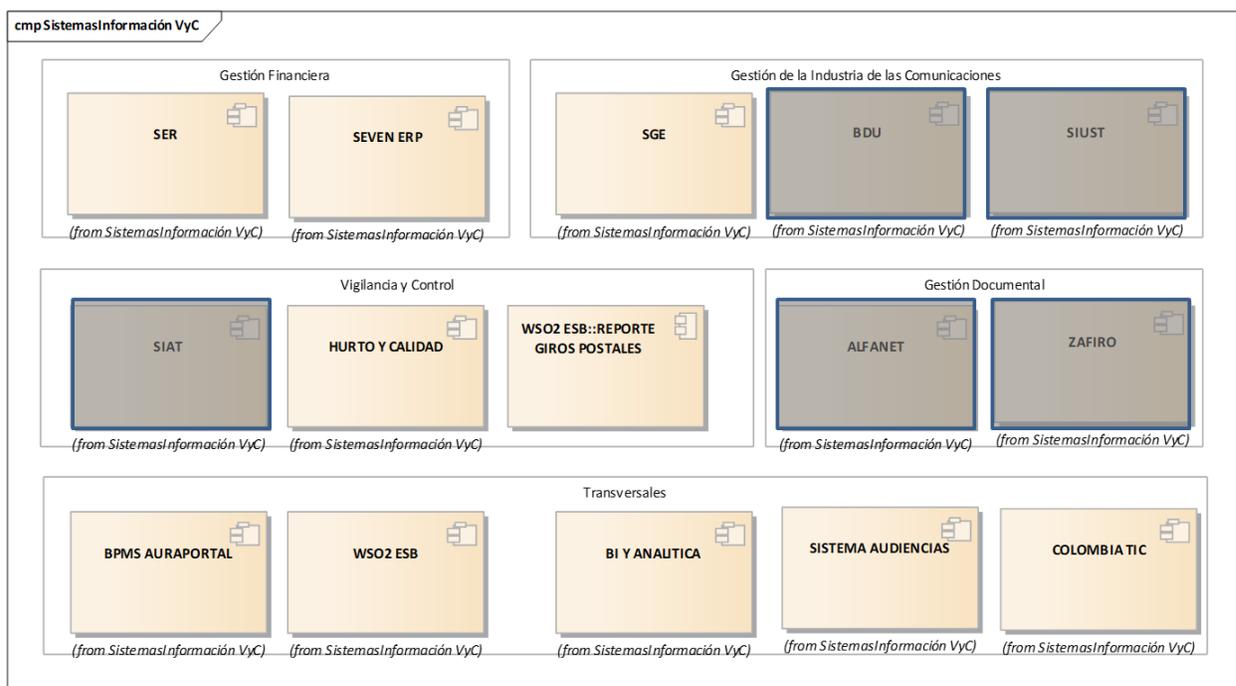


Ilustración 5. Sistemas de información alineados a los procesos MinTIC

Fuente: UT Bisa Grow, 2020.

Se desarrolló el diagnóstico de mantenibilidad¹⁰ de los sistemas de información del proceso de Vigilancia y Control y sistemas de información relevantes para el proceso. Para los sistemas de información que aparecen en la ilustración anterior sombreados en color gris se recomienda evaluar su posible remoción del MinTIC, por su baja mantenibilidad. Es preciso aclarar que si bien el Sistema de Información Unificado para el Sector de las

¹⁰ Mantenibilidad: *Esta característica representa la capacidad del producto software para ser modificado efectiva y eficientemente, debido a necesidades evolutivas, correctivas o perfectivas.* Recuperado de: <https://iso25000.com/index.php/normas-iso-25000/iso-25010/26-mantenibilidad>



TIC (SIUST) aparece sombreado, el sistema de información HECCA que es el que soporta actualmente las obligaciones de reporte de información por parte de los vigilados no desaparece en la propuesta del estado deseado del Modelo de Inspección, Vigilancia y Control (TO – BE). De igual forma, esta propuesta se planteó siguiendo los lineamientos de la Oficina de TI del MinTIC.

A continuación, se presenta una breve descripción del catálogo de sistemas de información involucrados en el proceso de Vigilancia y Control:

Sistema Información	Descripción
SER	Sistema Electrónico de Recaudo (SER): sistema de información para el pago electrónico de obligaciones financieras de los Clientes - Operadores de servicios de telecomunicaciones.
Seven ERP	El Planeador de Recursos Empresariales o en inglés Enterprise Resource Planning (ERP): Sistema para gerenciar eficientemente las necesidades en las áreas Administrativas, Financieras, Comerciales, Manufactura y Recursos Humanos de las organizaciones.
AuraPortal	Sistema de información donde se ejecutan los procesos de negocio de MinTIC.
Alfanet	Gestor documental de MinTIC. El sistema Alfa® se concibió como un Desarrollo lógico que permitía radicar documentos recibidos, registrar documentos enviados, realizar trámites, gestión, archivo y consulta.
Zafiro	Gestor documental de MinTIC.
BDU Plus	Base de datos Única (BDU). Sistema de información para hacer la liquidación de derechos, administrar la información técnica, y en general, controlar todos los datos relacionados con los clientes y sus expedientes dentro de la institución.
SIAT	Sistema de información de alarmas tempranas, existen tres SIAT: <ul style="list-style-type: none"> ● SIAT Radiodifusión. ● SIAT Comunicaciones. ● SIAT Postales.
SIUST	Sistema de Información Unificado del Sector de Telecomunicaciones - SIUST por medio del cual se permite la captura de los reportes de información de los proveedores de redes y/o servicios de telecomunicaciones y operadores postales.
Hurto y Calidad	Sistema para que los operadores reporten la información relacionada con el hurto de celulares en Colombia y de la calidad de los servicios de telefonía móvil.
SGE	El Sistema de Gestión de Espectro - permite realizar la gestión, análisis, administración y planeación del espectro radioeléctrico.
SGE Front Office	Componente WEB desarrollado por MinTIC para habilitar las funcionalidades de SGE en web. También permite la comunicación del sistema SGE mediante servicios WEB.
WSO2	Bus de servicios empresariales MinTIC, componente de software que habilita la capacidad de integración e interoperabilidad entre los sistemas de información.
Colombia TIC	Colombia TIC es el Sistema de información Integral con los datos, variables e indicadores relevantes, sobre el sector de las Tecnologías de la Información y las Comunicaciones, que facilita la fijación de metas, estrategias, programas y proyectos para su desarrollo.





BI Y ANALÍTICA	<p>Los sistemas de información que se usan para el desarrollo de inteligencia de negocio y analítica, en MinTIC se cuentan con los siguientes sistemas:</p> <ul style="list-style-type: none"> ● IBM SPSS o IBM Statistical Package for the Social Sciences: Ofrece análisis estadístico avanzado, una vasta biblioteca de algoritmos de machine learning, análisis de texto, extensibilidad de código abierto, integración con big data e implementación continua en las aplicaciones. ● POWER BI: Solución de análisis empresarial que permite visualizar los datos y compartir información con toda la organización, o insertarla en su aplicación o sitio web. ● SQL REPORTING SERVICES: Es un subsistema de SQL Server que permite la creación de informes gráficos, móviles e impresos utilizando SQL Server y otras fuentes de datos.
WSO2 ESB: REPORTE GIROS POSTALES PAGOS	<p>Es un servicio web que se expone por medio del ESB WSO2 para recibir de los operadores postales, el reporte de los giros postales de pago que se transan por medio de sus aplicaciones, esta información se procesa por medio de los funcionarios de Vigilancia y Control y se convierte en insumo para planear la vigilancia de los operadores postales.</p>
SQL SERVER MDM	<p>Base de datos para la gestión de datos maestros, actualmente se encuentra implementada sobre SQL SERVER y es la iniciativa de MinTIC como repositorio central de datos.</p>

Tabla 3. Descripción Sistemas de información

Fuente: UT Bisa Grow, 2020.

Como resultados principales del estado actual en este dominio se presentan los siguientes:

- *Alfanet y Zafiro*: Estos sistemas de información de gestión documental, se encuentran en el mapa de ruta de proyectos de la Oficina de Tecnologías de la Información del MinTIC marcados para ser reemplazados por un nuevo gestor documental llamado AZDIGITAL. Este nuevo sistema contará con firmas y estampados digitales sobre los documentos y fue contemplado en el diseño del TO BE.
- *BDU*: El sistema de información BDU, se planteó como candidato para su remoción o disposición final. Como oportunidad se plantea un nuevo diseño en el documento del TO BE.
- *BPMS*: El uso del BPMS Aura Portal es un lineamiento de la oficina de TI del MinTIC. Este sistema fue contemplado para el diseño de procesos automatizados en el diseño del estado deseado o TO BE.
- *BI y Analítica*: Existen tres herramientas para realizar analítica y reportes, que son IBM SPSS, POWER BI y Reporting Services. Sin embargo, no existen procesos o procedimientos en la cadena valor del proceso de vigilancia y control donde se asignen actividades de analítica de datos, por lo tanto, los resultados del uso no se controlan a través de los procedimientos actualmente establecidos. Todas las herramientas con las que cuenta MinTIC para BI y analítica fueron tenidas en cuenta para el diseño de los sistemas de información en el estado deseado o TO BE.
- *Hurto y Calidad*: El sistema de información Hurto y Calidad, se planteó como candidato para continuar en producción en MinTIC y, por tanto, fue considerado para el diseño del TO BE.
- *SIAT¹¹ Comunicaciones, Radiodifusión y Postales*: teniendo en cuenta el uso actual que se está dando a estos sistemas de información y la evaluación de mantenibilidad, se plantearon como candidatos para su reemplazo. Como oportunidad se planteó un nuevo diseño en el documento del TO BE.

¹¹ *Sistema de Información de Alertas Tempranas.*





- *SIUST*: El sistema de información SIUST, se planteó como candidato para su remoción. Como oportunidad se plantea un nuevo diseño en el documento del TO BE. La herramienta HECCA, que forma parte de este sistema, se mantiene y se puede usar en creación de formularios, servicios web o cargue de documentación. Actualmente, solo se usa la opción de cargue de documentación. Los lineamientos que se recibieron por parte de la oficina de TI son que este componente sea mantenido para las obligaciones relacionadas con reporte de información por parte de los operadores. Se contemplaron dichas funcionalidades y lineamientos en el diseño del TO BE del presente proyecto.
- *Sistema de información versus servicios de TV*: Con ocasión de la expedición de la Ley 1978 de 2019, expedida recientemente, se asignaron las facultades de inspección, vigilancia y control del servicio de televisión al MinTIC. Sin embargo, no se encontró ningún sistema de información donde repose dicha información histórica y/o actual del sector. Actualmente se está adelantando la migración de esta información y se tienen en cuenta dichos servicios para el diseño del TO BE.
- *SEVEN*: El sistema de información SEVEN, se identificó como uno de los sistemas con el que se debe continuar. Por tal razón fue considerado para el diseño del TO BE.
- *SER*: El sistema de información SER, se identificó como uno de los sistemas con el que se debe continuar. Por tal razón fue considerado para el diseño del TO BE.
- *SGE*: El sistema de información SGE, se identificó como uno de los sistemas con el que se debe continuar. Por tal razón fue considerado para el diseño del TO BE.
- *WS02*: Bus de servicios empresariales de MinTIC, componente para integrar los sistemas de información de MinTIC y el desarrollo de la interoperabilidad. Su uso apalancado en la estrategia de arquitectura orientada por servicios es un lineamiento entregado por la oficina de TI y fue considerado en el diseño del TO BE.

4.5. Dominio Servicios Tecnológicos

En este dominio se revisó la infraestructura tecnológica existente que soporta los sistemas de información o fuentes de información en el proceso de vigilancia y control. Se hizo un recuento de los servidores, sus características y capacidades, evaluando:

- TIPOS DE SISTEMA OPERACIONAL EMPLEADO
- AMBIENTES DE PRUEBA
- UBICACIÓN DE LOS SERVIDORES
- AMBIENTE VIRTUALIZADO

En la siguiente ilustración se presentan los sistemas que soportan los procesos de vigilancia y control. Sobre estos sistemas se realizó un análisis, en cuanto a la infraestructura actual, con el fin de evidenciar las oportunidades de mejora en materia de disponibilidad, confidencialidad e integridad de la información con el fin de evitar modificaciones no autorizadas de la misma.

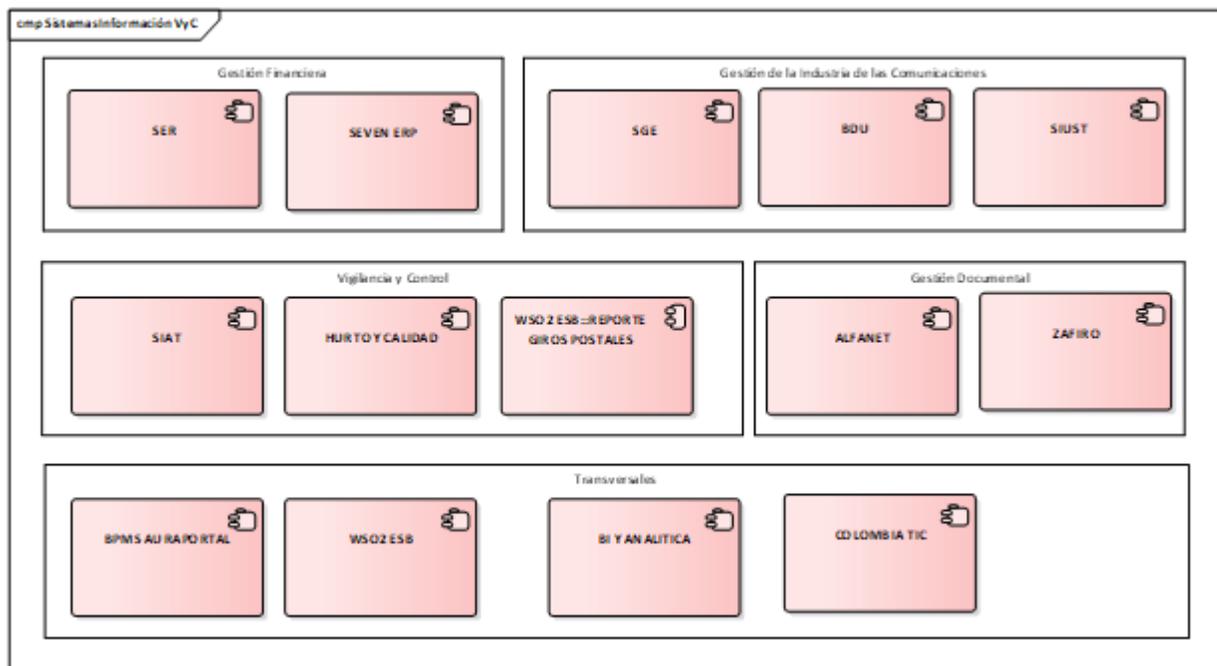


Ilustración 6. Sistemas de información que interactúan o son fuente de información en el proceso de Vigilancia y Control
Fuente: UT Bisa Grow, 2020.

Tipos de Sistemas Operacionales Empleados

El propósito del análisis realizado era contar con elementos que permitieran determinar inversiones en licenciamiento actuales y contribuir en la toma de decisiones, como lo son costos de implementación de futuros sistemas de la Dirección de Vigilancia y Control, así como la actualización requerida ante una culminación del periodo de soporte del fabricante. De acuerdo con esta información, se realizó el análisis correspondiente, identificando necesidades de actualización de los sistemas de información y sistemas operativos.

