



CONTRATO DE CONSULTORIA ELECTRÓNICO SECOP II No.
287 DEL 2021 CELEBRADO ENTRE LA SUPERINTENDENCIA
DE TRANSPORTE Y GROW DATA SAS.



Modelo de Operación SICOV

Versión 0.3

Modelo de Operación - SICOV

CONTRATO DE CONSULTORÍA 287 DE 2021

Diciembre de 2021

Contrato No. 287 de 2021

Objeto del Contrato: Contratar el servicio de consultoría especializada para la elaboración de los estudios, diseños y modelos de las condiciones técnicas, administrativas, tecnológicas, financieras y jurídicas para identificar y definir la alternativa o propuesta necesaria para el funcionamiento en la instalación, implementación, operación y mantenimiento del sistema de control y vigilancia -SICOV-, que le permita a la Superintendencia de Transporte la vigilancia, inspección y control del manejo legal y reglamentario al que están sujetos los organismos de Apoyo a las Autoridades de Tránsito (OAT)..





CONTROL DE VERSIONES			
VERSIÓN	FECHA	ELABORADO POR	MOTIVO
0.1	29/10/2021	Mario Briceño / Giovanni Serrano	Creación inicial del documento

REFERENCIAS CONTRACTUALES DEL ENTREGABLE:
Contrato de consultoría 287 de 2021 – SICOV entre Grow Data y la Superintendencia de Transporte, diagnóstico técnico.

APROBACIÓN POR LA ENTIDAD			
NOMBRE	ROL	FIRMA	FECHA
Dra. Adriana Margarita Urbina Pinedo	Supervisora Contrato de consultoría 287 de 2021 - SICOV		30-12-2021
Ing. Jorge Guillermo Neira Bossa	Supervisor Contrato de consultoría 287 de 2021 - SICOV		30-12-2021

APROBACIÓN POR GROW DATA			
NOMBRE	ROL	FIRMA	FECHA
Ing. Mario Briceño	Gerentes de Proyecto Grow Data Contrato de consultoría 287 de 2021 - SICOV		30-12-2021
Ing. Giovanni Serrano	Gerente de Proyecto Grow Data		30-12-2021



Contenido

1	Introducción	6
2	Objetivo	7
3	Marco Metodológico.....	7
3.1	Componente Jurídico.....	8
3.2	Componente Financiero	10
3.3	Componente Tecnológico.....	13
4	Análisis de los modelos de operación propuestos para SICOV	14
4.1	Modelo de operación actual.....	14
4.2	Modelo de operación Federado	16
4.3	Modelo Centralizado	18
5	Modelo Alternativo – Esquema Federado	20
5.1	Arquitectura de sistemas de información federado	20
5.1.1	Arquitectura conceptual SICOV federado	21
5.1.2	Diagrama de interoperabilidad de los sistemas o aplicaciones modelo federado	29
5.2	Arquitectura de Datos Modelo Federado	30
5.2.1	Arquitectura Conceptual TO BE - CDA.....	30
5.2.2	Arquitectura Conceptual TO BE - CRC	33
5.2.3	Arquitectura Conceptual TO BE - CEA	36
5.2.4	Arquitectura Conceptual TO BE - CIA	38
5.2.5	Arquitectura Conceptual TO BE - CALE.....	41
6	Modelo Propuesto – Esquema Centralizado	43
6.1	Principales preocupaciones	43
6.2	Controles.....	44
6.3	Análisis tecnológico del esquema centralizado	46
6.3.1	Gestión Integral de Servicios basados en tecnología.....	46
6.3.2	Riesgos asociados al modelo centralizado	47
6.3.3	Centros de Datos definidos por software	49
6.4	Estructura conceptual del Modelo Centralizado	49
6.5	Arquitectura de Referencia del Modelo Centralizado	51



6.5.1	Zona de canales.....	52
6.5.2	Zona de seguridad	53
6.5.3	Zona transversal	53
6.5.4	Zona misional.....	53
6.5.5	Zona control	53
6.5.6	Zona de interoperabilidad	53
6.5.7	Zona de eventos.....	53
6.5.8	Zona de dispositivos físicos	54
6.5.9	Zona de almacenamiento	54
7	Instalación, Implementación, Operación y Mantenimiento.....	55
7.1	Plazos de ejecución	55
7.2	Requerimientos técnicos para el inicio	56
7.3	Requerimientos técnicos para la instalación – implementación	57
7.4	Requerimientos técnicos para la operación y mantenimiento.....	59
7.5	Parámetros, metas de control y desempeño.....	61
7.5.1	Acuerdos de niveles de servicio	61
7.5.2	Análisis de la Gestión.....	68
8	Aspectos Técnicos Contractuales.....	68
8.1	Perfiles técnicos de las empresas – análisis del sector	68
8.1.1	Perspectivas del sector	69
8.1.2	Evolución del subsector de servicios de tecnologías de la información tic	70
8.1.3	Composición del sector TIC en Colombia	73
8.1.4	Perfil técnico detallado	74
8.2	Perfiles de los profesionales claves	77



Ilustraciones

Ilustración 1 - Componentes consultivos – SICOV	7
Ilustración 2 - SICOV Actual	15
Ilustración 3 - SICOV - Federado	17
Ilustración 4 - SICOV Centralizado	19
Ilustración 5 Diagrama conceptual SICOV Federado.....	21
Ilustración 6 Arquitectura de referencia sistemas de información SICOV-CRC.....	23
Ilustración 7 Arquitectura de referencia sistemas de información SICOV-CEA	25
Ilustración 8 Arquitectura de referencia sistemas de información SICOV-CALE	26
Ilustración 9 Arquitectura de referencia sistemas de información SICOV-CIA	27
Ilustración 10 Arquitectura de referencia sistemas de información SICOV-CDA	28
Ilustración 11 Diagrama de interoperabilidad SICOV federado TO BE.....	29
Ilustración 12. Arquitectura Conceptual TOBE - CDA	30
Ilustración 13. Arquitectura Conceptual TOBE - CRC	33
Ilustración 14. Arquitectura Conceptual TOBE - CEA.....	36
Ilustración 15. Arquitectura Conceptual TOBE - CIA.....	38
Ilustración 16. Arquitectura Conceptual TOBE - CALE	41
Ilustración 17 - Modelo Propuesto SICOV Centralizado	49
Ilustración 18 – Arquitectura de referencia modelo centralizado	52
Ilustración 19 - Plazo de Ejecución	55
Ilustración 20 - fuerza laboral en Colombia - 2017	71



1 Introducción

El contrato 287 del 2021 celebrado entre la Superintendencia de Transporte y Grow Data SAS, dentro de sus objetivos de alto nivel se encuentra identificar y definir la mejor alternativa para la instalación, implementación, operación y mantenimiento del sistema de control y vigilancia -SICOV-, que le permita a la Superintendencia de Transporte la vigilancia, inspección y control del manejo legal y reglamentario al que están sujetos los organismos de Apoyo a las Autoridades de Tránsito (OAT).

Para dar cumplimiento al objetivo planteado y teniendo en cuenta que la estructura del presente proyecto se basa sobre tres líneas consultivas (Tecnológica, Jurídica y Financiera), se define como estrategia táctica el desarrollar el proyecto siguiendo estas líneas consultivas de forma paralela e independiente, pero sin perder de vista que la solución final debe guardar una completa alineación y coherencia entre las definiciones que se desarrollen dentro de cada línea consultiva.

Entendiendo el reto por afrontar, se definen actividades y objetivos propios de cada línea consultiva, a la vez que se definen elementos consultivos transversales que buscan identificar y asegurar esos puntos de convergencia entre todos los ámbitos de la presente consultoría, con el objetivo de generar un resultado completamente integrado y coherente en sus definiciones.