Ambiente de prueba

Los ambientes de prueba son de gran importancia para la realización de ajustes, atención de incidentes y nuevos desarrollos que se estén realizando o sea requeridos. Dentro de la información que se suministró se evidenció que algunos sistemas no cuentan con ambiente de pruebas, lo cual es de suma importancia para desarrollos, ajustes e incidentes que se requiera probar, en lo posible con infraestructura igual o similar a los de producción. En la siguiente ilustración se presenta el análisis realizado:

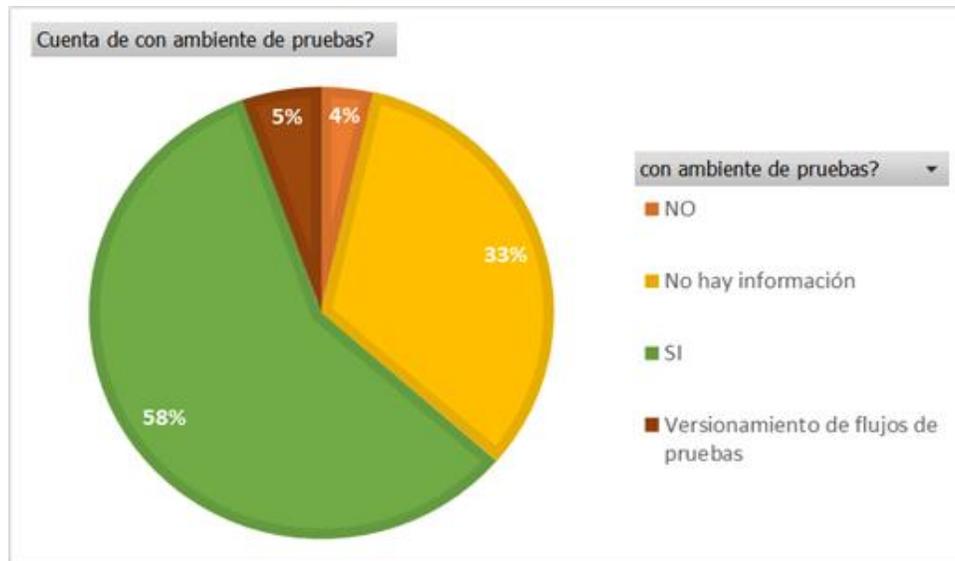


Ilustración 7. Ambientes de pruebas

Fuente: UT Bisa Grow, 2020.

Sin embargo, los ambientes de pruebas se implementan a discreción del MinTIC en el momento de desarrollar o actualizar los sistemas de información.

Ambiente virtualizado

Los ambientes virtualizados son de gran ayuda por cuanto permiten aumentar la disponibilidad de los sistemas, minimiza costos de infraestructura, permitiendo entre otras cosas crear ambientes de prueba similar al de producción, maximizando los recursos para soportar los diferentes sistemas de información disponibles para la Dirección de Vigilancia y Control. El desplegar los sistemas en servidores virtualizados funcionará correctamente, siempre que se cuente con hardware de características requeridas según análisis periódico de capacidad. La distribución actual de ambientes virtualizados en comparación de sistemas que hacen uso físico de la máquina es de 89% y 11%, respectivamente.

De acuerdo con la anterior información, acerca de la infraestructura que soporta los sistemas de información que apoyan al proceso de vigilancia y control, se identificó que:

- Actualmente, las aplicaciones se encuentran alojadas en servidores que se localizan en las instalaciones de MinTIC que, si bien cuentan con alta disponibilidad, se aconseja estén alojadas en un datacenter especializado fuera de la entidad en esquema redundante, por cuanto esto:
 - Brinda mayor seguridad, permitiendo resguardar los datos ante robo o pérdida de información o ante daño de servidores, contando con elementos de hardware y software especializado ante cualquier ataque cibernético.
 - Brinda respaldo a todo nivel de la información en diferentes ubicaciones, con lo cual se anula cualquier pérdida de información. Si bien actualmente MinTIC cuenta con respaldo de información en diferentes medios como son cinta, nube y otros dispositivos de



almacenamiento, mediante el software Veeam Backup y otros mecanismos, se aconseja dejar esta tarea en centros de datos, que se encarguen de dicha actividad.

- Alojarse la información en un datacenter permite que los sistemas de información de la Entidad presenten un uso permanente, es decir alta disponibilidad, sin que existan caídas de los mismos por inconvenientes de infraestructura. Si bien MinTIC cuenta con sistemas en alta disponibilidad, un centro de datos brindará los elementos necesarios para escalar las aplicaciones ante incrementos en el uso de los servicios por parte de los diferentes usuarios.
- Los datacenter por ser centros especializados en dichas tecnologías, brindan soporte sobre las diferentes plataformas tecnológicas con las que cuenta MinTIC.
- Brinda servicio de Internet y dispositivos de alta disponibilidad, lo cual garantiza la continuidad de los servicios de la Dirección de Vigilancia y Control de MinTIC. Lo anterior por cuanto a la infraestructura se refiere. Hay diferentes elementos que pueden llegar a fallar ocasionando indisposición de los sistemas, con lo cual un centro de datos brinda sistemas redundantes que garantizan la continuidad de la operación.

4.6. Resumen resultados estado actual

Con el análisis del estado actual del modelo de vigilancia y control en cada uno de los dominios, se destacan los siguientes resultados sobre los cuales se plantearán mejoras en el estado deseado TO BE:

Estrategia:

- No hay una única definición de sector TIC y de los servicios que lo componen. Hay varias definiciones en normativas, páginas web, sistemas de información y esto dificulta el tener claridad sobre el objeto de inspección, vigilancia y control. Adicionalmente la normativa es en algunos casos compleja y está dispersa en distintas fuentes.
- Modelo actual con enfoque reactivo y no preventivo. Esto se corregirá en el estado deseado al migrar a un enfoque basado en riesgos y que contiene la implementación de una estrategia de alto impacto en materia de divulgación normativa. Lo anterior en aras de prevenir el incumplimiento por desconocimiento.
- Se requiere tener una articulación permanente con otras entidades como la Superintendencia de Industria y Comercio, la Comisión de Regulación de Comunicaciones y la Agencia Nacional del Espectro.

Negocio:

- El modelo de vigilancia y control actual se estableció en 2012 y se encuentra desactualizado, sobre todo si se tiene en cuenta normativa reciente como las Leyes 1955 y 1978 de 2019.
- Algunos procedimientos no se encuentran alineados con las funciones del Decreto 1414 de 2017.
- No están documentadas algunas interacciones entre procedimientos y hay diferencias entre la operación y la documentación. Esto se solventa en la propuesta del estado deseado TO BE.
- Hay algunos procedimientos particulares que no aplican para los vigilados de todos los sectores.
- Las matrices de obligaciones no están diseñadas bajo un enfoque de gestión de riesgos y se actualizan de forma manual.





Información:

- Múltiples sistemas de información con datos replicados y sin interconectar.
- Se planteará en el TO BE la forma de lograr una mayor alineación entre las tablas de retención documental (TRD) y el proceso actual.
- Almacenamiento de información no estructurada en algunos casos (ej. Datos no estructurados como pdf).
- Falta de herramientas y procesos de Big Data.
- Los operadores no pueden acceder a su propia información para autorregularse. Este es uno de los puntos clave del estado deseado del nuevo modelo que se plantea en la siguiente sección.

Sistemas de información:

- La no claridad en la definición de sectores TIC, servicios TIC y postales, se ve reflejado en el diseño de los sistemas de información.
- Existen tres herramientas para generar BI y Analítica en MinTIC, sin embargo, no existen procesos en la cadena valor del proceso de Vigilancia y Control donde se asignen actividades de analítica.
- Los sistemas que actualmente son expuestos hacia el operador, no se encuentran homogenizados en su presentación gráfica.
- No se dispone de interoperabilidad entre algunos sistemas.

Servicios tecnológicos:

- Algunos de los sistemas operativos deben ser actualizados y, en los casos en que se requiera, se deberán ejecutar los ambientes de pruebas cuando se desarrollen o actualicen los sistemas de información.
- Todos los diseños de los nuevos sistemas de información en el estado deseado TO BE se alinearán con lineamientos de nuevas tecnologías.

5. ARQUITECTURA OBJETIVO (TO-BE)

De acuerdo con lo analizado en la sección anterior y con base en el planteamiento de la Dirección de Vigilancia y Control del Ministerio TIC de contar con un modelo de Inspección, Vigilancia y Control preventivo y predictivo que contribuya al fortalecimiento del ejercicio de sus funciones y proporcione a los prestadores de servicios de telecomunicaciones y servicios postales herramientas que les permitan monitorear el estado de cumplimiento de sus obligaciones, la presente sección suministra la propuesta de un nuevo modelo cuyo enfoque mantiene los lineamientos de Arquitectura Empresarial definidos por el Ministerio TIC.

Dicho lo anterior, a continuación, se presenta la propuesta desarrollada para los dominios de Estrategia, Negocio, Información, Sistemas de Información y Servicios Tecnológicos.





5.1. DOMINIO ESTRATEGIA

De acuerdo con los análisis realizados a la Guía de la OCDE para el cumplimiento regulatorio y las inspecciones, Plan Nacional de Desarrollo 2018-2022 “Pacto por Colombia, Pacto por la Equidad”, Ley 1955 de 2019 que expide el Plan Nacional de Desarrollo, plan TIC 2018-2022 “El Futuro Digital es de Todos”, el Plan Estratégico de Tecnologías de Información (PETI) de MinTIC 2019 - 2023 y la Política de Gobierno Digital, la Ilustración 8 muestra la relación que el Modelo de Inspección, Vigilancia y Control con cada uno de los planes y normatividad deberá tener para cumplir eficientemente los objetivos propuestos:

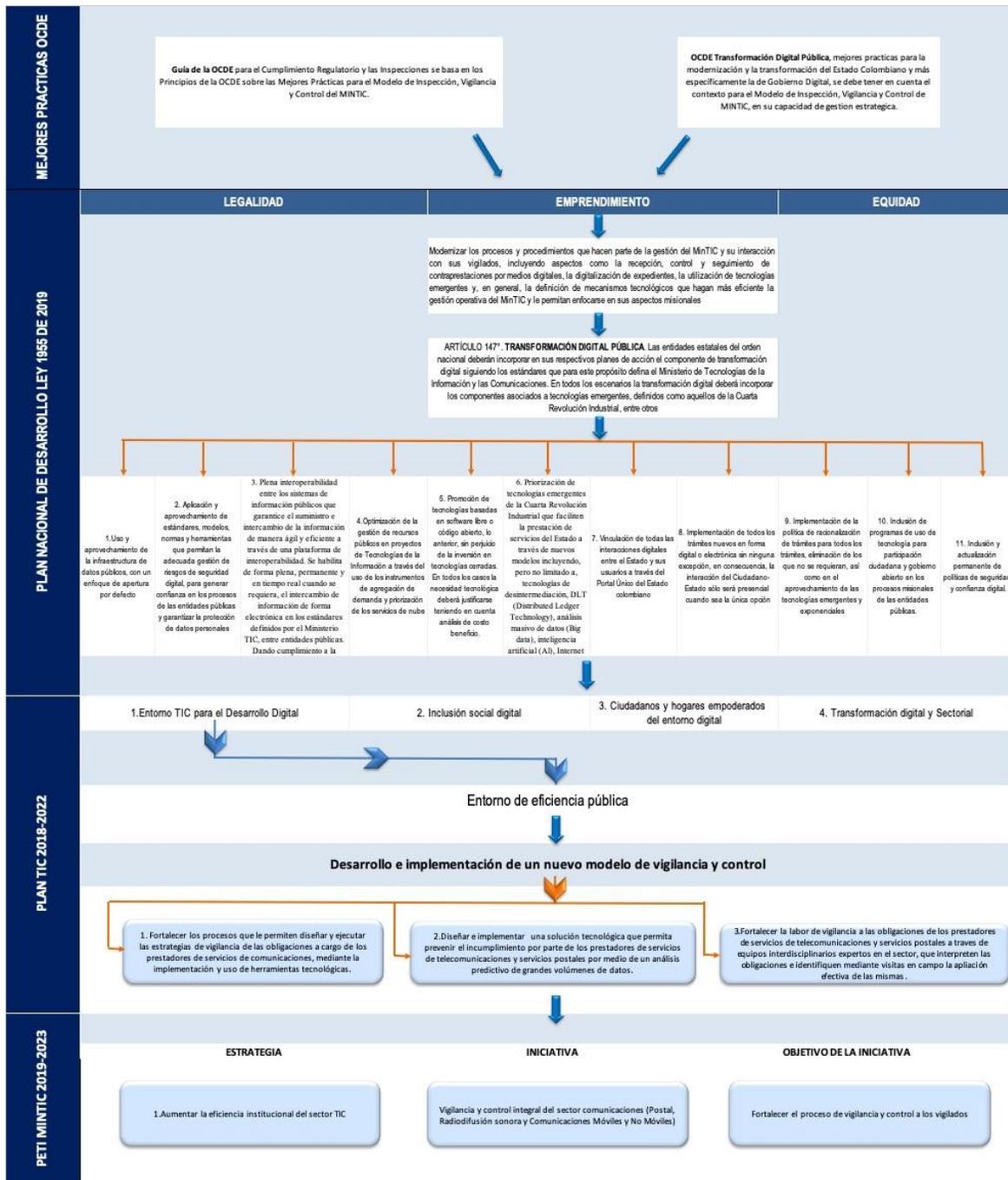


Ilustración 8. Relación entre planes, normatividad y modelo de Vigilancia y Control

Fuente: Contrato de Consultoría 837 de 2019 - Dirección de Vigilancia y Control

En cuanto a las matrices de obligaciones elaboradas por la Dirección de Vigilancia y Control para el seguimiento de las obligaciones de los prestadores de servicios de telecomunicaciones (móviles, no móviles, radiodifusión sonora y televisión) y servicios postales, el resultado del diagnóstico arroja que éstas se constituyen como un elemento indispensable en el ejercicio de inspección y vigilancia. Sin embargo, pese a que existe una labor de consolidación de unos formatos que resumen todas las obligaciones, éste no es el mecanismo idóneo para





administrar la información de interés tanto de los operadores como de quienes desarrollan las actividades de inspección, vigilancia y control. Lo anterior, teniendo en cuenta que la estructura, la cual es diferente para cada sector, dificulta su lectura y entendimiento. Por lo tanto, se plantea la necesidad de una reestructuración de los mencionados instrumentos.

Dicho lo anterior y con base en el análisis de los criterios de pertinencia, vigencia, eficiencia e idoneidad realizado para cada una de las matrices de obligaciones, éstas deberán elaborarse en un formato que permita el intercambio de datos o consulta de otros sistemas de información. Esto con el fin de que las matrices reciban informes de otras fuentes que permitan su actualización de forma permanente, pues en la actualidad, ésta se lleva a cabo de forma manual.

La propuesta para la automatización de las matrices de obligaciones consiste en que se integre la información de sector TIC, servicios, obligaciones y formatos de reporte de obligaciones en una sola base de datos, para que todos los sistemas de información del Ministerio hagan uso de esa base de datos unificada.

Ahora, en lo que respecta a la planeación de las visitas, el diagnóstico arroja que según la aplicación del modelo actual no se siguen los criterios de riesgo como lo plantea el manual de buenas prácticas de la OCDE. En la actualidad no existen criterios de priorización reglamentados por el Ministerio que sigan el principio de enfoque de riesgos. Por ello, es necesario incluir procedimientos en el nuevo proceso de Inspección, Vigilancia y Control (IVC) para cumplir con el enfoque basado en riesgos propuesto por la OCDE.

La actualización, así como la elaboración y revisión de las cinco matrices (móvil, no móvil, radiodifusión sonora, televisión y postal), debería hacerse a través de una metodología única, bajo criterios y estándares unificados. Igualmente, ante la cantidad de obligaciones y operadores, es recomendable establecer un enfoque de riesgo para priorizar las visitas de aquellas obligaciones y/u operadores clasificados como de riesgo alto, aleatorias para los de riesgo medio e implementar un mecanismo de autorregulación para los de riesgo bajo.

El enfoque de riesgo permitiría direccionar las funciones de inspección, vigilancia y control para aquellas obligaciones u operadores con mayor riesgo de incumplimiento (teniendo en cuenta la cantidad de operadores e infracciones y el impacto de la obligación que se incumple, entre otros) y llevar a cabo actividades de prevención para este tipo de riesgos.

Sobre el particular la OCDE señala también como uno de los principios sobre las mejores prácticas, lo siguiente: “Las tecnologías de la información y la comunicación deben utilizarse para maximizar el enfoque en los riesgos, promover la coordinación y el intercambio de información a fin de garantizar el uso óptimo de los recursos” (OCDE, 2014).

Ahora bien, con el fin de implementar un enfoque de riesgos para la verificación del cumplimiento de las obligaciones por parte de los prestadores de servicios, es necesario procesar la información que posee el Ministerio TIC sobre la labor que realizan los consultores externos y/o los colaboradores del Ministerio en materia de inspección y vigilancia. En síntesis, deben consolidarse y procesarse todos los datos que le permitan a la entidad generar una matriz de riesgo, considerando que el factor de riesgo a mitigar es el incumplimiento de las obligaciones.

5.2. DOMINIO NEGOCIO

Para desarrollar una nueva Arquitectura de Negocio, teniendo en cuenta las oportunidades de mejora identificadas del estado actual de Vigilancia y Control, se plantea un nuevo modelo basado en el ciclo de mejora continua de Planeación, Inspección, Vigilancia y Control dónde los recursos clave corresponden al uso de tecnologías de la información, uso eficiente y oportuno de la información, aplicación efectiva de las normas y cumplimiento de las estrategias institucionales, cuyo foco central son los prestadores de servicios de telecomunicaciones y servicios postales.

La siguiente ilustración representa el ciclo propuesto en el Nuevo Modelo de Inspección, Vigilancia y Control:

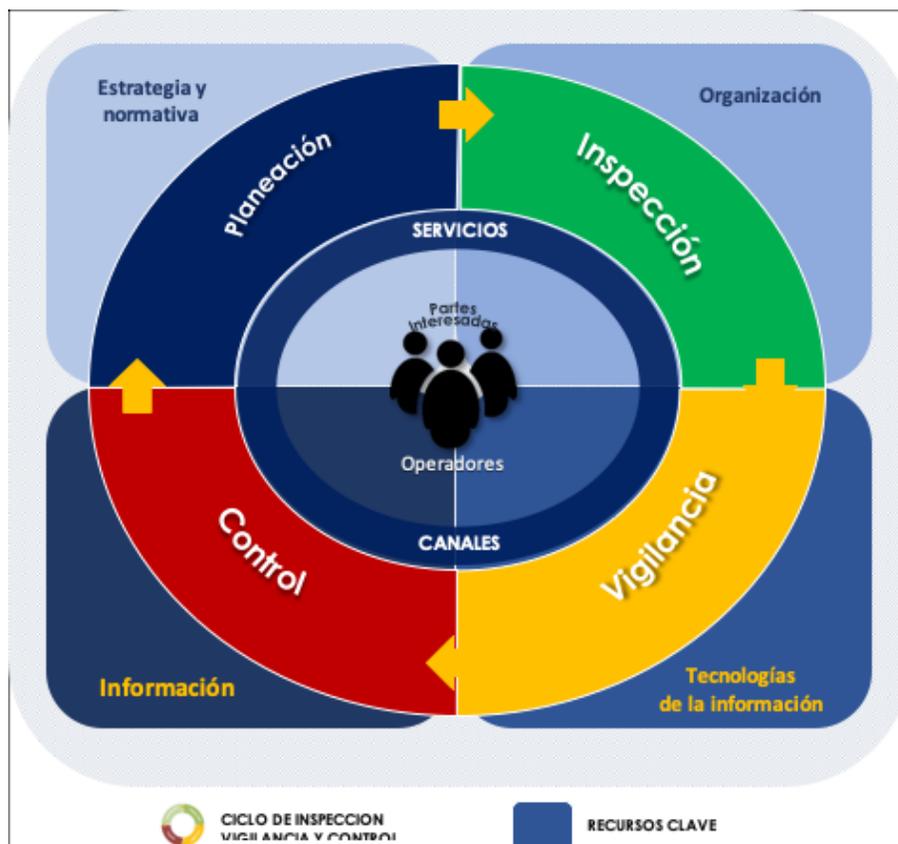


Ilustración 9. Ciclo de mejora continua del modelo de Inspección, Vigilancia y Control propuesto
Fuente: MinTIC – UT Bisa Grow, 2020

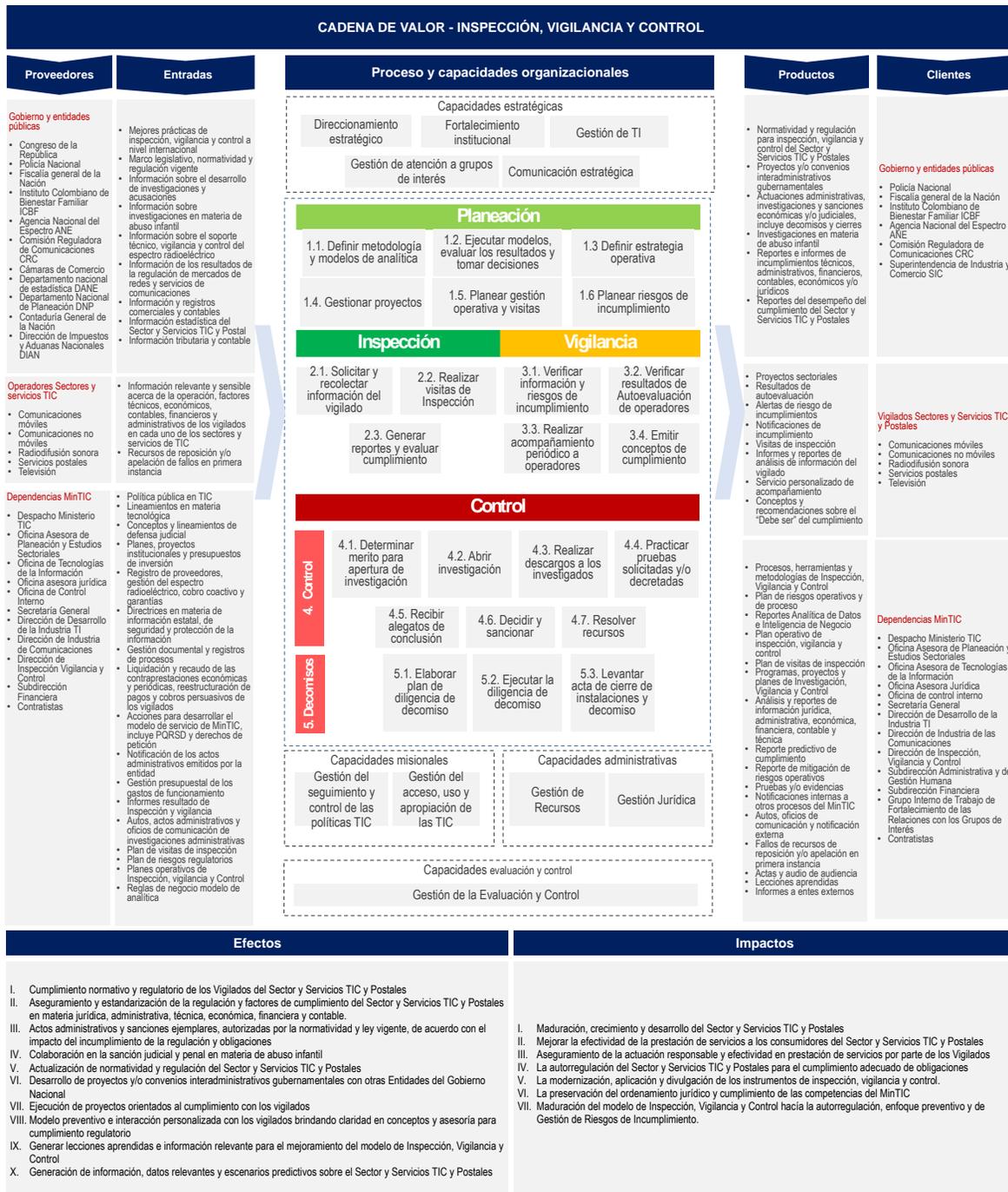


Ilustración 10. Cadena de valor Modelo de Inspección, Vigilancia y Control propuesto

Fuente: UT Bisa Grow, 2020.

La cadena de valor representa en la parte central, los procesos y capacidades organizacionales que corresponden a la secuencia de pasos lógicos, organizados que de forma iterativa transforman la información y datos relevantes de los Proveedores en Productos o Servicios que generan un efecto e impacto en la sociedad. Cabe resaltar que los límites del proceso están enmarcados dentro de la normatividad aplicable y es acorde con las funciones de la estructura organizacional que los ejecuta.





El proceso de Inspección, Vigilancia y Control comprende las etapas representadas en el modelo de Inspección, Vigilancia y Control: Planeación, Inspección, Vigilancia y Control.

- **Planeación:** Se refiere a las actividades principales que requiere la Dirección de Vigilancia y Control para generar de manera regular los planes de trabajo para optimizar de forma periódica los recursos con los que cuenta y de esta forma enfocar sus esfuerzos en los puntos críticos de la regulación vigente. Esto incluye el análisis de la información mediante la analítica de datos e inteligencia de negocio.
- **Inspección:** Corresponde a las principales actividades y acciones encaminadas al seguimiento, monitoreo y evaluación del cumplimiento de obligaciones legales, reglamentarias y regulatorias de los vigilados.
- **Vigilancia:** Son las actividades que están encaminadas a advertir, prevenir, orientar, asistir y propender porque los vigilados cumplan con las obligaciones legales, reglamentarias y regulatorias que les corresponde en los ámbitos jurídico, financiero, técnico, administrativo y de riesgos.
- **Control:** Actividades que deben sancionar las actuaciones que, por acción o por omisión de los sujetos vigilados, se aparten de las obligaciones legales, reglamentarias, regulatorias y de riesgos que les corresponden. Incluye las diligencias de cierre de instalaciones o decomiso de presuntos prestadores ilegales de los sectores y servicios de TIC dispuestos en la normatividad vigente.

Estas cuatro etapas constituyen las capacidades organizacionales del modelo, las cuales corresponden a las herramientas, metodologías y recursos físicos y económicos que no hacen parte de la Dirección Vigilancia y Control, y que se requieren para cumplir con los objetivos y metas del proceso. Es a través de estas capacidades que el proceso de Inspección, Vigilancia y Control genera sinergias con los otros procesos del Ministerio y aprovecha al máximo los recursos adicionales sin tener la necesidad de duplicar y superponer herramientas, procesos y/o responsabilidades. Esto alineado con el principio de la OCDE “Coordinación y consolidación: menos duplicaciones y superposiciones implican un mejor uso de los recursos públicos, minimizan la carga de los sujetos regulados y maximizan su efectividad” (OCDE, 2014).

De acuerdo con lo anterior y con base en los lineamientos de Arquitectura Empresarial, el nuevo modelo de vigilancia y control deberá fortalecer su operación a través de la interacción oportuna y eficiente con las capacidades organizacionales estratégicas con que cuenta la entidad, siendo éstas: Direccionamiento Estratégico, Fortalecimiento Institucional, Gestión TI, Gestión de Atención a Grupos de Interés y Comunicación Estratégica. Así mismo, deberá fortalecer su interacción con las capacidades institucionales misionales relacionadas con el Seguimiento y Control de Políticas TIC y Acceso, Uso y Apropiación de las TIC y con las capacidades organizacionales de apoyo.

De acuerdo con la indagación realizada, el modelo propuesto plantea como clientes a entidades públicas, tales como: la Policía Nacional, Fiscalía general de la Nación, Instituto Colombiano de Bienestar Familiar (ICBF), Agencia Nacional del Espectro (ANE), Comisión Regulación de Comunicaciones (CRC) y la Superintendencia de Industria y Comercio (SIC), quienes podrán hacer uso de la información que suministre el Modelo de Inspección, Vigilancia y Control; se consideran clientes los prestadores de servicios de telecomunicaciones y servicios postales quienes contribuyen a la dinámica del ejercicio y aportan en el fortalecimiento y construcción del mismo, y por último y no menos importante, las dependencias del Ministerio que aportan dinámicamente con la inspección y vigilancia de las obligaciones a cargo de los prestadores de servicios de telecomunicaciones y postales.





Como resultado de la aplicación del modelo se plantean los productos que corresponden a los resultados generados a partir del proceso de transformación y que responden a intereses particulares de las partes interesadas, de acuerdo con los objetivos y metas establecidos para el proceso. De igual forma que están organizados los clientes del proceso de Inspección, Vigilancia y Control (Gobierno, Vigilados y Dependencias Internas del Ministerio), están organizados los productos.

De acuerdo con lo anterior, los efectos esperados del desarrollo del proceso de Inspección, Vigilancia y control son:

- I. Cumplimiento normativo y regulatorio de los vigilados del Sector y Servicios de telecomunicaciones y postales.
- II. Aseguramiento y estandarización de la regulación y factores de cumplimiento del Sector y Servicios de telecomunicaciones y postales en materia jurídica, administrativa, técnica, económica, financiera y contable.
- III. Actos administrativos y sanciones ejemplares, autorizadas por la normatividad y ley vigente, de acuerdo con el impacto del incumplimiento de la regulación y obligaciones.
- IV. Colaboración en la sanción judicial y penal en materia de abuso infantil.
- V. Actualización de normatividad y regulación del Sector y Servicios de telecomunicaciones y postales.
- VI. Desarrollo de proyectos y/o convenios interadministrativos gubernamentales con otras Entidades del Gobierno Nacional.
- VII. Ejecución de proyectos orientados al cumplimiento de los vigilados.
- VIII. Modelo preventivo e interacción personalizada con los vigilados brindando claridad en conceptos y asesoría para cumplimiento.
- IX. Generar lecciones aprendidas e información relevante para el mejoramiento del modelo de Inspección, Vigilancia y Control.
- X. Generación de información, datos relevantes y escenarios predictivos sobre el Sector y Servicios de telecomunicaciones y postales.

En cuanto a los impactos, corresponden a los cambios en las condiciones de las partes interesadas que son objeto del proceso de Inspección, Vigilancia y Control:

- I. Maduración, crecimiento y desarrollo del Sector y Servicios de telecomunicaciones y postales.
- II. Mejorar la efectividad de la prestación de servicios a los consumidores del Sector y Servicios de telecomunicaciones y postales.
- III. Aseguramiento de la actuación responsable y efectividad en prestación de servicios por parte de los vigilados.
- IV. La autorregulación del Sector y Servicios de telecomunicaciones y postales para el cumplimiento adecuado de obligaciones.
- V. La modernización, aplicación y divulgación de los instrumentos de inspección, vigilancia y control.
- VI. La preservación del ordenamiento jurídico y cumplimiento de las competencias del MinTIC.
- VII. Maduración del modelo de Inspección, Vigilancia y Control hacia la autorregulación, enfoque preventivo, predictivo y de Gestión de Riesgos de Incumplimiento.