El presente documento toma los resultados y definiciones realizadas en cada una de estas líneas consultivas con el fin de presentar las alternativas de operación analizadas y detallar el modelo seleccionado para el Sistema de Control de Vigilancia – SICOV dadas sus ventajas.

Adicionalmente, en el presente documento se definen los requerimientos técnicos necesarios para la instalación, implementación, operación y mantenimiento de SICOV. De igual forma, se presentan los indicadores de gestión mediante los cuales se apoya la definición de los elementos de control del concesionario de SICOV para de esta forma tener elementos objetivos para establecer el desempeño y nivel de cumplimiento de las obligaciones establecidas.

2 Objetivo

El objetivo del Modelo de Operación SICOV es el de presentar las diferentes opciones de solución identificadas y analizadas, para de esta forma llegar a plantear el modelo final propuesto.

De igual forma, se presenta el alcance, especificaciones, plazos para la instalación, implementación, operación y mantenimiento de la arquitectura objetivo definida para SICOV, dentro de la cual se incluyen parámetros, metas de control y desempeño para la medición y control de la ejecución del contrato.

3 Marco Metodológico

A nivel metodológico, el desarrollo del proyecto ha construido diferentes documentos en cada uno de los ámbitos que lo estructuran, siendo el componente jurídico, el componente financiero el componente técnico y el componente tecnológico los ámbitos que se han desarrollado a nivel consultivo.

Ilustración 1 - Componentes consultivos – SICOV



Fuente: Desarrollo propio, Grow Data 2021

Dentro de cada uno de estos ámbitos se han descrito todos los marcos metodológicos sobre los cuales se soportan, siendo TOGAF 9.2 el marco de trabajo de Arquitectura Empresarial y el Marco de Referencia de Arquitectura Empresarial MRAE que desde el ámbito tecnológico soportan metodológicamente el desarrollo de este componente.

Dentro del ámbito jurídico, se encuentran dos grandes líneas que soportan las definiciones realizadas : (i) la normatividad colombiana vigente y (ii) las normas de calidad aplicables.

Para encontrar mayor detalle a nivel metodológico, se podrán consultar los documentos que en cada uno de estos ámbitos se han producido. Para el caso del desarrollo del presente documento, se retoman los conceptos que de forma general se han definido en cada uno de estos ámbitos y se aplican a la estructuración del modelo operación teniendo en cuenta los principales lineamientos de cada uno de estos ámbitos los cuales a continuación se describen basados en los siguientes escenarios:

- Escenario 1: Un operador / concesionario por cada tipo de OAT
- Escenario 2: Un operador / concesionario para todos los tipos de OAT

3.1 Componente Jurídico

Dentro del ámbito jurídico se tiene el objetivo de identificar entre otros:

- La titularidad de la información que se genere en el sistema (software),
- La naturaleza jurídica de los cobros, tarifas o aportes propios de cada modelo
- Los posibles escenarios para la puesta en funcionamiento del SICOV a la luz de lo dispuesto en el Ley 2050 de 2020
- Las normas constitucionales y legales sobre libre competencia, para efectos de determinar las implicaciones, modelos o alternativas tengan frente a los tipos de OAT y los usuarios.

Para el desarrollo estructurado del análisis jurídico, se tienen en cuenta las diferentes normas de carácter Constitucional y Legal, en especial, aquellas que tienen como disposición la protección de libre competencia económica, con la finalidad de determinar las posibles implicaciones que traigan consigo los posibles escenarios planteados, para dar cumplimiento a lo dispuesto en el artículo 22 de la Ley 2050 de 2020, de cara a los diferentes tipos de Organismos de Apoyo a las Autoridades de Transito (OAT) y los usuarios finales.

En concordancia con lo enunciado anteriormente, el análisis realizado se estructuró de la siguiente manera:



1. Análisis del marco regulatorio actual relacionado con el Sistema de Control y Vigilancia de la Superintendencia de Transporte, así como, la diferente normativa que establece las reglas de operación y registro de los Organismos de Apoyo a las Autoridades de Tránsito (OAT) en especial, aquellas que han sido expedidas por el Ministerio de Transporte y la Superintendencia de Transporte como Órgano de Inspección Vigilancia y Control.
2. Análisis del alcance dispuesto en el artículo 22 de la Ley 2050 de 2020 "*Por medio de la cual se modifica y adiciona la Ley 1503 de 2011 y se dictan otras disposiciones en Seguridad Vial y Tránsito*", con el objetivo de establecer dentro del marco del Sistema de Compra Pública, cuál sería la tipología contractual más idónea para contratar el servicio de instalación, implementación, operación y mantenimiento del Sistema de Control y Vigilancia-SICOV.
3. Conclusiones del análisis de las diferentes opciones, modelos o alternativas planteadas para dar cumplimiento a lo dispuesto en el artículo 22 de la Ley 2050 de 2020, de cara a los diferentes tipos de Organismos de Apoyo a las Autoridades de Tránsito (OAT) y los usuarios.

El detalle del desarrollo realizado y las respectivas conclusiones podrá ser consultado en los documentos entregables del ámbito jurídico (Análisis de la estructura jurídica, Informe Final).

Dentro del ámbito jurídico y luego de haber hecho un análisis respecto de la conveniencia, viabilidad, y ventajas de los escenarios propuestos, Grow Data a través de su equipo consultor y luego del respectivo análisis identifica que el modelo centralizado tiene jurídicamente más ventajas que el modelo distribuido argumentado a través de los siguientes conceptos generales:

- **Estructuración del proceso (precontractual y contractual):** contemplando la dificultad y el esfuerzo requerido para estructurar todo un proceso contractual, se identifica que a través de un modelo centralizado esta dificultad disminuye al tener que hacer un solo proceso y no cinco procesos contractuales como lo demandaría el modelo de un homologado por cada tipo de OAT.
- **Supervisión del contrato:** las labores de supervisión y control sobre un modelo centralizado optimizan el uso de recursos y enfocan a la entidad en un solo contrato / proveedor haciendo que estas labores puedan ser ejecutadas con menores recursos y con menores requerimientos (financieros, administrativos, logísticos, técnicos) hacia la Superintendencia de Transporte.
- **Finalización del contrato:** una de las grandes dificultades identificadas en el país a nivel contractual es la finalización del contrato y el inicio de uno nuevo. Cuando la

entidad hace esa transición con el mismo operador el proceso es simple y no genera mayores impactos en la operación. Dado que jurídicamente esto no es posible garantizar es necesario prever que al finalizar el contrato de adjudicación sea un nuevo operador (concesionario) quien llegue a tomar la operación. En este caso, y por experiencias de diferentes entidades estatales el cambio de operador genera en muchos casos, traumatismo en la operación, es por esto que jurídicamente se contemplan cláusulas que a través de un modelo centralizado (un solo concesionario), facilitarán estas transiciones, aspecto que con un modelo distribuido (un homologado / concesionario por OAT) aumentaría dramáticamente la complejidad de estas labores.

- **Labores de control financiero:** a través de un modelo centralizado se emplearía un modelo de recaudo y control financiero el cual dentro de sus obligaciones estaría el de aportar toda la información requerida (frecuencia - detalle) para las labores de supervisión y control financiero respecto del recaudo gestionado a nivel de SICOV. A través de un modelo distribuido, estas labores aumentan su complejidad dado que es muy probable que cada concesionario utilice mecanismos de recaudo diferentes dificultando de esta forma la recolección, centralización y análisis de esta información, así como el proceso de dispersión de los valores de la tarifa.

3.2 Componente Financiero

La definición del modelo financiero es utilizada para establecer la estructura financiera de una empresa, proyecto o línea de negocio, entre otros. Estos modelos se basan en datos históricos, la situación estructural y las proyecciones estimadas.