Partes interesadas del Modelo de Inspección, Vigilancia y Control propuesto





Bajo el entendido de que partes interesadas corresponde a la identificación de las interacciones y actores claves que deben interactuar con el proceso de Inspección, Vigilancia y Control para generar los efectos e impactos esperados que se definieron en la cadena de valor, la siguiente tabla resume las partes interesadas del Modelo de Inspección, Vigilancia y Control:

Clasificación	Parte interesada	Información y datos relevantes
Gobierno y Entidades públicas	Congreso de la República	Control político y administrativo del gobierno
	Policía Nacional	Información relacionada con el desarrollo de procedimientos de investigación criminal
	Fiscalía general de la Nación	Información relacionada con investigaciones y acusaciones de los presuntos responsables de cometer delitos
	Instituto Colombiano de Bienestar Familiar ICBF	Información relacionada con la prevención y protección integral de la primera infancia, niñez, adolescencia y bienestar de las familias en Colombia en materia de abuso infantil
	Agencia Nacional del Espectro ANE	Información relacionada con el soporte técnico para la gestión, planeación, vigilancia y control del espectro radioeléctrico
	Comisión Reguladora de Comunicaciones CRC	Información relacionada con competencia, abuso de posición dominante, regulación de mercados de redes y servicios de comunicaciones
	Cámaras de Comercio	Información y registros comerciales y contables
	Departamento nacional de estadística DANE	Información estadística de sectores TIC
	Departamento Nacional de Planeación DNP	Lineamientos de interoperabilidad y planes nacionales de desarrollo, entre otros afines.
	Contraloría General de la Nación	Información contable
	Dirección de Impuestos y Aduanas Nacionales DIAN	Información tributaria
Prestadores de Servicios de Telecomunicaciones y Servicios Postales	Comunicaciones móviles	Información relevante y sensible acerca de la operación, factores técnicos, económicos, contables, financieros y administrativos de los Operadores en cada uno de los sectores y servicios de TIC
	Comunicaciones no móviles	
	Radiodifusión sonora	
	Servicios postales	
Funcionarios y Contratistas de la Dirección de Vigilancia y Control	Televisión	
		Personal externo que desarrollan actividades relacionadas con la administración funcionamiento del MinTIC en misión, bajo supervisión administrativa y técnica de un experto





Dependencias del MinTIC	Despacho Ministerio TIC	Política pública en TIC
	Oficina Asesora de Planeación y Estudios Sectoriales	Coordinar la ejecución de planes, proyectos institucionales y presupuestos de inversión
	Oficina de Tecnologías de la Información	Desarrollar lineamientos, en materia tecnológica, necesarios para definir políticas, estrategias y prácticas que soporten la gestión del sector en beneficio de la prestación efectiva de sus servicios
	Oficina asesora jurídica	Asesoría en asuntos jurídicos, conceptos y lineamientos de defensa judicial
	Oficina de Control Interno	Liderar el Sistema de Control Interno de la Entidad asegurando el correcto desarrollo del proceso de Inspección, Vigilancia y Control
	Secretaría General	Dirigir los procesos de notificación y publicidad de todos los actos administrativos, gestión documental, archivo, PQRDS, Inventarios de bienes muebles e inmuebles,
	Dirección de Desarrollo de la Industria TI	Liderar el desarrollo de las políticas para la Industria y Tecnologías de la Información
	Dirección de Industria de Comunicaciones	Formular y elaborar propuestas de política sectorial y planes para el desarrollo y provisión de redes, servicios de telecomunicaciones, radiodifusión sonora, servicios postales y la producción filatélica. Administrar el registro de proveedores de Redes y Servicios de Telecomunicaciones, gestión del espectro radioeléctrico, cobro coactivo y constitución de garantías
	Subdirección Financiera	Coordinar el presupuesto de funcionamiento, recibir, revisar, generar e informar las autoliquidaciones de derechos correspondientes a las contraprestaciones que se causan a favor del Fondo de Tecnologías de la Información y las Comunicaciones.
		Liderar las acciones de gestión de cartera, cobro persuasivo, elaborar y mantener actualizada la información referente a los estados de cuentas de los operadores.

Tabla 4. Partes interesadas de Modelo propuesto

Fuente: UT Bisa Grow, 2020.

Los canales de comunicación son los medios que el proceso de Inspección, Vigilancia y Control utiliza para interactuar con las partes interesadas, como se aprecia en la siguiente figura.



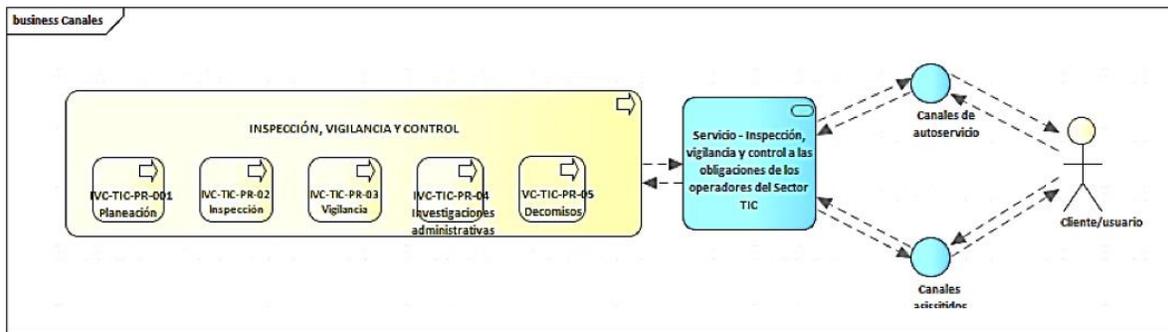


Ilustración 11. Canales de comunicación vs. procesos

Fuente: UT Bisa Grow, 2020.

En cuanto a los procesos, la propuesta parte de los lineamientos establecidos por el Ministerio TIC en el documento Manual del Modelo Integrado de Gestión y Manual norma fundamental, se definieron los Subprocesos del Proceso de Inspección, Vigilancia y Control como procedimientos, toda vez que las características de este tipo de documento permiten evidenciar el método de trabajo e interacción con otras áreas. En la siguiente tabla, se detallan los procedimientos propuestos dentro del nuevo modelo de Inspección Vigilancia y Control:



CÓDIGO	PROCESO	PROCEDIMIENTO	OBJETIVO DEL PROCEDIMIENTO	ALCANCE DEL PROCEDIMIENTO	CÓDIGO	ACTIVIDADES CLAVE
IVC-TIC-MA-001	INSPECCIÓN, VIGILANCIA Y CONTROL	PLANEACIÓN	Desarrollar la planeación de las operaciones de Inspección, Vigilancia y Control de acuerdo con los resultados de la Analítica de Datos y Gestión de riesgos de incumplimiento del Sector y Servicios TIC	Desde la definición de la metodología de Inspección, Vigilancia y Control y del modelo de analítica predictiva hasta la gestión de proyectos de IVC. Incluye la ejecución del modelo de analítica, la evaluación de sus resultados, la toma de decisiones, la gestión de proyectos; la planeación de riesgos de incumplimiento, de la operación y visitas.	IVC-TIC-PR-001	Actualizar y definir metodología de Inspección, Vigilancia y Control
						Definir modelo de analítica
						Ejecutar modelos, evaluar los resultados y tomar decisiones
						Definir estrategia operativa
						Priorizar y gestionar proyectos
						Planear gestión operativa y visitas
		Planear riesgos de incumplimiento				
		INSPECCIÓN	Hacer seguimiento, monitoreo y evaluación del cumplimiento de las obligaciones legales reglamentarias, contractuales y regulatorias por medio de la recolección, confirmación y análisis de la información de los operadores.	Comprende la solicitud y recolección de información de los operadores, la ejecución y desarrollo de las visitas de inspección, la generación de informes de verificación de cumplimiento. Incluye la verificación de obligaciones en materia de abuso sexual infantil y adolescentes, y decomisos	IVC-TIC-PR-002	Solicitar y recolectar información del vigilado
						Realizar Visitas de Inspección
Generar reportes y evaluar cumplimiento						
VIGILANCIA	Impartir las directrices e instrucciones a los operadores con el	Desde la verificación del tablero de riesgos de incumplimiento, la verificación de los resultados de Autogestión de los operadores, la	IVC-TIC-PR-003	Verificar información y riesgos de incumplimiento		





	fin de advertir, prevenir, orientar, asistir y propender el cumplimiento de sus obligaciones legales reglamentarias, contractuales y regulatorias	asistencia periódica a los operadores, la emisión de conceptos de cumplimiento y comunicados		<p>Verificar Autoevaluación de operadores</p> <p>Realizar acompañamiento periódico a los operadores</p> <p>Emitir conceptos de cumplimiento y comunicados a los operadores</p>
INVESTIGACIONES ADMINISTRATIVAS	Adelantar las averiguaciones preliminares que resulten necesarias en el desarrollo de sus funciones de inspección y vigilancia para sancionar las actuaciones que, por acción o por omisión de los sujetos vigilados, se aparten de las obligaciones legales, reglamentarias, contractuales y regulatorias que les corresponden.	Desde la atención de las solicitudes de investigaciones administrativas, hasta la determinación de consecuencias judiciales o sancionatorias en primera instancia, entre ellos cierres, decomisos e investigaciones material de abuso sexual infantil y adolescentes.	IVC-TIC-PR-004	<p>Determinar mérito para apertura de investigación</p> <p>Abrir investigación</p> <p>Realizar descargos</p> <p>Practicar pruebas decretadas</p> <p>Recibir alegatos de conclusión</p> <p>Decidir y sancionar</p> <p>Resolver recursos</p> <p>Comunicar a entes externos</p>
DECOMISOS	Llevar a cabo las diligencias de cierre de instalaciones o decomiso de presuntos prestadores ilegales de los sectores y servicios de TIC dispuestos en la normatividad vigente	Desde la verificación de la prestación ilegal de servicios TIC incluyendo la logística, ejecución de la diligencia de cierre de instalaciones o decomiso, la custodia de los bienes durante la investigación administrativa hasta la disposición definitiva de los bienes decomisados.	IVC-TIC-PR-005	<p>Elaborar plan de decomiso</p> <p>Ejecutar la diligencia de decomiso</p> <p>Levantar acta de cierre de instalaciones y decomiso</p>

Tabla 5. Procedimientos nuevo modelo

Fuente: UT Bisa Grow, 2020.





Cabe aclarar que existen componentes de servicio institucional que son el resultado del desarrollo de Inspección, Vigilancia y Control soportado con otras capacidades organizacionales del Ministerio, como lo son atención a PQRSD y trámites, plan operativo y presupuestos de inversión y funcionamiento de IVC y proyectos orientados a la IVC. Estos componentes de servicio institucional no están incluidos dentro del alcance del proceso de Inspección, Vigilancia y Control y por tanto no están codificados, toda vez que corresponden a otros procesos de la Entidad.

Por el contrario, tenemos los componentes de servicio institucional que se generan con las propias capacidades organizacionales de Inspección, Vigilancia y Control, que corresponden a los componentes de servicio institucional codificados: Analítica de datos para el mejoramiento y planeación operativa, Generación de información, Planeación operativa de Inspección, Vigilancia y Control, Gestión de riesgos de incumplimiento, Recolección de información, Visitas, Seguimiento, monitoreo y evaluación, Advertir y prevenir, Autoevaluación de los operadores, Orientar y asistir, Impartir directrices, Investigaciones administrativas y Decomisos.

El componente de servicio institucional de Gestión de Riesgos de Incumplimiento presenta un comportamiento particular, porque si bien existe la capacidad del procedimiento “lineamientos para la administración de riesgos” esta debe adaptarse al Modelo de Inspección, Vigilancia y Control para poder desarrollar la gestión de riesgos de incumplimiento de los Vigilados del Sector y Servicios de telecomunicaciones y servicios postales de acuerdo con las políticas y definiciones del Ministerio en materia de Gestión de Riesgos.

5.3. DOMINIO DE INFORMACIÓN

Para diseñar el estado deseado del dominio de información, se realizó un nuevo catálogo de entidades de información proponiendo entidades para metadatos, entidades para repositorios transaccionales centralizados y entidades para generar interoperabilidad. Posteriormente, se realizó un alineamiento con procesos y sistemas de información para lograr una sinergia y llevar el proceso de Inspección, Vigilancia y Control (IVC) a una arquitectura centralizada en datos.

Para el proceso de IVC, se requieren ochenta y nueve (89) entidades, entre las cuales se encuentran ocho (8) documentos, doce (12) documentos de apoyo, cuatro (4) reportes, cincuenta y cinco (55) entidades transaccionales y diez (10) entidades importadas. Salvo por los documentos y documentos de apoyo, las demás entidades son de tipo estructurada.

El cambio más significativo al catálogo de entidades de información propuesto respecto a la arquitectura actual o AS-IS, es convertir en información estructurada la información disponible durante todo el proceso. Adicionalmente, se propone unificar la información, estandarizar y tener una definición clara de los datos manejados. Es necesario también, que las nuevas entidades implementadas y desplegadas en el modelo propuesto (y las provenientes de otros procesos como Industria, Cartera, Planeación, etc.), tengan un modo de construcción con alineamientos únicos, optimizadas y con la metadata que permita identificar todos los datos que componen una entidad con una estructura única, con fuente centralizada y con información veraz para todo el proceso, y que además, esta metadata esté alojada en el repositorio documental para que pueda ser fácilmente consultada cuando se generen proyectos de mantenimiento preventivo, evolutivo y nuevas implementaciones.

En lo que respecta al Modelo de Entidad de Datos, o EDM por sus siglas en inglés, describe las interacciones de los datos transaccionales propuestos encontrados en el Catálogo de Entidades de Información, independientemente del sistema en el que estén almacenados. El siguiente diagrama muestra la propuesta de cómo las entidades se encuentran debidamente relacionadas entre sí:



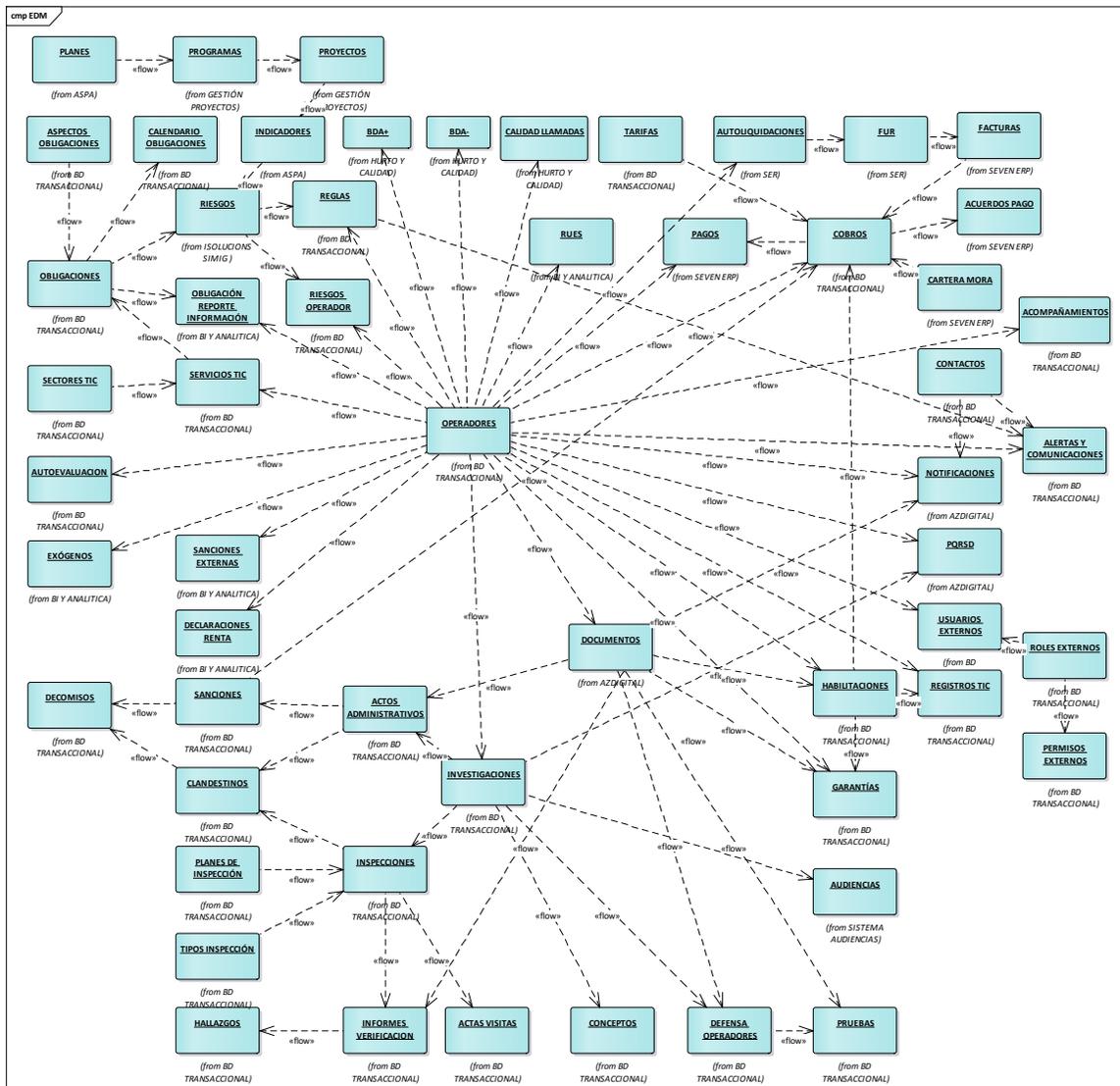


Ilustración 12. Diagrama del modelo de entidades de datos.
Fuente: UT Bisa Grow, 2020.

El anterior diagrama demuestra que la entidad de información OPERADORES es el dato principal. También, hay otras entidades importantes como INVESTIGACIONES y DOCUMENTOS que se usan recurrentemente en todo el proceso de IVC.

Este modelo sirve como fuente de información de la arquitectura para las implementaciones propuestas como iniciativas en el presente proyecto. Con él, se puede entender la conexión de información de las entidades planteadas.

En lo que respecta al Catálogo de Entidades Maestras propuesto obtenido mediante el análisis de Gestión de Datos Maestros, MDM, por sus siglas en inglés Master Data Management, con los cuales se busca obtener una única fuente de información para que los sistemas que interactúen con estos datos coincidan. Las entidades de información se muestran agrupadas por la asociación interna de dependencia que tienen entre





sí, presentando las entidades fuertes y referenciales como las primeras por cada cuadro, y debajo de ellas (con sangría) las entidades que solo representan valor a partir de las referenciales.

OPERADORES HABILITACIONES	CONTACTOS	SECTORES TIC SERVICIOS TIC ESTUDIOS DE SECTOR	OBLIGACIONES ASPECTOS OBLIGACIONES CALENDARIO OBLIGACIONES
DIVIPOLA	USUARIOS EXTERNOS ROLES EXTERNOS PERMISOS EXTERNOS	TARIFAS	

Tabla 6. Catálogo de entidades maestras
Fuente: UT Bisa Grow, 2020.

En este contexto, se proponen 14 entidades de datos para agregar al MDM. Actualmente, ya existe un almacén para MDM y en este existe la entidad de información OPERADORES, para el cual se recomienda ser complementado para que sus características y atributos coincidan con los datos que se requieran en todo el proceso de IVC. Para complementar la información de cada una de las entidades se debe tomar el catálogo de entidades de información.

El objetivo de almacenar estas entidades de información en un almacén de datos maestros es tener una única fuente de información para los datos que son indispensables en múltiples sistemas de información del MinTIC.

Por otra parte, también se propone un almacenamiento único para varias entidades transaccionales, denominado BD TX SECTOR, o Base de Datos Transaccionales del Sector, que tiene el mismo objetivo de unificar y crear certeza sobre el dato, pero con entidades con un mayor nivel de transaccionalidad y creado específicamente para las entidades del proceso de Inspección, Vigilancia y Control.

Respecto a interoperabilidad, se elaboró el catálogo de Entidades de Interoperabilidad, que se describe en la siguiente tabla:

Entidad	Clasificación interna	Descripción	Productor	Clasificación	Tipo de información	Frecuencia de Generación	Soporte	Formato
OPERADORES	SALIDA	Conjunto de datos de los operadores de los servicios de telecomunicaciones	Industria	Pública	Estructurada	No Aplica	Medio Electrónico	Conjunto de Datos
HABILITACIONES	SALIDA	Conjunto de datos de las habilitaciones, licencias y/o concesiones realizadas a los operadores que les permiten prestar el servicio	Industria	Pública	Estructurada	No Aplica	Medio Electrónico	Conjunto de Datos
SANCCIONES	SALIDA	Conjunto de datos de las sanciones realizadas a los operadores mediante el proceso de control	Vigilancia y Control	Pública	Estructurada	No Aplica	Medio Electrónico	Conjunto de Datos
INVESTIGACIONES	SALIDA	Conjunto de datos de las investigaciones abiertas a los operadores, se debe generar niveles de acceso de la información para mantener la privacidad de la información	Vigilancia y Control	Semiprivada	Estructurada	No Aplica	Medio Electrónico	Conjunto de Datos





Entidad	Clasificación interna	Descripción	Productor	Clasificación	Tipo de información	Frecuencia de Generación	Soporte	Formato
ESTADÍSTICAS DEL SECTOR	SALIDA	Conjunto de datos resultado del proceso de generación de estadísticas, base del boletín trimestral	MinTIC	Pública	Estructurada	Trimestral	Medio Electrónico	Conjunto de Datos
BOLETÍN TRIMESTRAL	SALIDA	Conjunto de datos generado por MinTIC para presentar las estadísticas del sector	Planeación	Pública	No Estructurada	Trimestral	Medio Electrónico	Conjunto de Datos
OBLIGACIÓN REPORTE DE INFORMACIÓN	ENTRADA	Datos reportados por los operadores de las obligaciones para cargue masivo	Operadores	Pública	Semiestructurada	No Aplica	Medio Electrónico	Archivos Planos
BDA +	ENTRADA	Archivos de cargue de la base de datos positiva de los operadores para el proceso de hurto	Operadores	Privada	Semiestructurada	No Aplica	Medio Electrónico	Archivos Planos
BDA -	ENTRADA	Archivos de cargue de la base de datos negativa de los operadores para el proceso de hurto	Operadores	Privada	Semiestructurada	No Aplica	Medio Electrónico	Archivos Planos
CALIDAD LLAMADAS	ENTRADA	Archivos de cargue de los indicadores técnicos de la calidad de las llamadas	Operadores	Privada	Semiestructurada	No Aplica	Medio Electrónico	Archivos Planos
RECAUDOS BANCO	ENTRADA	Archivos de cargue de los recaudos bancarios para obtener los datos de pagos de los operadores por medios bancarios	Bancos	Privada	Semiestructurada	No Aplica	Medio Electrónico	Archivos Planos
FRECUENCIAS	ENTRADA	Registro de las frecuencias del espectro otorgadas y disponibles para las solicitudes de los operadores	Agencia Nacional del Espectro ANE	Pública	Estructurada	No Aplica	Medio Electrónico	Conjunto de Datos
ANTECEDENTES JUDICIALES	ENTRADA	Información relacionada con los antecedentes judiciales asociados a las personas naturales relacionadas con los operadores	Policía Nacional	Pública	Estructurada	No Aplica	Medio Electrónico	Conjunto de Datos
REGISTRO DE MEDIDAS CORRECTIVAS	ENTRADA	Información relacionada con el registro nacional de medidas correctivas asociados a las personas naturales relacionadas con los operadores	Policía Nacional	Pública	Estructurada	No Aplica	Medio Electrónico	Conjunto de Datos
ANTECEDENTES DISCIPLINARIOS	ENTRADA	Información relacionada con los antecedentes judiciales asociados a las personas naturales y jurídicas relacionadas con los operadores	Procuraduría General de la Nación	Pública	Estructurada	No Aplica	Medio Electrónico	Conjunto de Datos
ANTECEDENTES FISCAL	ENTRADA	Información relacionada con los antecedentes fiscales asociados a las personas naturales y jurídicas relacionadas con los operadores	Contraloría General de la Nación	Pública	Estructurada	No Aplica	Medio Electrónico	Conjunto de Datos
INVESTIGACIONES	ENTRADA	Información de las investigaciones de prevención y protección integral de la primera infancia, niñez, adolescencia y bienestar de las familias en Colombia en materia de abuso	Instituto Colombiano de Bienestar Familiar ICBF	Privada	Estructurada	No Aplica	Medio Electrónico	Conjunto de Datos





Entidad	Clasificación interna	Descripción	Productor	Clasificación	Tipo de información	Frecuencia de Generación	Soporte	Formato
		infantil relacionadas con los operadores						
SANCI ONES	ENT RAD A	Información relacionada con las sanciones por competencia en materia de abuso de posición dominante, regulación de mercados de redes y servicios de comunicaciones relacionadas con los operadores	Comisión Reguladora de Comunicaciones CRC	Pública	Estructurada	No Aplica	Medio Electrónico	Conjunto de Datos
SANCI ONES	ENT RAD A	Información relacionada con sanciones por libre competencia económica, derechos consumidores, entre otros relacionadas con los operadores	Superintendencia de Industria y Comercio SIC	Pública	Estructurada	No Aplica	Medio Electrónico	Conjunto de Datos
SANCI ONES	ENT RAD A	Información relacionada de las sanciones asociadas con el operador en la ANE	Agencia Nacional del Espectro ANE	Pública	Estructurada	No Aplica	Medio Electrónico	Conjunto de Datos
SANCI ONES	ENT RAD A	Información relacionada con las sanciones de competencia, abuso de posición dominante, regulación de mercados de redes y servicios de comunicaciones relacionadas con los operadores	Comisión Reguladora de Comunicaciones CRC	Pública	Estructurada	No Aplica	Medio Electrónico	Conjunto de Datos
REGISTRO COMERCIAL - RUES	ENT RAD A	Información y registros comerciales de las personas jurídicas asociadas al operador	Confecámaras	Pública	Estructurada	No Aplica	Medio Electrónico	Conjunto de Datos
DEUDOS	ENT RAD A	Información relacionada con deudores morosos del estado relacionada con los operadores	Contaduría General de la Nación	Pública	Estructurada	No Aplica	Medio Electrónico	Conjunto de Datos
DATOS EXÓGENOS	ENT RAD A	Información tributaria y contable reportada por los operadores	DIAN	Privada	Estructurada	No Aplica	Medio Electrónico	Conjunto de Datos
DECLARACIONES RENTA	ENT RAD A	Registro de la declaración de renta de las personas naturales y jurídicas relacionadas con los operadores	DIAN	Privada	Estructurada	No Aplica	Medio Electrónico	Conjunto de Datos
CIUDADANO	ENT RAD A	Registro de las personas naturales en el servicio de autenticación de ciudadano	Registraduría	Pública	Estructurada	No Aplica	Medio Electrónico	Conjunto de Datos

Tabla 7. Catálogo de Entidades de Información Interoperables

Fuente: UT Bisa Grow, 2020.

De la anterior tabla, se proponen según su clasificación, tres (3) nuevas entidades de salida que pueden ser albergadas en Datos Abiertos y/o Colombia TIC (OPERADORES, HABILITACIONES, INVESTIGACIONES, SANCIONES), para agregar a las dos (2) que ya se publican actualmente (ESTADÍSTICAS DEL SECTOR Y BOLETÍN TRIMESTRAL) como información que agrega valor de cara a la ciudadanía y a otras entidades que requieran dicha información para sus procesos. Por otra parte, se proponen veinte (20) datos de entrada para el proceso de IVC, de los cuales, seis (6) ya se encuentran actualmente implementados (OBLIGACIÓN REPORTE DE INFORMACIÓN, BDA +, BDA -, CALIDAD LLAMADAS, RECAUDOS BANCOS,



FRECUENCIAS), y catorce (14) serían nuevas fuentes de información que se utilizarían principalmente en el modelo de análisis de información.

Se propone incrementar la interoperabilidad, tanto en información de entrada, que permitirá la obtención de información para el análisis predictivo y preventivo, como para la información de salida, que tiene el fin de que las partes interesadas obtengan información relevante generada en el proceso de IVC del MinTIC. Con base en lo anteriormente expuesto se busca llegar a un nuevo nivel de madurez presentado a continuación:

- **Metadatos: Nivel 4 Optimización**, Los datos estructurales de las entidades de información son uniformes y existen lineamientos claros para la arquitectura de las aplicaciones que los usen. Los metadatos estructurales se encuentran incrustados en los almacenes y los diagramas, diseños y diccionarios se encuentran en un repositorio de arquitectura de tecnología.
- **Datos Maestros: Nivel 5 Liderazgo**, los datos maestros son diseñados de manera óptima, y se encuentran en un repositorio único siendo accedidos por todos los sistemas que requieren su información mediante una arquitectura claramente definida. Además, existen indicadores sobre su uso y calidad.
- **Datos Operacionales Estructurados: Nivel 5 Liderazgo**, los datos estructurados son diseñados de manera óptima, y se encuentran en repositorios únicos transaccionales siendo accedidos por todos los sistemas que requieren su información mediante una arquitectura claramente definida. Además, existen indicadores sobre su uso y calidad.
- **Datos Operacionales No Estructurados: Nivel 4 Optimización**, los datos no estructurados son diseñados de manera óptima, y se encuentran en un repositorio único siendo accedidos por todos los sistemas que requieren su información mediante una arquitectura claramente definida.
- **Datos Analíticos: Nivel 5 Liderazgo**, los datos analíticos fueron diseñados mediante un proceso de gobierno del dato y obtienen información que permite la toma de decisiones, tanto a nivel de proceso como a nivel de usuario final (operadores). Además, existen indicadores sobre la calidad de la información en sí misma.

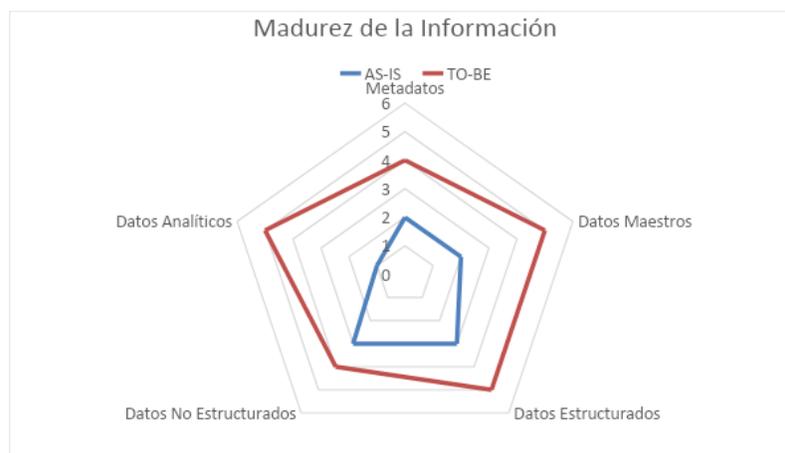


Ilustración 13. Madurez de los pilares de la información deseada

Fuente: Elaboración propia, 2020



Al comparar la información con los sistemas de información, se concluye que la mayoría de los datos tendrán repositorios comunes, los cuales se resumen en:

- Los datos de usuario interno se manejarán por medio del directorio activo de MinTIC, mientras que los usuarios externos deberán consumir los servicios de GOV.CO para autenticación y deberán consumir los datos de autorización mediante el MDM de la Entidad.
- Los datos maestros serán alojados en el MDM, los cuales se encuentran identificados en el Catálogo de Entidades Maestras.
- Varias entidades de datos se almacenarán en su respectivo sistema, por ejemplo, las referentes a la Documentación se almacenarán en el repositorio de AZDigital, o los datos financieros en Seven.
- Los datos de los procesos de flujos BPM de IVC no se almacenarán en Auraportal, tampoco los datos del resultado del proceso de Monitoreo. Estos se alojarán en una base de datos transaccional del proceso, denominada en el catálogo como BD TX SECTOR, o Base de Datos Transaccional de Sector.
- Todos los datos importados, se pueden almacenar en Bodega de Datos, o DWH por sus siglas en inglés de Data Warehouse, y deberán ser consumidos mediante Data Marts (subconjunto de datos con un propósito específico) y presentados a través de las herramientas de inteligencia de negocio o BI.

En lo concerniente al análisis realizado de los procesos y procedimientos respecto a la información, como lo establecen los lineamientos de Arquitectura Empresarial, para el apropiado uso y explotación de la información deberá existir una alineación de los dominios de estrategia, sistemas e información. El catálogo presenta 175 relaciones para las 40 actividades, de los cuatro procedimientos del modelo propuesto: planeación, inspección, vigilancia y control.

Por último, del análisis del dominio de Información se pudo concluir que existe una desarticulación respecto a los datos que actualmente existen y las tablas de retención documental del proceso de IVC. Por lo tanto, se propone generar nuevos tipos documentales que estén más asociados a las entidades del proceso propuesto.

5.4. DOMINIO SISTEMAS DE INFORMACIÓN

La arquitectura de los componentes de sistemas de información propuestos para el Modelo de Inspección, Vigilancia y Control se estructuran bajo una arquitectura centrada en los datos. Se deberá considerar que la entidad información es la misma para:

- Los componentes de información, los que a su vez deben estar alineados al dominio de información del modelo de arquitectura empresarial de MinTIC.
- Sistemas de información e integraciones, los que a su vez deben estar alineados al dominio de sistemas de información del modelo de arquitectura empresarial de MinTIC.
- Servicios de integraciones, los que a su vez deben estar alineados al marco de interoperabilidad de MinTIC.
- Activos de información, los que a su vez deben estar alineados al modelo de seguridad y privacidad de la información MSPI de MinTIC.
- Tabla de retención documental del nuevo proceso de IVC.
- Glosario de MinTIC.