El proceso de construcción del modelo financiero para SICOV parte de la identificación de las fuentes de ingresos, sus costos, su estructura de capital, endeudamiento, etc., así como todos los factores externos que influyen en la estructura financiera.

El modelo financiero se basa en lo que sería una operación normal de SICOV, considerando las principales variables que puedan afectar en un momento dado el desarrollo del Sistema que nos compete. Un buen modelo es lo suficientemente detallado como para no dejar ningún factor clave fuera, pero a la vez simple como para que se pueda seguir usando por parte de los usuarios del modelo y de la información generada.

Teniendo en cuenta lo anterior y para realizar un análisis comparativo entre los dos escenarios más convenientes para definir el modelo operativo de SICOV, se seleccionaron las variables que estructuran el modelo financiero para de esta forma identificar desde el punto de vista de costos, cuál podría ser el más conveniente para la Supertransporte. Las variables analizadas son los costos relacionados con:

- **Centro de Procesamiento de Datos (CPD) - Principal:**

Dentro de este ítem se incluyen todos los elementos de la infraestructura tecnológica de software y hardware requerido para el soporte y operación de SICOV. Para el escenario uno, cada homologado deberá tener su data center y su propia infraestructura. En el escenario 2, bajo la figura de un modelo centralizado, el tener un sólo centro de procesamiento de datos se identifica eficiencia a nivel de costos al no tener que duplicar canales de comunicación, unificación a nivel de equipos de seguridad y red perimetral.

De igual forma la infraestructura adquirida puede ser fácilmente reutilizada para las diferentes funciones de los OAT. Esto implica que luego de haber instalado y puesto en operación la infraestructura del primer tipo de OAT, el resto de las implementaciones podrá aprovechar esta infraestructura y crecer de forma eficiente encontrando allí grandes eficiencias a nivel de costos al simplemente tener que aumentar la capacidad de la infraestructura y no tener que incurrir en compras adicionales.

- **Ambiente secundario / Data Center contingencia (CPD secundario)**

El ambiente secundario o de contingencia debe entrar en operación en el caso que el ambiente primario tenga una indisponibilidad total o parcial. Esto implica tener la misma infraestructura replicada en este ambiente de contingencia, pero para efectos de operación se estima que la infraestructura de contingencia debe mantener las mismas características técnicas, pero al 60% a nivel de dimensionamiento y por ende encontrar de esta forma una reducción de costos adicional sin dejar de cumplir con los conceptos de disponibilidad, capacidad o desempeño.

- **Equipos para la operación SICOV OAT**

Haciendo un análisis entre los dos escenarios, no fue posible cuantificar un porcentaje de disminución entre los costos de los kits requeridos para el apoyo a la operación. Si bien esto es cierto, se identifica una clara posibilidad de reducción de costos asociados a economías de escala, dado que si un solo operador realiza la compra de todos los elementos es muy probable que los fabricantes ofrezcan porcentajes de descuento por este tipo de compras en volumen. Para la identificación detallada de los elementos que conforman los kits de cada OAT, consultar los documentos: SICOV KIT CRC Costos – Precio, SICOV KIT CEA Costos – Precio, SICOV KIT CIA Costos – Precio, SICOV KIT CALE Costos – Precio, SICOV KIT CDA Costos – Precio.

- **Mantenimiento**

Los costos asociados al mantenimiento a nivel de software y hardware son dependientes de los costos del CPD primario y el CPD secundario. Por tanto, una reducción en estos costos, directamente incidirán en los costos de mantenimiento. El porcentaje de reducción a nivel

de costos de la infraestructura tecnológica tendrá un porcentaje igual de reducción en el mantenimiento. Adicionalmente, se contempla un costo de mantenimiento asociado al Sistema de Información de Control y Vigilancia el cual se enfoca en cambios evolutivos, inclusión de nuevas funcionalidades y estabilización de la funcionalidad.

- **Rehabilitación y Mejoramiento**

Los costos asociados al mejoramiento y rehabilitación de la infraestructura de software y de hardware son dependientes de los costos del CPD primario y el CPD secundario. Por tanto, el porcentaje de ahorro a nivel de costos en la infraestructura tecnológica tendrá un porcentaje igual de reducción en los costos de rehabilitación y mejoramiento, entendiéndose estos costos como los derivados de daños, pérdida, hurto, daños por fluido eléctricos y en general, todos aquellos eventos no contemplados y que no pueden ser considerados dentro del concepto de garantía y mantenimiento

- **Desarrollo software**

En cuanto a los costos de desarrollo de software y analizando los dos escenarios posibles para SICOV, en el escenario dos se identifica un porcentaje de ahorro de al menos el 20% derivado de la unificación de esfuerzos a nivel de desarrollo de software, de la cantidad de personas requeridas, infraestructura tecnológica para el desarrollo del software y en general, la disminución del tiempo de desarrollo del software, el cual redundará en utilizar de igual forma menos tiempo el personal o la infraestructura, disminuyendo de esta forma los costos directos de desarrollo.

Adicionalmente, se identifican aspectos que a través de la centralización del desarrollo se ven positivamente impactadas dado que serán ejecutadas de forma optimizada: comparativamente se podrán ejecutar en menores tiempos y con mejores indicadores de efectividad (menor cantidad de errores):

- Estandarización a nivel de código y componentes
- Automatización de pruebas
- Unificación de reglas de negocio

- **Monitoreo y control**

Al comparar los costos asociados a los servicios de monitoreo NOC / SOC requeridos para la operación de SICOV, se identifica que el modelo centralizado puede optimizar sus costos en aproximadamente un 20% a través de un uso más eficiente de puestos de trabajo, personal de monitoreo, infraestructura de software y hardware, así como de los costos de licenciamiento de los aplicativos propios de SOC / NOC.

- **Soporte**

Al identificar los costos asociados al soporte técnico y funcional de SICOV, se encuentra que bajo el escenario dos (Modelo Centralizado) se pueden encontrar eficiencias a nivel de costos que pueden llegar a ofrecer hasta un 30% de ahorro al poder optimizar el uso de puestos de trabajo, cantidad de personal, mejor aprovechamiento de la infraestructura de software y hardware.

- **Administración y Gestión**

Una vez identificados los costos de administración y gestión, los cuales en su gran mayoría están asociados a costos de nómina, costos operativos, elementos y servicios requeridos en administración y gestión de SICOV, se evidencia que a través de la centralización de todos estos requerimientos administrativos se pueden tener eficiencia a nivel de costos de aproximadamente un 30%. Este ahorro se puede asociar directamente a la reducción de costos de por ejemplo arrendamientos, reducción de puestos de trabajo, optimización del personal requerido entre otros aspectos.

El detalle del modelo financiero que soportan los porcentajes de ahorro en costos podrá ser consultado en los documentos generados desde el ámbito financiero: Análisis del Modelo Financiero, Modelo Financiero y los soportes respectivos.

3.3 Componente Tecnológico

A nivel metodológico general, el diseño del modelo de operación se alinea con el Diagnóstico Tecnológico, Diagnóstico Técnico y el Documento de Definición de Arquitectura (ADD), a fin de tener una completa alineación entre todas las definiciones realizadas a nivel de:

- Enfoque a nivel de Arquitectura Empresarial desarrollando los temas relacionados alrededor de estos ámbitos.
- Definición de la Arquitectura empresarial Objetivo para SICOV.
- Identificación detallada de la situación actual del sistema de control y vigilancia.
- Análisis de las diferentes alternativas de solución.

El cumplimiento de los anteriores conceptos en primera instancia se describe en el documento de diagnóstico técnico y documento diagnóstico tecnológico desarrollado en la fase dos del presente proyecto "Estudio y Diagnóstico". De igual forma, en la fase tres "Evaluar y Proponer" se desarrolla el documento definición de arquitectura – ADD, siendo la

descripción de la situación actual (AS-IS) un componente de este entregable permitiendo su consulta y ofreciendo información detallada respecto de la situación actual de SICOV.