- Entradas y salidas del nuevo proceso de Inspección, Vigilancia y Control.
- Trámites y servicios que se exponen en GOV.CO alineados a la transformación digital de Colombia.
- Datos abiertos.
- Lenguaje Común de Intercambio de Información.

A continuación, una ilustración de la arquitectura centrada en datos, propuesta para el Modelo de Inspección, Vigilancia y Control:

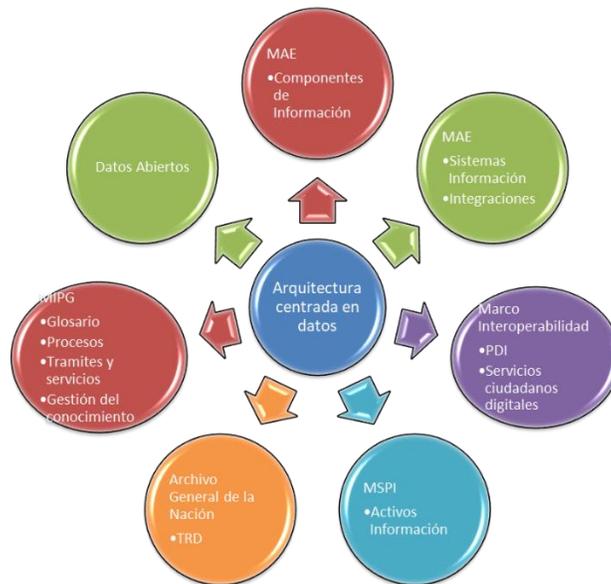


Ilustración 14. Arquitectura centrada en datos.

Fuente: Elaboración propia, 2020

Con esto se comprende que cada entidad de información que es diseñada y presentada en los componentes de sistemas de información se encuentra contemplada en el dominio de información del presente proyecto y se entregará al gobierno de datos de MinTIC para su correspondiente ciclo de vida y controles de calidad.

En el dominio de sistemas de información se desarrolló el análisis y diseño de arquitectura empresarial de sistemas de información de cada uno de los servicios del nuevo proceso de Inspección, Vigilancia y Control. A continuación, se presenta el diagrama general de los componentes de sistemas de información contra los servicios de negocio y los procedimientos del nuevo proceso de inspección, vigilancia y control.

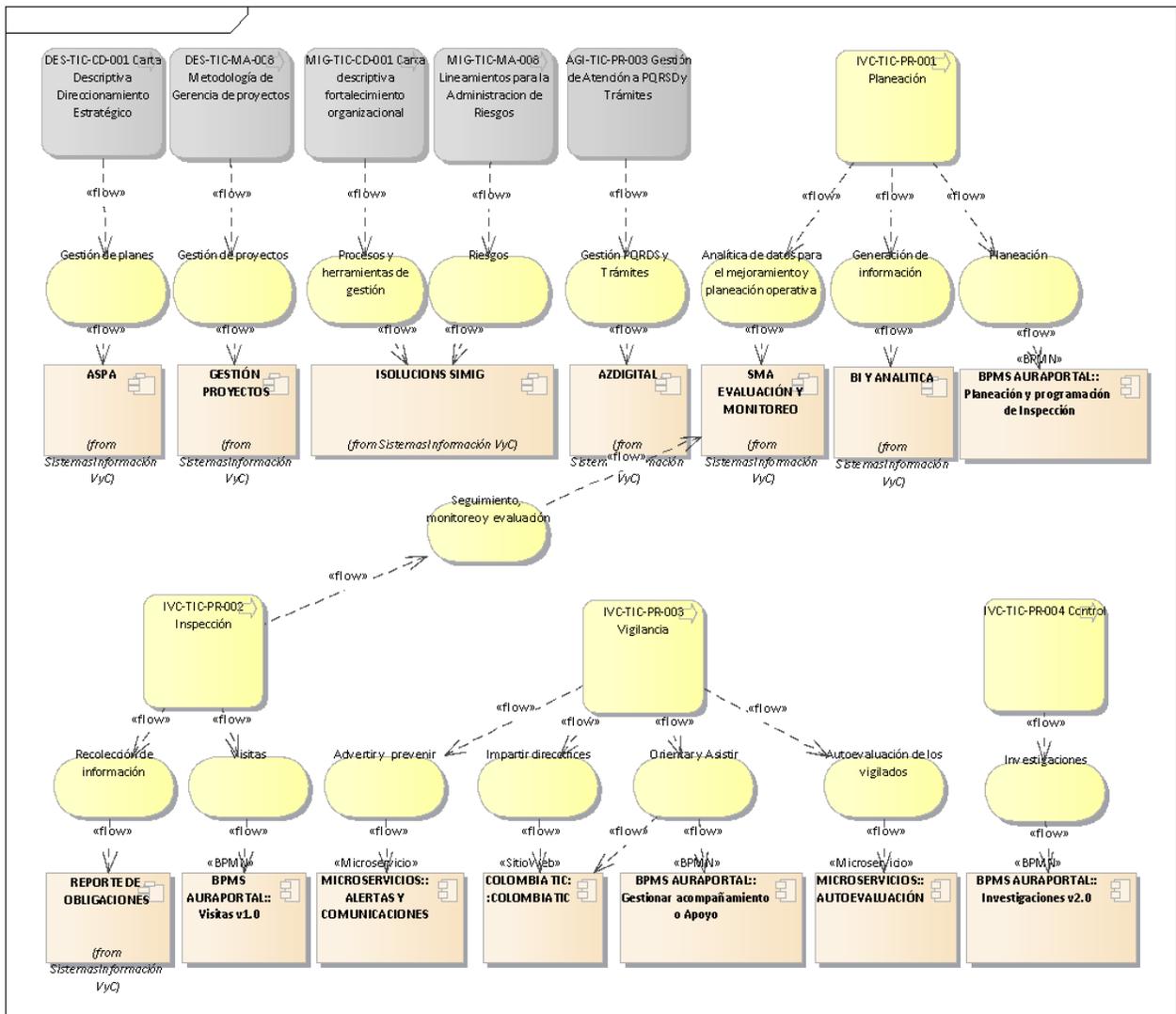


Ilustración 15. Procedimientos vs servicios de negocio vs sistemas de información

Fuente: Elaboración propia, 2020

Respecto al diagrama observamos que:

- Se presentan en color gris los procedimientos que ya existen en el MIG de MinTIC pero que fueron incluidos como parte del nuevo proceso de IVC. Lo anterior, indica que se contempló el análisis de los sistemas de información alineado a dichos procedimientos de negocio.
- Se presentan en color amarillo los siguientes procedimientos: Planeación, Inspección, Vigilancia y Control del nuevo proceso de IVC.
- Se presentan en color amarillo (y debajo de los procedimientos) los servicios de negocio del nuevo proceso de IVC, alineados con los componentes de sistemas de información presentados en color rosado al igual que se presentaron en el metamodelo.
- El diseño propuesto de cada uno de los sistemas de información se apalancó en los lineamientos entregados por la oficina de TI y las mejores prácticas del mercado, como Arquitectura Orientada por

Servicios (SOA), Arquitectura Orientada a Eventos, Arquitectura Centrada en Datos, Microservicios, Analítica Avanzada y Big Data.

- Por cada uno de estos componentes se desarrolló una arquitectura empresarial de sistemas de información y sus posibles integraciones.
- La base para que todos los diseños de sistemas de información aquí propuestos sean analizados, diseñados, desarrollados y puestos en producción, es fortalecer los procesos de desarrollo de software, gobierno del dato e infraestructura, que forman parte de los procesos de Gestión de TI.
- Se encuentra también el alineamiento entre las actividades de los procedimientos, los sistemas de información y las entidades de información.

Para solventar la integración e interoperabilidad entre todos los sistemas de información, se siguieron los lineamientos de la oficina de TI de MinTIC y se desarrolló la propuesta de arquitectura orientada en servicios de la siguiente forma:

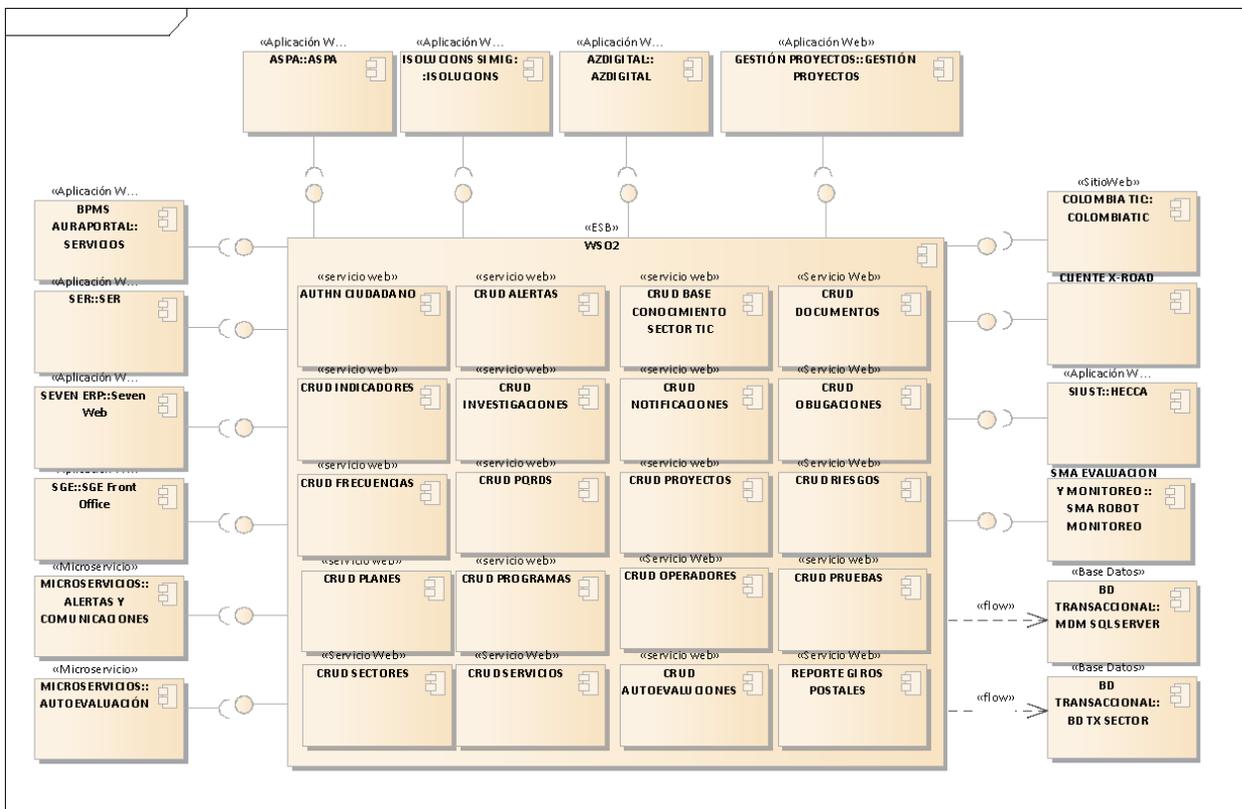


Ilustración 16. Ejemplo de uso del ESB WS02

Fuente: Elaboración propia, 2020

La ilustración anterior muestra cómo se plantea integrar los diferentes sistemas haciendo uso del bus de datos.



5.5. DOMINIO DE SERVICIOS TECNOLÓGICOS

Para el dominio de servicios tecnológicos se propuso la distribución de los diferentes sistemas de información diseñados, en los centros de datos con los que cuenta el MinTIC.





6. ANÁLISIS DE BRECHAS Y PLAN DE ACCIÓN

El análisis de brechas se define como un método para evaluar las diferencias entre el estado actual y el esperado en una organización o negocio. Se refiere al espacio entre “dónde estamos ahora” (el estado actual) y “dónde queremos estar” (el estado objetivo). En esta sección se presenta una breve descripción de cómo se planteó el plan de acción que permitirá cerrar las brechas encontradas entre el estado actual y estado objetivo del modelo de Inspección, Vigilancia y Control. Como resultado del análisis de brechas, se generan los catálogos de brechas que constituyen la base para la definición de acciones de cierre y su agrupamiento lógico en el portafolio de planes, programas y proyectos. Las brechas se clasifican por dominio de la arquitectura empresarial en brechas de negocio/estrategia, información, sistemas de información, y servicios tecnológicos.

Basado en el análisis de la información documental existente, las mesas técnicas de levantamiento de información con los actores clave y los resultados del ejercicio de arquitectura, se identificaron las siguientes brechas clave que comprometen la capacidad de la entidad para la vigilancia, la inspección y el control. Las brechas son descritas en términos del dominio de arquitectura, la capacidad que impactan y el tipo de elemento de arquitectura asociado. A continuación, se describen los tipos de brechas encontrados:

- *Brechas de Planeación:* Corresponden a las brechas del dominio de negocio que actualmente no permiten desarrollar la planeación de las operaciones de Inspección, Vigilancia y Control de acuerdo con los resultados de la Analítica de Datos y Gestión de riesgos de incumplimiento del Sector y Servicios de telecomunicaciones y servicios postales. Las brechas de planeación incluyen aquellas que se relacionan con la definición de la metodología, el modelo de analítica predictiva y la gestión de proyectos de Inspección, Vigilancia y Control.
- *Brechas de Inspección:* Son las brechas del dominio de negocio que condicionan la capacidad de desarrollar de una manera óptima, el seguimiento, monitoreo y evaluación del cumplimiento de las obligaciones legales, reglamentarias, contractuales y regulatorias por medio de la recolección, confirmación y análisis de la información de los operadores, bien sea de manera presencial o remota. Estas brechas incluyen aquellas relacionadas con la solicitud y recolección de información de los operadores, la ejecución y desarrollo de las visitas de inspección y verificaciones remotas, así como la generación de informes de verificación de cumplimiento y la verificación de obligaciones en materia de abuso sexual infantil y adolescentes, y decomisos.
- *Brechas de Vigilancia:* Son las brechas que condicionan la capacidad para impartir las directrices e instrucciones a los operadores con el fin de advertir, prevenir, orientar, asistir y propender por el cumplimiento de sus obligaciones legales reglamentarias, contractuales y regulatorias. Incluyen las brechas relacionadas desde la verificación de presuntos incumplimientos, la verificación de los resultados de autogestión de los vigilados, la asistencia periódica a los vigilados, la emisión de conceptos de cumplimiento y comunicados.





- *Brechas de Control:* Corresponden a las brechas que condicionan la capacidad para decidir sobre los procesos que, por acción o por omisión de los sujetos vigilados, incumplen las obligaciones legales, reglamentarias, contractuales y regulatorias que les corresponden. Las brechas de control comprenden las relacionadas con i) adelantar las averiguaciones preliminares que resulten necesarias en el desarrollo de sus funciones de inspección y vigilancia para decidir las actuaciones producto de incumplimiento por parte de los vigilados, ii) llevar a cabo las diligencias de cierre de instalaciones o decomiso de presuntos prestadores informales de los sectores y servicios de TIC dispuestos en la normatividad vigente; iii) la atención de las solicitudes de investigaciones administrativas, hasta la determinación de consecuencias sancionatorias en primera instancia, entre ellos cierres, decomisos e investigaciones relacionadas con material de abuso sexual infantil y adolescentes, y iv) la verificación de la prestación informal de servicios de telecomunicaciones y servicios postales incluyendo la logística, ejecución de la diligencia de cierre de instalaciones o decomiso.

6.1. PORTAFOLIO DE PROYECTOS Y PLAN DE ACCIÓN

El desarrollo de la última etapa de la fase I del proyecto consistió en el análisis de brechas entre la situación actual (AS-IS) del modelo y el diseño su estado objetivo (TO-BE). Con base en el análisis de brechas se formuló un portafolio de programas y proyectos y la priorización de los proyectos de acuerdo con dos criterios que se desarrollan en la presente sección.

El portafolio de programas y proyectos busca alinear las capacidades institucionales para la instauración del nuevo Modelo de Inspección, Vigilancia y Control, con las tecnologías digitales para impulsar de manera radical la entrega de valor público a los ciudadanos y a la entidad.