El presente documento retoma los diagnósticos jurídicos, financieros, técnicos y tecnológicos para describir las fortalezas y debilidades de la actual operación de SICOV. Con base en esta información, se desarrolla el modelo de operación propuesto, el cual está alineado a las definiciones realizadas a nivel de arquitectura objetivo TO-BE.

A continuación, se presenta el análisis realizado de las diferentes opciones, modelos y alternativas identificadas para la operación del sistema de control y vigilancia – SICOV, alineando este análisis con las definiciones realizadas a nivel de arquitectura de negocio y arquitectura de T.I.

4 Análisis de los modelos de operación propuestos para SICOV

4.1 Modelo de operación actual

Es importante precisar, que en la actualidad, existen diferentes estructuras tecnológicas, las cuales son operadas y de propiedad de cada uno de los cinco operadores que a la fecha se encuentran homologados o autorizados por parte de la Superintendencia de Transporte para apoyar en la función de vigilancia y control a través de Sistema de Control y Vigilancia SICOV.

Tabla - Actuales Homologados

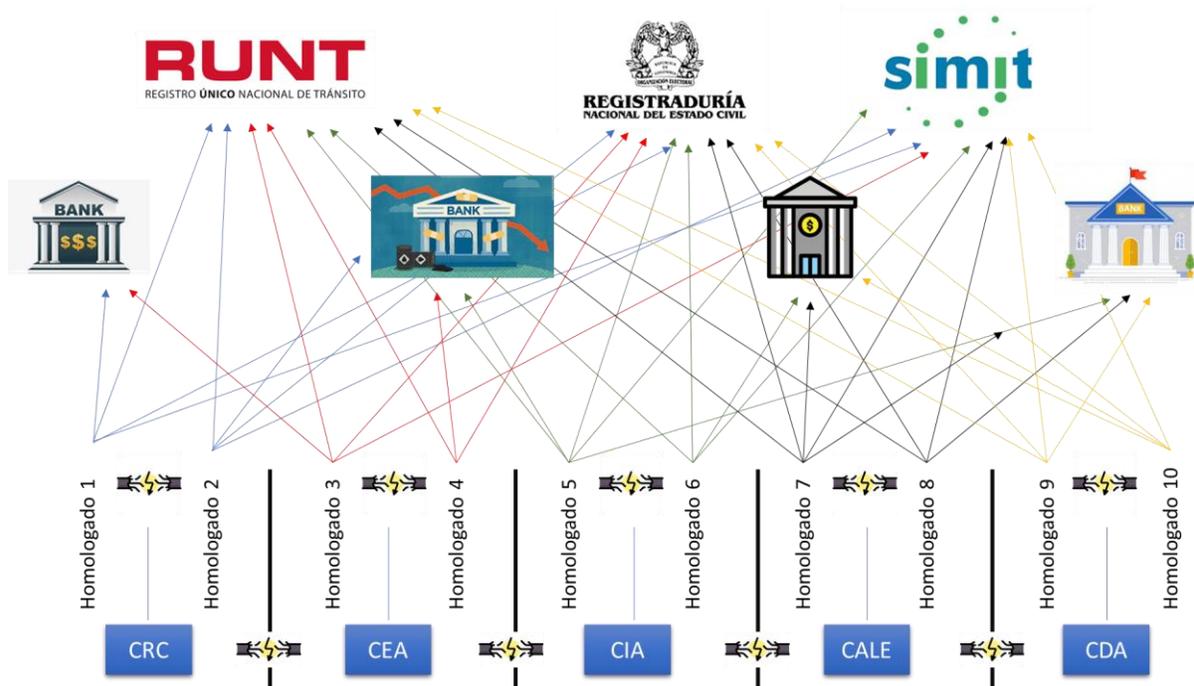
OAT	HOMOLOGADO
CRC	Olimpia IT S.A.S
	Consorcio SICOV - CRC
CDA	Compañía Internacional de Integración S.A. - CI2 S.A.
	Indra Sistemas S.A.
CEA	Olimpia IT S.A.S
	Consorcio Sistema Integrado de Gestión y Seguridad para CEAS y CIAS

CIA	Sin apoyo tecnológico
CALE	Sin operación

Fuente: Desarrollo propio, Grow Data 2021

Este fenómeno de tener una multiplicidad de operadores, genera que cada uno de ellos tenga diferentes procedimientos internos, así como plataformas tecnológicas y sistemas de información para desarrollar las diferentes actividades para las cuales fueron autorizados u homologados; además, no existen estándares para el registro e intercambio de información, impidiendo tener una uniformidad en los procedimientos e incluso en las tarifas que pueden llegar a cobrar por determinado servicio prestado, lo cual trae implicaciones para los consumidores finales, es decir, todos aquellos que requieren acceder a los servicios que presta cada uno de estos organismos.

Ilustración 2 - SICOV Actual



Fuente: Desarrollo propio, Grow Data 2021



A través de la información proporcionada por los actuales homologados del sistema, la información documental recibida, la información proporcionada por CONFEOG y la información recolectada en campo, a través de visitas a los homologados y algunos OAT, se identifica un modelo que gráficamente se describe en la anterior imagen.

A nivel tecnológico, cada homologado busca el cumplimiento de sus responsabilidades a través de diferentes estrategias tecnológicas, todas ellas válidas pero diferentes entre sí. Esto quiere decir que, por ejemplo, en el caso de los CDA, cada homologado tiene un centro de procesamiento de datos CPD y un desarrollo de software propio que cumplen con los mismos objetivos misionales y normativos.

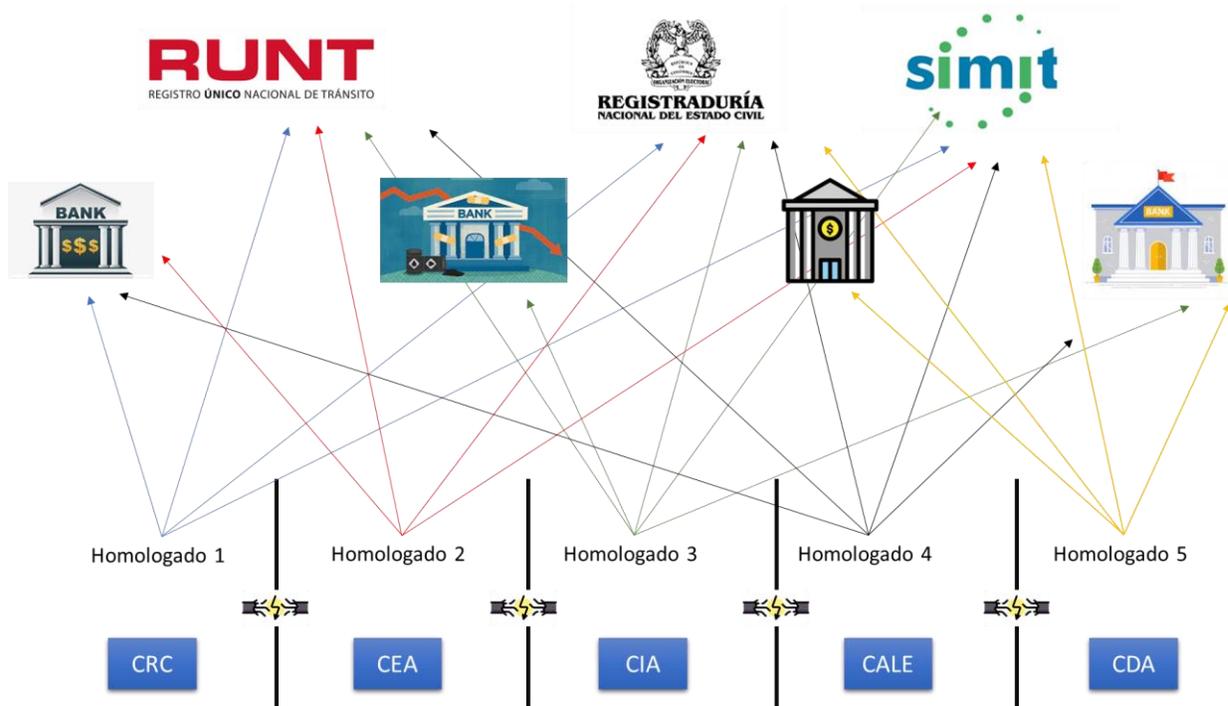
De igual forma, para el caso de CRC, se identifican dos homologados que tienen esquemas de monitoreo propios, así como de mesas de servicio distintas, las cuales, si bien cumplen con los objetivos de supervisión y control, al analizar de una forma integral a SICOV, se identifican como aspectos duplicados y que por ende requieren sus propios presupuestos, incidiendo este aspecto directamente en los costos asociados a la tarifa SICOV.

Otro aspecto analizado y de muy alta relevancia son los procedimientos de interoperabilidad. Como se puede apreciar en la gráfica del modelo actual, cada homologado debe hacer sus procedimientos y desarrollos de interoperabilidad para recaudo e intercambio de información. Si bien estos aspectos dan cumplimiento a lo requerido normativamente, al realizar un análisis integral se identifican ineficiencias financieras y dificultades operativas, traducidas en dificultades a nivel de supervisión (por ejemplo, oportunidad en el control y seguimiento de tarifas), dificultades operativas (controles transversales - validación de identidad) e ineficiencias financieras (duplicidad de costos).

4.2 Modelo de operación Federado

De acuerdo con el análisis realizado del modelo actual de operación de SICOV, se identificaron aspectos que si bien cumplían con los aspectos normativos, al realizar un análisis integral, emergían ineficiencias y grandes oportunidades de mejora, es por esto que se analiza un modelo de operación federado el cual consiste en soportar la operación de SICOV a través de un concesionario por OAT.

Ilustración 3 - SICOV - Federado



Fuente: Desarrollo propio, Grow Data 2021

Como se puede ver en la anterior gráfica, las ineficiencias de tener dos homologados para la gestión y control de un solo tipo de OAT, quedan solventadas con este modelo. Teniendo presente el espíritu de la presente consultoría lo origina la necesidad de generar la mejor opción para la entidad, al hacer los análisis de forma integral, se siguen presentando ineficiencias y oportunidades de mejora, ya no a nivel interno del OAT, sino a nivel transversal de SICOV.

Con el presente modelo se garantiza la unicidad y centralización de información, pero únicamente al nivel de cada tipo de OAT, no al nivel SICOV. Se garantiza la aplicación de controles al nivel de los diferentes tipos de OAT, pero no a nivel transversal cómo debe hacer SICOV. Si bien con el modelo federado se gana eficiencias, aun se identifican grandes oportunidades de mejora.

Siguiendo con las variables analizadas en el modelo actual, se puede concluir que:

- **A nivel de supervisión** y control, se mitigan las deficiencias asociadas tener que duplicar actividades como por ejemplo la conciliación entre los ingresos y la dispersión de fondos, control de tarifas, control de quejas y reclamos, entre otros. Si bien el modelo federado gana en eficiencia respecto del modelo actual, se siguen identificando oportunidades de mejora a nivel de controles y procedimientos transversales: Se gana en eficiencia por cada uno de los tipos de OAT pero sigue siendo ineficiente la gestión integral de SICOV.
- **A nivel de costos**, se eliminan muchas de las ineficiencias derivadas de la duplicidad de costos como: en el modelo actual se requiere un software por cada homologado de la misma OAT, se requiere un SOC y una mesa de servicios por cada Homologado. Si bien se gana en eficiencia no se llega a un nivel optimizado al tener un modelo completamente centralizado.
- **A nivel técnico y tecnológico**, se logran eficiencias a nivel de integración y centralización de información, pero únicamente a nivel de cada tipo de OAT. Dentro de este ámbito se logra una consolidación de elementos como los son los Centros de Datos, Plataformas de Seguridad, Procesamiento y Almacenamiento, Redes o networking de Centro de datos. Si bien esto se gana al consolidar la operación por OAT, se siguen identificando oportunidades de mejora a nivel transversal en este sentido.

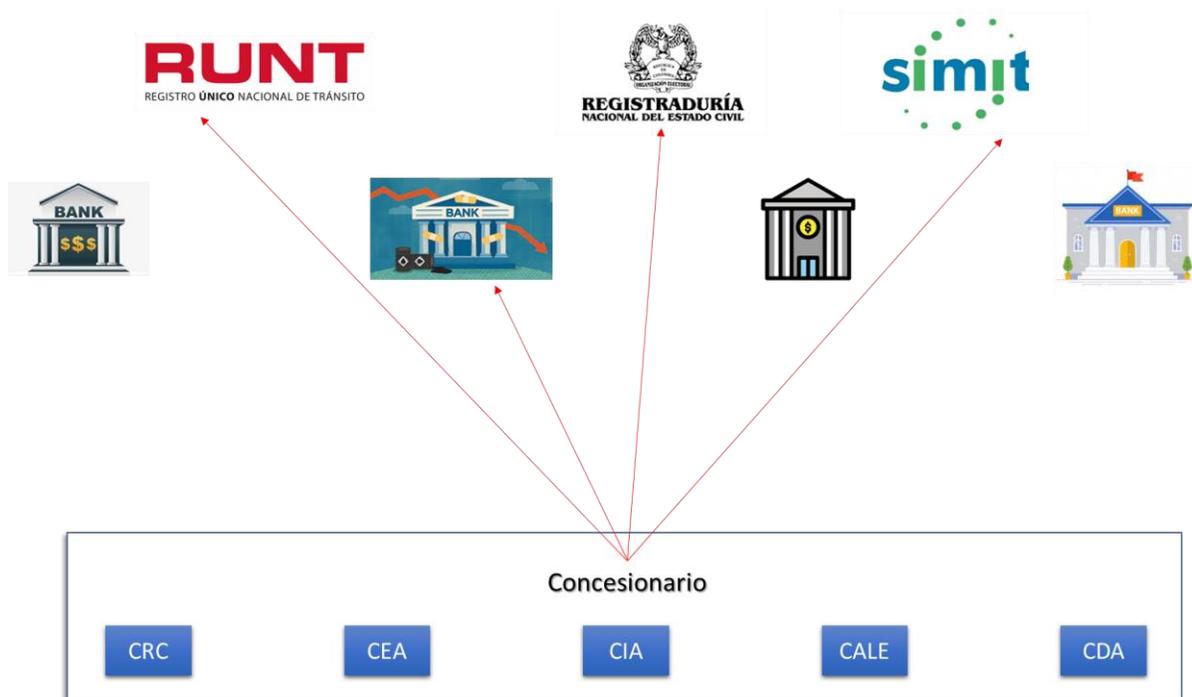
De igual forma, el modelo de interoperabilidad al ser consolidado por cada OAT (modelo federado) logra un nivel de optimización, sigue necesitando establecer acuerdos e implementación por cada concesionario.

- Los aspectos relacionados con la evolución de la supervisión y control a través de la implementación y fortalecimiento de controles en el respectivo software, en este modelo, encontrarán una gran dificultad, dado que cada concesionario podrá diseñar arquitecturas propias que posiblemente generen barreras o grandes limitaciones al momento de intentar implementar controles transversales cómo así lo debe hacer SICOV.