El propósito de esta sección consiste en presentar una propuesta de prioridades para la lista de proyectos incluidos en este plan de implementación y migración de la Arquitectura Empresarial para el Modelo de Inspección, Vigilancia y Control. El programa de proyectos propuesto debe ser sometido previamente a un proceso de validación de prioridades que tenga en cuenta las restricciones internas de la entidad, los costos involucrados y los beneficios esperados con cada uno de ellos.

Inicialmente, se plantea que para el cierre de brechas se deben desarrollar 37 proyectos enmarcados en programas de los diferentes dominios de arquitectura, como se muestra en la siguiente ilustración:



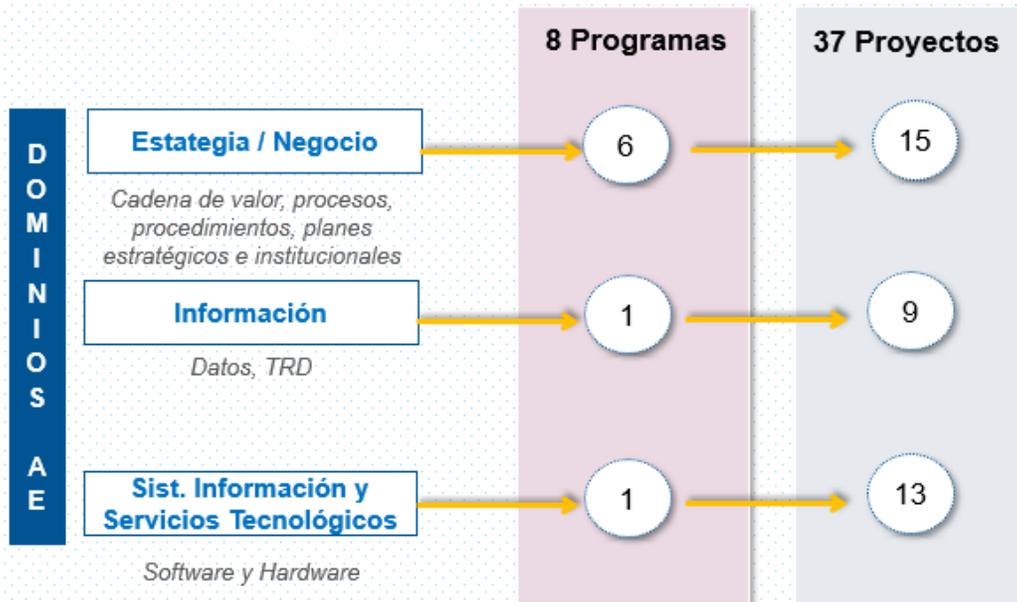


Ilustración 17. Programas y proyectos del plan de acción¹²

Fuente: MinTIC – UT Bisa Grow, 2020

Adicionalmente, se evaluó la prioridad de estos proyectos y se calculó un tiempo estimado para su ejecución. A continuación, se presenta una ilustración con los criterios empleados para clasificar los proyectos en tres niveles de priorización:

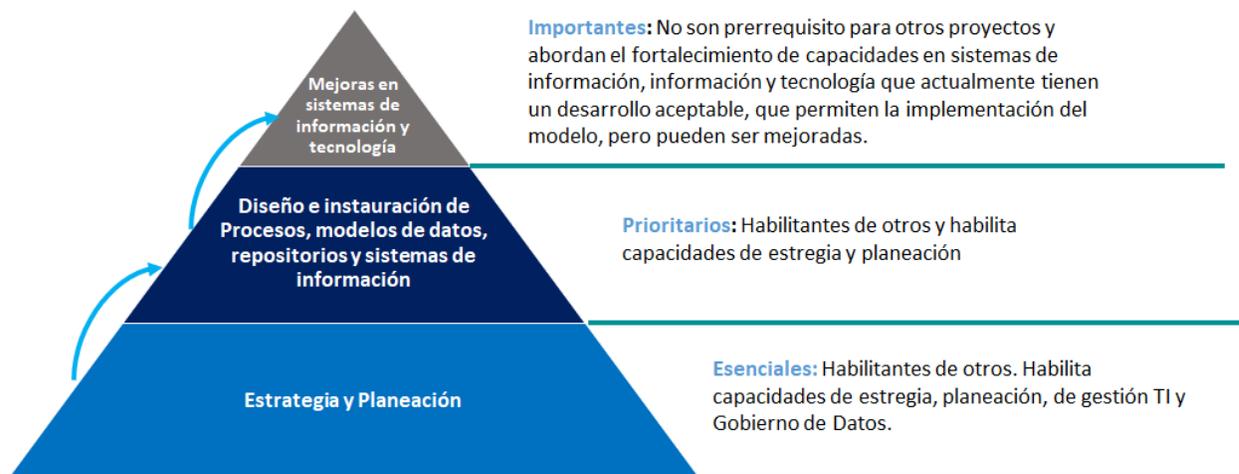


Ilustración 18. Criterios de priorización

Fuente: MinTIC – UT Bisa Grow, 2020

¹² Los programas agrupan proyectos relacionados con temáticas similares. En particular, se proponen los siguientes programas: 1) Habilitar los recursos para el desarrollo del nuevo modelo IVC; 2) Implementación de la Capacidad de Planeación; 3) Implementación de la Capacidad de Vigilancia; 4) Implementación de la Capacidad de Control; 5) Consolidación de la capacidad de Gobierno del Dato; 6) Implementación de la Capacidad de Recolección de información y; 7) Instaurar la capacidad de Arquitectura empresarial.

Para determinar los niveles de prioridad que se muestran en la ilustración anterior, se utilizaron los siguientes criterios de importancia relativa entre los proyectos:

- *Relaciones de precedencia:* Prerrequisitos entre proyectos.
- *Capacidades que impacta:* La propuesta de priorización impacta primero capacidades estratégicas y de planeación, que son requeridas para habilitar el desarrollo de procesos, sistemas de información y repositorios, para finalmente centrarse en capacidades que no son prerrequisito, pero que tienen oportunidad de mejora.

Adicionalmente, se tuvieron en cuenta tres periodos de tiempo estimado de los proyectos:

- Corto plazo (1 a 6 meses).
- Mediano plazo (6 meses a 1 año).
- Largo plazo (más de 1 año).

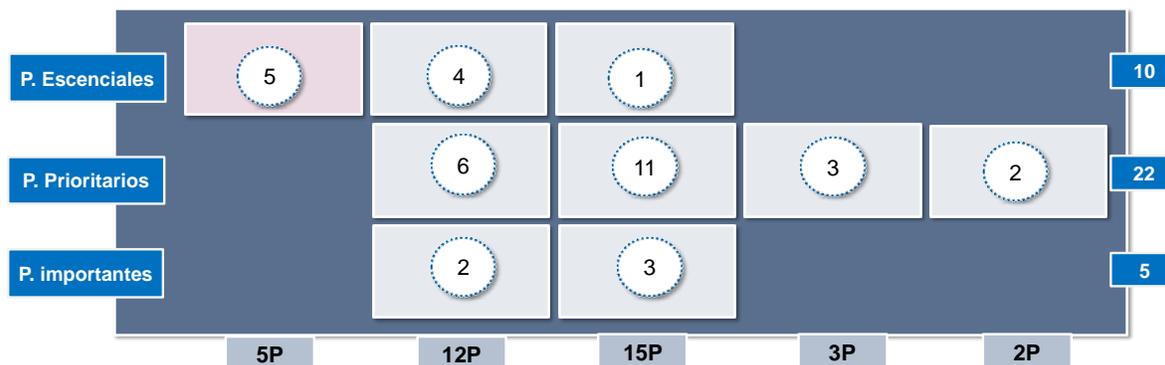


Ilustración 19. Resultados proyectos

Fuente: MinTIC, 2020.

La hoja de ruta o plan de acción esencial corresponde a la relacionada con los proyectos esenciales o básicos, los cuales impactan capacidades habilitantes para el Modelo de Inspección, Vigilancia y Control. Adicionalmente, estos proyectos son prerrequisitos de otros, y por ello se consideran esenciales.

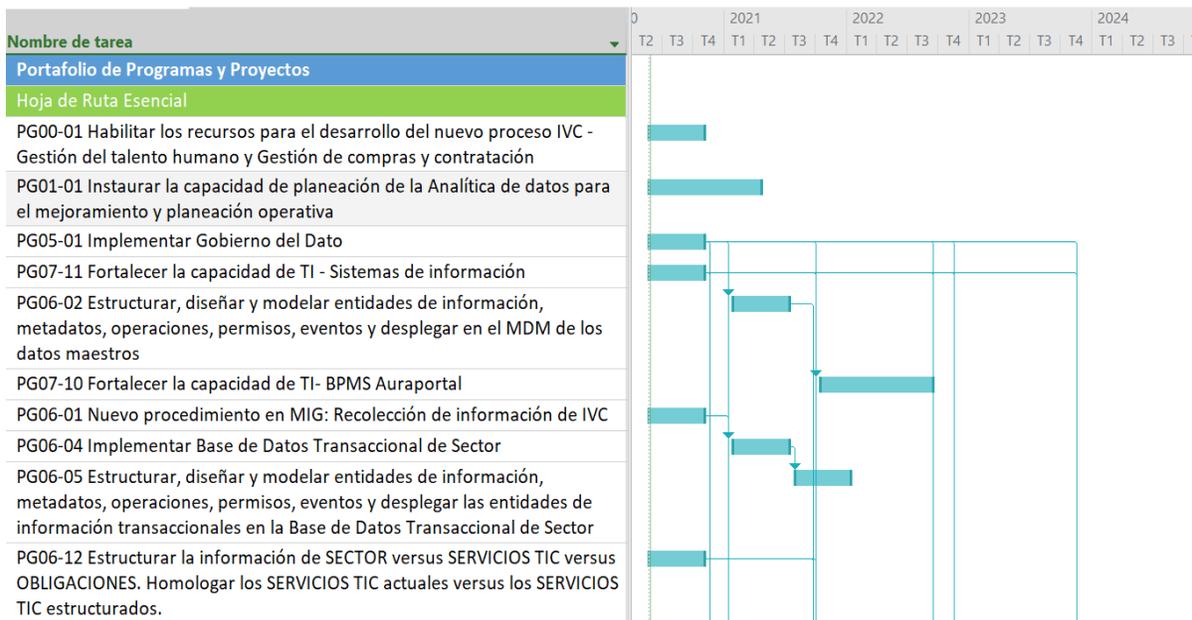


Ilustración 20. Hoja de ruta esencial
Fuente: UT Bisa Grow, 2020.

La hoja de ruta o plan de acción para proyectos con prioridad alta cierra las brechas para el diseño e instauración de procesos, modelos de datos, repositorios y sistemas de información específicos requeridos para la Vigilancia, Inspección y Control.



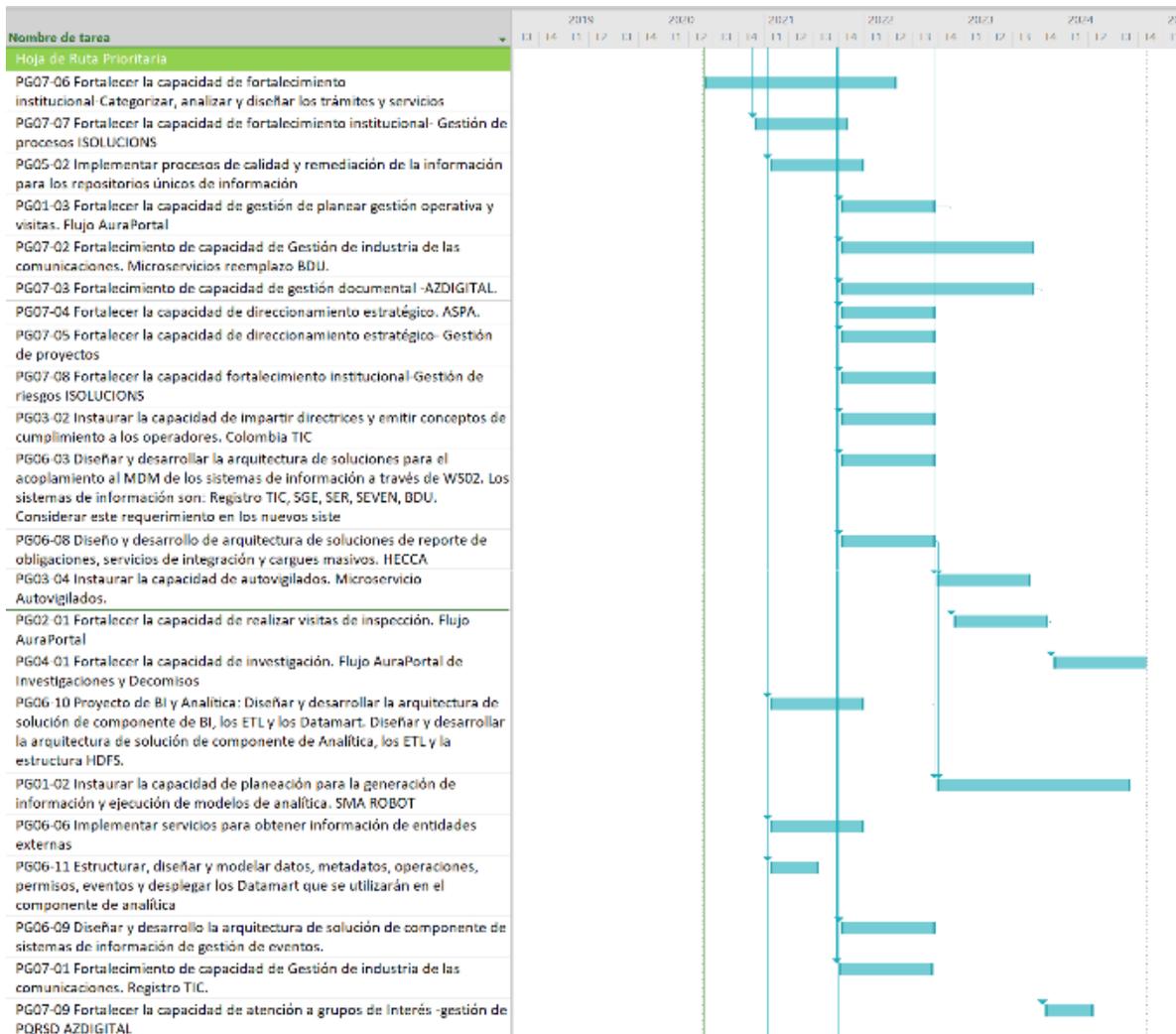


Ilustración 21. Hoja de ruta prioritaria

Fuente: UT Bisa Grow, 2020.

La hoja de ruta o plan de acción para proyectos importantes impacta capacidades en sistemas de información, información y tecnología que actualmente tienen un desarrollo aceptable para permitir la implementación del modelo, pero pueden ser mejoradas.

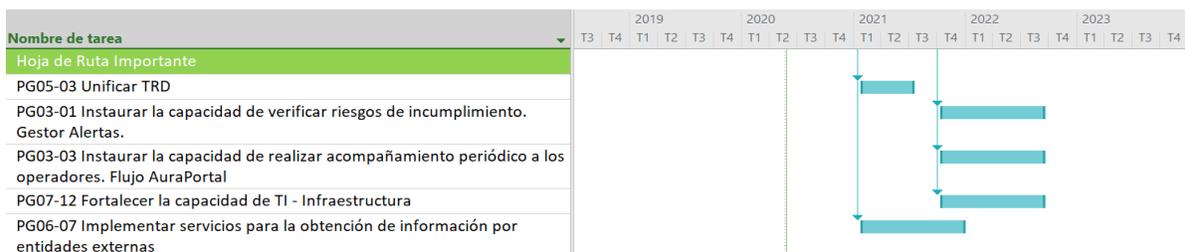


Ilustración 22. Hoja de ruta importante

Fuente: UT Bisa Grow, 2020.