4.3 Modelo Centralizado

Como tercer modelo analizado se encuentra el centralizado. Este modelo busca a través de un solo concesionario soportar toda la operación de SICOV. Completando la comparación entre los diferentes modelos, a continuación, se presenta el modelo y el resultado del análisis hecho.

Ilustración 4 - SICOV Centralizado



Fuente: Desarrollo propio, Grow Data 2021

El modelo centralizado elimina la gran mayoría de aspectos identificados como duplicidades e ineficiencias en la operación, tomando elementos técnicos como el centro de procesamiento de datos – CPD, bajo este modelo se necesitaría uno solo. De igual forma elementos como el NOC / SOC y la mesa de servicios también serían únicos, centralizados y unificados evitando la duplicidad identificada en el modelo actual y en el modelo federado.

En la ilustración 4 - SICOV Centralizado se puede ver gráficamente que solamente se necesitaría crear e implementar un mecanismo de interacción con entidades externas como lo son el RUNT, RNEC, SIMIT, Operador de Recaudo, contrastando este aspecto con los modelos anteriores (Modelo Actual y Modelo Federado) los cuales efectivamente requieren duplicar este tipo de interacción.

A nivel de costos, al no encontrar estas ineficiencias se identifican unas disminuciones en los costos de inversión y operativos los cuales inciden directamente en una rebaja de la tarifa SICOV.

A través del modelo centralizado se potencian las siguientes características de un sistema eficiente, alineado a las necesidades de la entidad en términos de supervisión y control, y con una completa viabilidad en su implementación:

- **Compatibilidad:** Al tener un solo operador la responsabilidad de desarrollar el nuevo SICOV, se garantiza el uso de una sola arquitectura ofreciendo una compatibilidad nativa a todos los componentes del sistema de información.
- **Integración:** A través de un modelo centralizado se garantiza la integración nativa de las diferentes funcionalidades propias de cada uno de los tipos de OAT.
- **Interoperabilidad:** El concepto de interoperabilidad bajo este modelo garantiza altos niveles de eficiencia dado a que a través de un esquema centralizado se podrán diseñar e implementar los mecanismos transversales mediante los cuales SICOV intercambia información de forma eficiente con otros sistemas de información alimentando la funcionalidad requerida por los procedimientos propios de un OAT.
- **Escalabilidad:** El tener una infraestructura centralizada que soporta la capa de datos y la capa de sistemas de información, así como la seguridad, facilita el crecimiento horizontal y vertical de cada uno de los elementos que soportan la infraestructura tecnológica.
- **Riesgo:** Dentro de un modelo centralizado se facilitan las labores de gestión administración y control de toda la plataforma tecnológica que soportará a SICOV mitigando riesgos asociados a la disponibilidad, confidencialidad e integridad de este sistema de información y sus componentes. En el entendido que la centralización de componentes puede generar puntos únicos de fallo que incidan directamente sobre la disponibilidad de SICOV, la mitigación de este riesgo se facilita a través de la centralización del esquema de monitoreo y soporte, la implementación del CPD y sus componentes bajo la figura de Todo como Servicio (Plataformas como Servicio, Infraestructura como Servicio, Software como Servicio, Seguridad como Servicio). Adicionalmente, el riesgo de disponibilidad se mitiga a través de un plan de continuidad soportado en un Centro de Procesamiento de Datos secundario

5 Modelo Alternativo – Esquema Federado

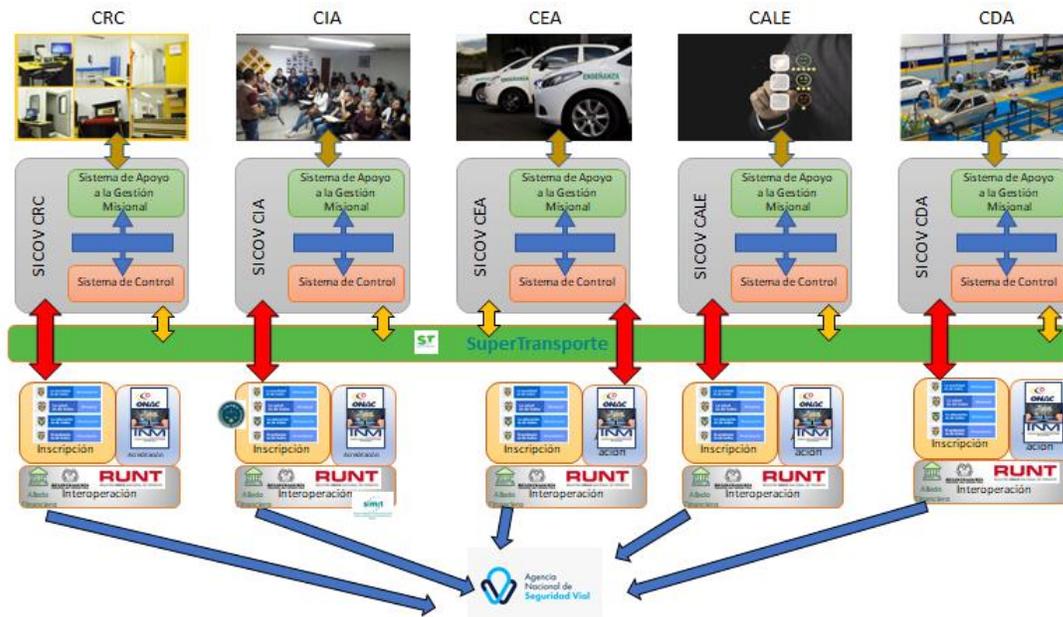
5.1 Arquitectura de sistemas de información federado

5.1.1 Arquitectura conceptual SICOV federado

Es aquella que se organiza de manera descentralizada a partir de la asociación de entidades o componentes de aplicación, los cuales acuerdan un propósito de negocio común.

5.1.1.1 Arquitectura de sistemas de información TO BE

Ilustración 5 Diagrama conceptual SICOV Federado



Fuente: Elaboración propia GrowData 2021

En la Ilustración 5 Diagrama conceptual SICOV Federado, se presenta el modelo elaborado por Grow Data para ilustrar el esquema de SICOV federado.

En la parte superior se encuentran los tipos de OAT's sujetos a inspección, vigilancia y control por parte de la Supertransporte, es decir, los CRC, los CEA, los CIA y los CDA que se encuentran operando en el momento de elaboración de este documento, así como los CALE que entrarán en operación en el futuro.

De acuerdo con el modelo TO BE, cada uno de los OAT tendrá una interacción directamente con un el sistema de apoyo a la gestión misional del SICOV especializado que posea cada



OAT que le servirá de apoyo directamente en la ejecución de actividades de sus procesos operativos.

En cada actividad, procedimiento o proceso del OAT que se identifique un punto de control, se establece una interoperabilidad con el sistema de control del SICOV, de tal forma que se pueda verificar el cumplimiento del aspecto a controlar, cualquiera que sea su índole y siempre y cuando se pueda implementar por medio de elementos tecnológicos que permitan realizar la actividad de control de manera automática.

Por lo anterior, cualquier acción de control que requiera de la participación de un tercero por medio de interoperabilidad (como la RNEC, el RUNT o cualquier otro) será realizada directamente por el sistema de control. Las acciones de captura de datos de los equipos biométricos, equipos médicos para evaluación de personas o equipos técnicos para evaluación de vehículos automotores, serán realizadas a través del sistema de control del SICOV específico para cada tipo de OAT.

De otra parte, las acciones de verificación de cumplimiento normativo, tanto para la inscripción inicial en el RUNT para poder operar, así como la verificación del cumplimiento de las condiciones que le permitan mantener dicha condición durante la operación, serán realizadas por el sistema de control del SICOV específico para cada tipo de OAT.

Finalmente, la Supertransporte, tendrá un rol fundamental, como consolidador de toda la información que requiera para dar cumplimiento a sus obligaciones y responsabilidades y la otra como ente de supervisión y administrador de las acciones de control de forma dinámica en el tiempo ejerciendo para ellos gobierno sobre dicha información. La Supertransporte necesitará definir los procesos internos para el desarrollo de dicha consolidación, lo mismo que las tecnologías necesarias.

5.1.1.2 Arquitectura de referencia para los sistemas de información del SICOV federados

De la misma forma que se estableció la arquitectura de referencia para el modelo centralizado, la arquitectura de referencia para un modelo de operación federado de SICOV tiene como propósito servir de base para orientar procesos de elaboración de arquitecturas de solución que atiendan preocupaciones específicas de interesados y den respuesta a requerimientos concretos para cada tipo de OAT.

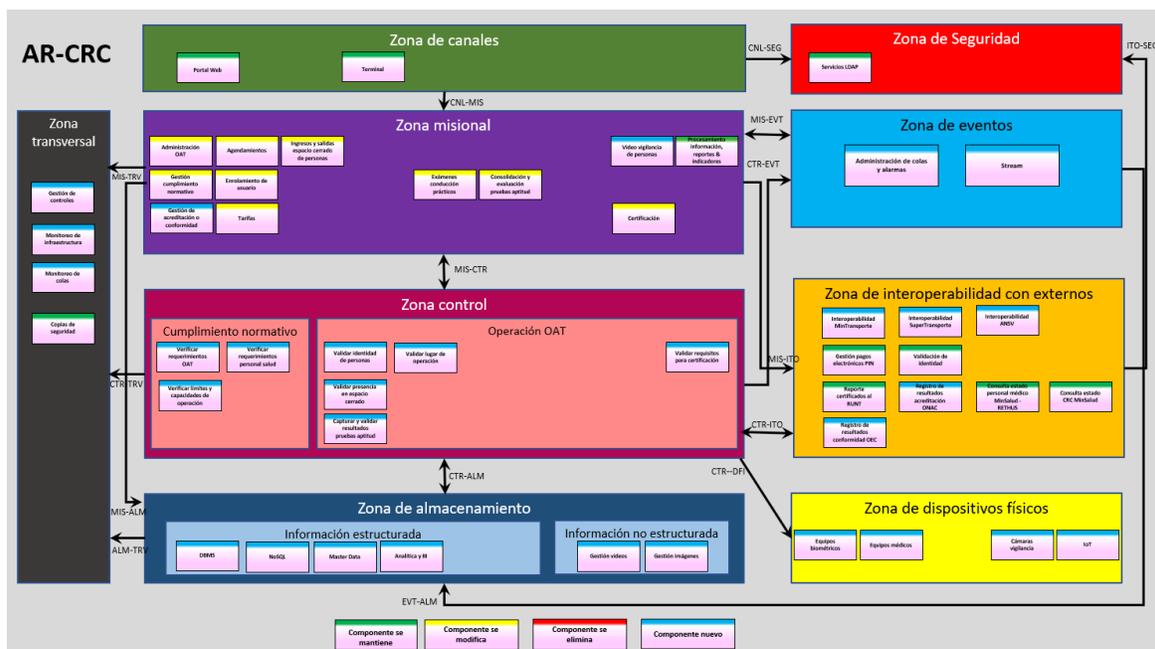
Las arquitecturas de referencia para soportar el modelo de operación federado de SICOV se diseñaron teniendo en cuenta las mismas consideraciones del SICOV centralizado:

- Delimitación de responsabilidades entre el sistema de gestión misional (SGM) y el Sistema de Control.
- El sistema de control actúa en cada punto de control identificado en los procesos y procedimientos misionales de los OAT.
- El SICOV está orientado a la automatización de los controles, mejorando la calidad y oportunidad de la información.

- El sistema de control deberá ofrecer mayor flexibilidad en la incorporación, modificación o eliminación de controles.
- En la Zona de Interoperabilidad, la interoperabilidad con Supertransporte se define más ampliamente, ya que tendrá un rol de reporte de información al consolidador Supertransporte asincrónicamente y garantizando las características de seguridad establecidas por la Supertransporte.

En las siguientes ilustraciones se presenta de forma gráfica las arquitecturas desarrolladas por Grow Data para cada uno de los cinco tipos de OAT's Cada una de las zonas que conforman las arquitecturas de referencia son similares a las zonas del modelo centralizado,

Ilustración 6 Arquitectura de referencia sistemas de información SICOV-CRC



Fuente: Elaboración propia GrowData 2021

por lo tanto, no se repiten en esta sección las descripciones y para un mejor entendimiento, se sugiere leer el numeral "Arquitectura Conceptual Modelo Centralizado" del ADD.

5.1.1.3 Arquitectura de referencia para los sistemas de información del SICOV-CRC federado

El principal aspecto que se debe tener en cuenta en la arquitectura de referencia para el SICOV-CRC, es la interoperabilidad con la Supertransporte. En el modelo centralizado, la interoperabilidad con la Supertransporte, tiene como propósito fundamental dar acceso a

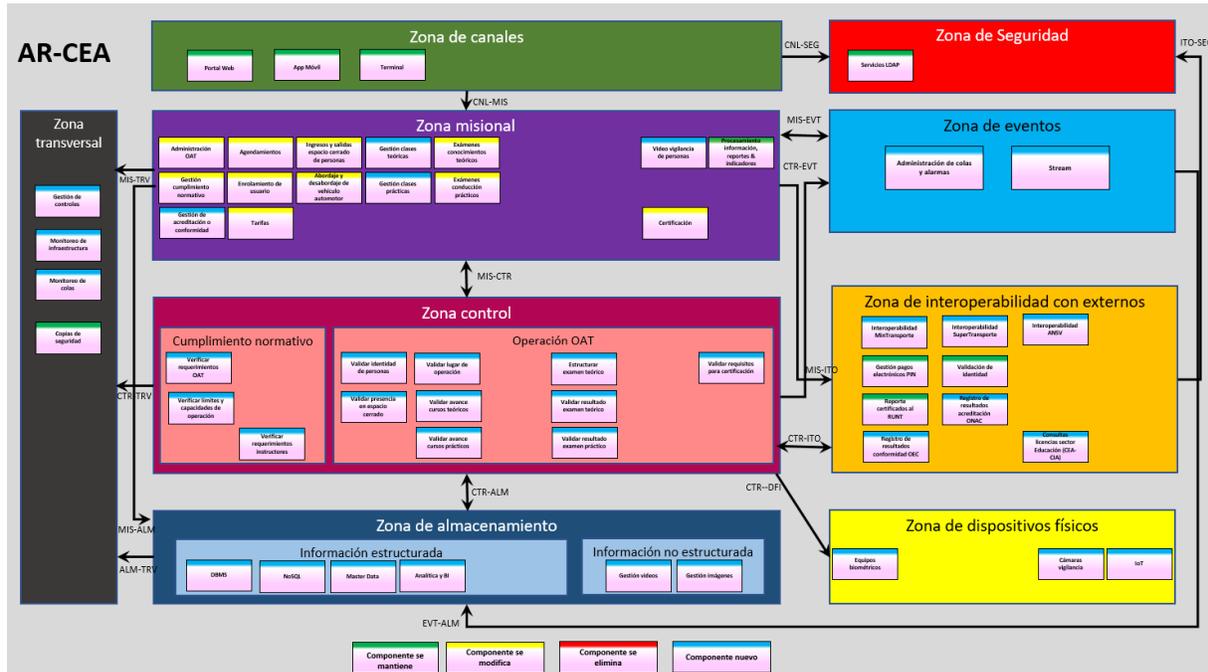


la SuperTransporte a la información centralizada del SICOV. En el caso federado esta interoperabilidad debe permitir la transmisión de la información relativa de los CRC requerida por la SuperTransporte para su procesamiento estandarizado bajo el gobierno de la propia SuperTransporte. En términos generales la arquitectura de referencia para el SICOV CRC toma los elementos misionales y de control exclusivos para los CRC. En cuanto a los componentes de la zona de dispositivos físicos, están presentes los biométricos, los equipos médicos y las cámaras de vigilancia, así como los IoT.