Finalmente es importante tener en cuenta que, para la implementación del portafolio de proyectos, es necesario que se involucren otras áreas del MinTIC. Con lo anterior, es claro que la implementación del plan de acción constituye un proyecto de transformación digital de Entidad. Esto puede evidenciarse en la siguiente tabla:

Área responsable del Proyecto	2020	2021	2022	2023	2024	TOTAL
DIVC	3	8	7	3	1	22
Otras Áreas	2	4	8	0	1	15
- TI	2	1	2			5
- TI- Planeación		2	3			5
- TI - SG		1	1		1	3
- TI - Industria			2			2
TOTAL	5	12	15	3	2	37

Tabla 8. Mapa de ruta - áreas involucradas

Fuente: MinTIC, 2020.

Finalmente, es necesario aclarar que este plan de acción constituye la línea base para la implementación de la segunda fase del proyecto. Por lo tanto, el MinTIC podrá realizar ajustes con el fin de optimizar tiempos y recursos. Se buscará generar victorias tempranas y ejecutar la totalidad de los proyectos propuestos puedan implementarse dentro del periodo 2020 a 2022.



7. CONCLUSIONES

En conclusión, el desarrollo de este proyecto consistió en diagnosticar el estado actual del modelo de vigilancia y control, y proponer un nuevo modelo de Inspección, Vigilancia y Control preventivo y predictivo basado en analítica de datos, todo esto bajo un enfoque de arquitectura empresarial. Del estado actual (AS IS) y el estado deseado (TO BE) es posible concluir que con la segunda fase del proyecto se implementarán los desarrollos necesarios que permitirán alcanzar mejoras en cada dominio. Algunas de las mejoras más importantes que se plantean para el nuevo modelo de inspección, vigilancia y control son las siguientes:

Estrategia:

- Se unificarán las definiciones de sector TIC y de los servicios que lo componen con el fin de brindar total claridad sobre el objeto de inspección, vigilancia y control. Adicionalmente, se buscará centralizar información normativa en un único lugar donde se actualice automáticamente y donde pueda ser fuente de consulta para los vigilados.
- Se migrará a un modelo preventivo, basado en riesgos y que contiene la implementación de una estrategia de alto impacto en materia de divulgación normativa. Lo anterior en aras de prevenir el incumplimiento por desconocimiento. Todo esto será posible a través de la automatización de procesos y depuración, alistamiento y análisis de grandes volúmenes de información (Big data).
- Se tendrá una articulación permanente al interior de la entidad y con otras entidades como la Superintendencia de Industria y Comercio, la Comisión de Regulación de Comunicaciones y la Agencia Nacional del Espectro.

Negocio:

- El nuevo modelo reflejará los cambios que influyen sobre éste y que derivan de la normativa reciente, como las Leyes 1955 y 1978 de 2019.
- Se documentará todo el proceso del nuevo modelo con descripciones completas e interacciones entre procedimientos. Los procedimientos aplicarán a todos los vigilados y se actualizarán de acuerdo con la norma ISO 9001: 2015.
- Las matrices de obligaciones permitirán realizar labores de inspección y vigilancia bajo un enfoque de gestión de riesgos y se actualizarán con el uso de tecnologías. De igual forma, se buscará que todas las obligaciones que puedan verificarse de manera remota se verifiquen de esta manera.

Información:

- Se hará una transformación de la información que se encuentra en los diferentes sistemas, con el fin de evitar la existencia de datos replicados y sin interconectar.
- Se alcanzará una mayor alineación entre las tablas de retención documental (TRD) y el proceso actual.
- En todos los casos se proponen maneras adecuadas de almacenar la información relevante para el proceso.
- Se desarrollarán herramientas y procesos de Big Data.



- Los operadores podrán acceder a su propia información para autorregularse. Este es uno de los puntos clave del estado deseado del nuevo modelo, pues contando con información completa y oportuna sobre el cumplimiento de las obligaciones, se podrá prevenir el incumplimiento por parte de los vigilados. Este mayor cumplimiento deriva a su vez en mejores servicios para todos los usuarios de servicios de telecomunicaciones y servicios postales.

Sistemas de información:

- Se utilizarán las herramientas para realizar ejercicios de BI y Analítica en MinTIC, generando los procedimientos necesarios en la cadena valor del proceso de Inspección, Vigilancia y Control donde se asignen actividades de analítica.
- Los sistemas que actualmente son expuestos hacia el operador serán homogenizados en su presentación gráfica y presentados bajo los lineamientos de GOV.CO.
- Se proponen soluciones para lograr la interoperabilidad entre los sistemas involucrados en el proceso de inspección, vigilancia y control.

Servicios tecnológicos:

- Se fortalecerá la infraestructura de computo que aloja los principales sistemas que soportan el modelo de Inspección, Vigilancia y Control, con el fin disponer de recursos en alta disponibilidad que aseguren la continuidad de la operación en caso de un evento de fallo.
- Se dispondrá de mayor capacidad de servicios en nube para soportar las aplicaciones con las que interactúa la Dirección de Vigilancia y Control.

El objetivo principal del nuevo modelo es generar capacidades para que la Dirección de Vigilancia y Control, a través de sus procesos y sistemas de información, le disponga y facilite a los vigilados todas las herramientas operativas y tecnológicas para que estos conozcan mejor sus responsabilidades y obligaciones con respecto a los servicios de telecomunicaciones y postales que prestan. De igual forma, se busca aumentar el cumplimiento a través de acciones preventivas para que así los prestadores puedan ofrecer mejores servicios a los ciudadanos.

El diseño del nuevo modelo de IVC, se desarrolló basado en el estudio de modelos de referencia de otros países, recomendaciones de la OCDE, principios del Plan Nacional de Desarrollo, principios de gobierno digital del estado colombiano y marcos de trabajo internacionales de tecnologías de la información. Todo lo anterior, con el fin acatar las políticas de modernización del sector TIC, para simplificar y modernizar los procesos de Inspección, Vigilancia y Control, además de proponer un portafolio de proyecto que ayude a focalizar las inversiones en tecnología de la información para ser ejemplo de transformación digital en el país.



8. BIBLIOGRAFÍA

- Isoluciones SA. (2020). La solución tecnológica. Recuperado de <https://web.isolucion.com.co/>
- Riesgos Cero. (2020). Mapa de calor herramienta de gestión de riesgos. Recuperado de <https://www.riesgoscero.com/blog/mapa-de-calor-una-herramienta-para-optimizar-la-gestion-de-riesgos>
- Oreilly. (2020). Data Modeling in Hadoop. Recuperado de <https://www.oreilly.com/library/view/hadoop-application-architectures/9781491910313/ch01.html>
- Data Flair. (2020). Hadoop Architecture. Recuperado de <https://data-flair.training/blogs/hadoop-architecture/>
- Data Flair. (2020). Hadoop Analytics Tools. Recuperado de <https://data-flair.training/blogs/hadoop-analytics-tools/>
- Minería de Datos y Aprendizaje. (2020). Operational Data Store (ODS). Recuperado de <http://www.lsi.us.es/redmidas/CEDI/papers/933.pdf>
- Microsoft Azure. (2020). Extracción, transformación y carga de datos (ETL) a escala. Recuperado de <https://docs.microsoft.com/es-es/azure/hdinsight/hadoop/apache-hadoop-etl-at-scale>
- Microsoft Azure. (2020). Extracción, transformación y carga de datos (ETL) a escala. Recuperado de <https://docs.microsoft.com/es-es/dotnet/architecture/microservices/multi-container-microservice-net-applications/rabbitmq-event-bus-development-test-environment>
- Microsoft Azure. (2020). Microservicios. Recuperado de <https://docs.microsoft.com/es-es/azure/architecture/guide/architecture-styles/microservices>
- Microsoft Azure. (2020). Arquitectura orientada por eventos. Recuperado de <https://docs.microsoft.com/es-es/azure/architecture/guide/architecture-styles/event-driven>
- Google Cloud. (2020). Cómo implementar sistemas basados en secuencias de eventos con Cloud Spanner. Recuperado de <https://cloud.google.com/solutions/deploying-event-sourced-systems-with-cloud-spanner?hl=es-419>
- WSO2. (2020). Mensajería usando Tópicos. Recuperado de <https://docs.wso2.com/display/EI6xx/Pub-Sub+Messaging+using+Topics>
- AWS. (2020). What is Pub/Sub Messaging. Recuperado de <https://aws.amazon.com/es/pub-sub-messaging/>
- AWS. (2020). Arquitectura orientada a eventos. Recuperado de <https://aws.amazon.com/es/event-driven-architecture/>
- SOA PATTERNS. (2020). Patrones de arquitectura orientada a servicios. Recuperado de <https://patterns.arcitura.com/soa-patterns>
- SOA PATTERNS. (2020). Patrones de diseño de mensajería de eventos. Recuperado de https://patterns.arcitura.com/soa-patterns/design_patterns/event_driven_messaging
- Open Gropup. (2020). Arquitectura orientada por servicios SOA. Recuperado de <http://www.opengroup.org/soa/source-book/soa/index.htm>
- WSO2. (2020). Mensajería publicar y suscribir, usando tópicos. Recuperado de <https://docs.wso2.com/display/EI6xx/Pub-Sub+Messaging+using+Topics>
- MICROSOFT. (2020). Microservicios CRUD. Recuperado de <https://docs.microsoft.com/en-us/dotnet/architecture/microservices/multi-container-microservice-net-applications/data-driven-crud-microservice>
- MICROSOFT. (2020). API gateway pattern Microservicios. Recuperado de <https://docs.microsoft.com/en-us/dotnet/architecture/microservices/architect-microservice-container-applications/direct-client-to-microservice-communication-versus-the-api-gateway-pattern>



- DAFP. (2020). Modelo integrado de planeación y gestión. Recuperado de <https://www.funcionpublica.gov.co/web/mipgg>
- DAFP. (2020). Guía metodológica de racionalización trámites y servicios. Recuperado de https://www.funcionpublica.gov.co/documents/418537/506911/2017-12-04_Guia_metodologica_racionalizacion_tramites_ajuste.pdf/b00c472f-8872-4553-bfce-6c8f97403054
- MinTIC (2020). MIG. Recuperado de <https://simig.mintic.gov.co/Documentacion/frmlListadoMaestroDocumentos.aspx>
- MinTIC (2020). ¿Qué es la Dirección de Vigilancia y Control del MinTIC? Recuperado de <https://www.mintic.gov.co/portal/inicio/5236:Estandares-y-Tecnologias>
- MinTIC (2020). Dirección de Vigilancia y Control. Recuperado de <https://www.mintic.gov.co/portal/inicio/Ministerio/Viceministerio-de-Conectividad-y-Digitalizacion/Direccion-de-Vigilancia-y-Control/>
- MinTIC (2020). Modelo de Vigilancia y Control. Recuperado de https://es.slideshare.net/Ministerio_TIC/modelo-de-direccin-vigilancia-y-control-2016
- MinTIC (2020). Modelo de Vigilancia y Control. Recuperado de https://www.slideshare.net/Ministerio_TIC/modelo-de-vigilancia-y-control-de-los-sectores-tic-radiodifusin-sonora-y-postal
- MinTIC (2020). Acerca del MinTIC. Recuperado de <https://www.mintic.gov.co/portal/inicio/Ministerio/Acerca-del-MinTIC/>
- MinTIC (2020). Sector TIC. Recuperado de <https://www.mintic.gov.co/portal/inicio/Sector-TIC/>
- MinTIC (2020). Industria TIC. Recuperado de <https://www.mintic.gov.co/portal/604/w3-propertyname-545.html?noredirect=1>
- MinTIC (2020). Sector e Industria TIC. Recuperado de <https://www.mintic.gov.co/portal/604/w3-propertyname-605.html?noredirect=1>
- MinTIC (2020). Modelo de vigilancia y control de los sectores TIC. Recuperado de <https://www.mintic.gov.co/portal/inicio/2811:Modelo-de-vigilancia-y-control-de-los-sectores-tic-radiodifusion-sonora-y-postal>
- MinTIC (2020). ABC del Modelo de vigilancia y control. Recuperado de https://es.slideshare.net/Ministerio_TIC/abc-del-modelo-de-vigilancia-y-control
- MinTIC (2020). Normograma MinTIC. Recuperado de <https://normograma.mintic.gov.co/mintic/docs/arboll/1000.htm>
- MinTIC (2020). Manuales y Documentos. Recuperado de <https://mintic.gov.co/portal/604/w3-article-6442.html?noredirect=1>
- Estudio de la OCDE sobre políticas y regulación de telecomunicaciones en Colombia (2014). https://read.oecd-ilibrary.org/science-and-technology/estudio-de-la-ocde-sobre-politicas-y-regulacion-de-telecomunicaciones-en-colombia_9789264209558-es
- Revisión del gobierno digital en Colombia (2018). https://read.oecd-ilibrary.org/governance/revision-del-gobierno-digital-en-colombia_9789264292147-es
- OECD Reviews of Digital Transformation: Going Digital in Colombia (2019) https://read.oecd-ilibrary.org/science-and-technology/oecd-reviews-of-digital-transformation-going-digital-in-colombia_781185b1-en
- MinTIC (2020). Colombia TIC. Recuperado de <https://www.mintic.gov.co/portal/inicio/Sector-TIC/Colombia-TIC-Estadisticas/>





IBM (2020). SPSS Statistics Software. Recuperado de <https://www.ibm.com/co-es/analytics/spss-statistics-software>

Microsoft (2020). What is power bi. Recuperado de <https://powerbi.microsoft.com/es-es/what-is-power-bi/>

Microsoft (2020). What is SQL Server Reporting Services. Recuperado de <https://docs.microsoft.com/en-us/sql/reporting-services/create-deploy-and-manage-mobile-and-paginated-reports?view=sql-server-ver15>

WSO2(2020). Enterprise service Bus. Recuperado de <https://wso2.com/products/enterprise-service-bus/>

MinTIC (2020). SGE. Recuperado de <https://www.mintic.gov.co/portal/inicio/Sistemas-MINTIC/SGE-Sistema-de-Gestion-del-Espectro/>

MinTIC (2020). Siust. Recuperado de <https://www.siust.gov.co/siust/>

MinTIC (2020). Manual de Usuario BDU. Recuperado de <https://www.mintic.gov.co/portal/inicio/2209:BDU>

Archivar LTDA. (2020). Producto. Recuperado de <http://www.archivarltda.com/>

AuraPortal (2020). Que es AuraPortal. Recuperado de <https://www.auraportal.com/es/>

DigitalWare (2020). ERP Seven. Recuperado de <http://www.digitalware.com.co/index.php/verticales/seven-erp-solucion-erp-basada-en-procesos>

MinTIC (2020). SER. Recuperado de <https://ser.mintic.gov.co/Home/About>

MinTIC (2020). Estándares y Tecnologías. Recuperado de <https://www.mintic.gov.co/portal/inicio/5236:Estandares-y-Tecnologias>

MinTIC (2020). Registros TIC y Postal. Recuperado de <https://www.mintic.gov.co/portal/inicio/Atencion-al-Publico/UTIC-Ventanilla-Unica-de-Tramites/Registros/>

MinTIC (2020). Aura Portal - Registros TIC y Postal. Recuperado de https://bpm.mintic.gov.co/AP/login.aspx?ReturnUrl=%2fAP%2fBPM_Mensajes_Crear.aspx%3fid%3d1072%26pag%3d107%26idPortal%3d0&id=1072&pag=107&idPortal=0

MinTIC (2020). Sector e Industria TIC. Recuperado de https://www.mintic.gov.co/portal/604/w3-propertyname-605.html?_noredirect=1

MinTIC (2020). Glosario MinTIC. Recuperado de <https://www.mintic.gov.co/portal/inicio/Glosario/>

MinTIC (2020). Sistemas MinTIC. Recuperado de <https://www.mintic.gov.co/portal/inicio/Sistemas-MINTIC/>

MinTIC (2020). Manual de Usuario BDU. Recuperado de <https://www.mintic.gov.co/portal/inicio/2209:BDU>

MinTIC (2020). Activos de información. Recuperado de <https://www.datos.gov.co/Ciencia-Tecnolog-a-e-Innovaci-n/Esquema-de-publicaci-n-e-informaci-n/uxzi-vdaj>

WEF (2016) The Fourth Industrial Revolution: what it means, how to respond. Publicado el 14 de Enero de 2016. Recuperado de: <https://www.weforum.org/agenda/2016/01/the-fourthindustrial-revolution-what-it-means-and-how-to-respond/>