5.1.1.4 Arquitectura de referencia para los sistemas de información del SICOV-CEA federado

El principal aspecto que se debe tener en cuenta en la arquitectura de referencia para el SICOV-CEA (Véase la ilustración Arquitectura de referencia sistemas de información SICOV-CEA), es también la interoperabilidad con la SuperTransporte de la misma forma que se describió previamente para los CRC. En términos generales la arquitectura de referencia para el SICOV CEA toma los elementos misionales y de control exclusivos para los CEA como son los aspectos relacionados al agendamiento de cursos teóricos y prácticos, así como el correspondiente proceso de evaluación. Esto aplica también para los componentes de control que se centran específicamente en las actividades propias de los CEA. En cuanto a los componentes de la zona de dispositivos físicos, están presentes los biométricos, las cámaras de vigilancia y los equipos IoT.

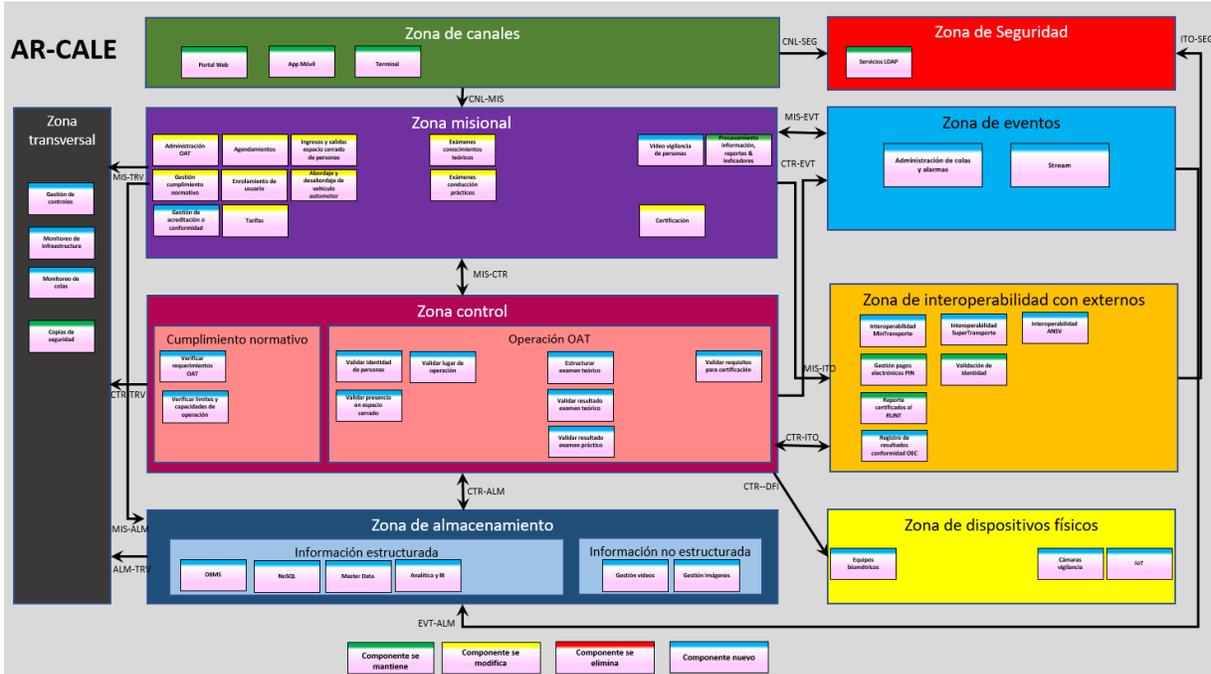
Ilustración 7 Arquitectura de referencia sistemas de información SICOV-CEA



Fuente: Elaboración propia Grow Data 2021

5.1.1.5 Arquitectura de referencia para los sistemas de información del SICOV-CALE federado

Ilustración 8 Arquitectura de referencia sistemas de información SICOV-CALE

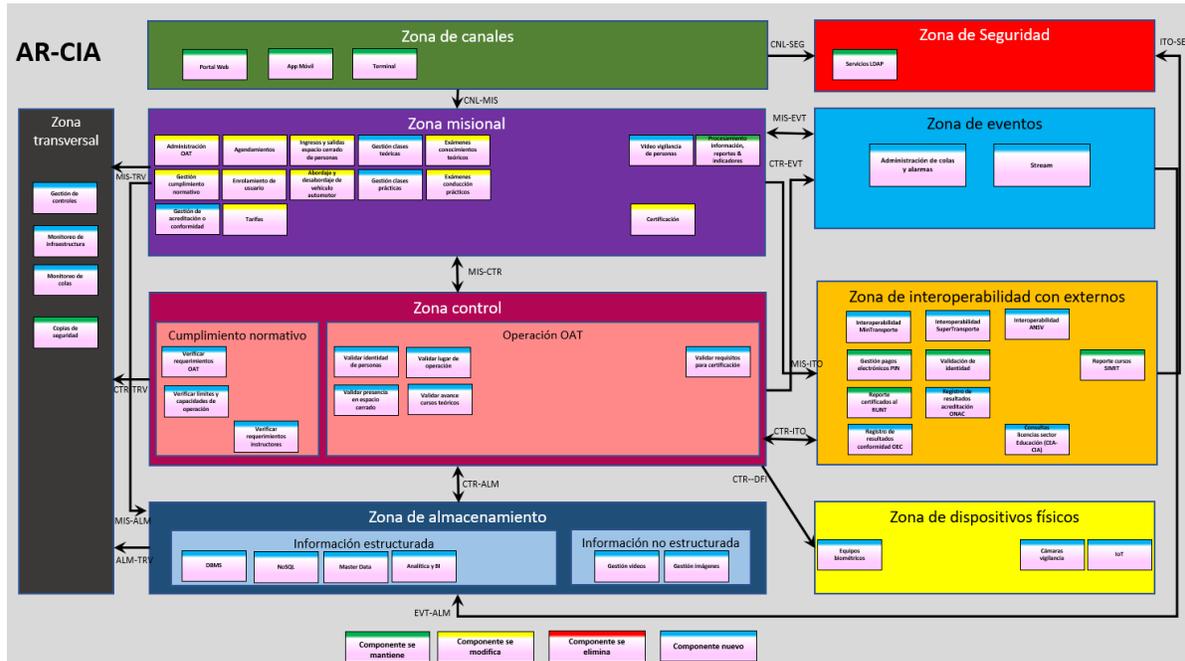


Fuente: Elaboración propia Grow Data 2021

El principal aspecto que se debe tener en cuenta en la arquitectura de referencia para el SICOV-CALE (Véase la ilustración Arquitectura de referencia sistemas de información SICOV-CALE), igual que en los anteriores, es la interoperabilidad con la SuperTransporte. En términos generales la arquitectura de referencia para el SICOV CALE toma los elementos misionales y de control exclusivos para los CALE como son los aspectos relacionados al agendamiento de los procesos de evaluación. Esto aplica también para los componentes de control que se centran específicamente en las actividades propias de los CALE. En cuanto a los componentes de la zona de dispositivos físicos, están presentes los biométricos, las cámaras de vigilancia y los equipos IoT.

5.1.1.6 Arquitectura de referencia para los sistemas de información del SICOV-CIA federado

Ilustración 9 Arquitectura de referencia sistemas de información SICOV-CIA

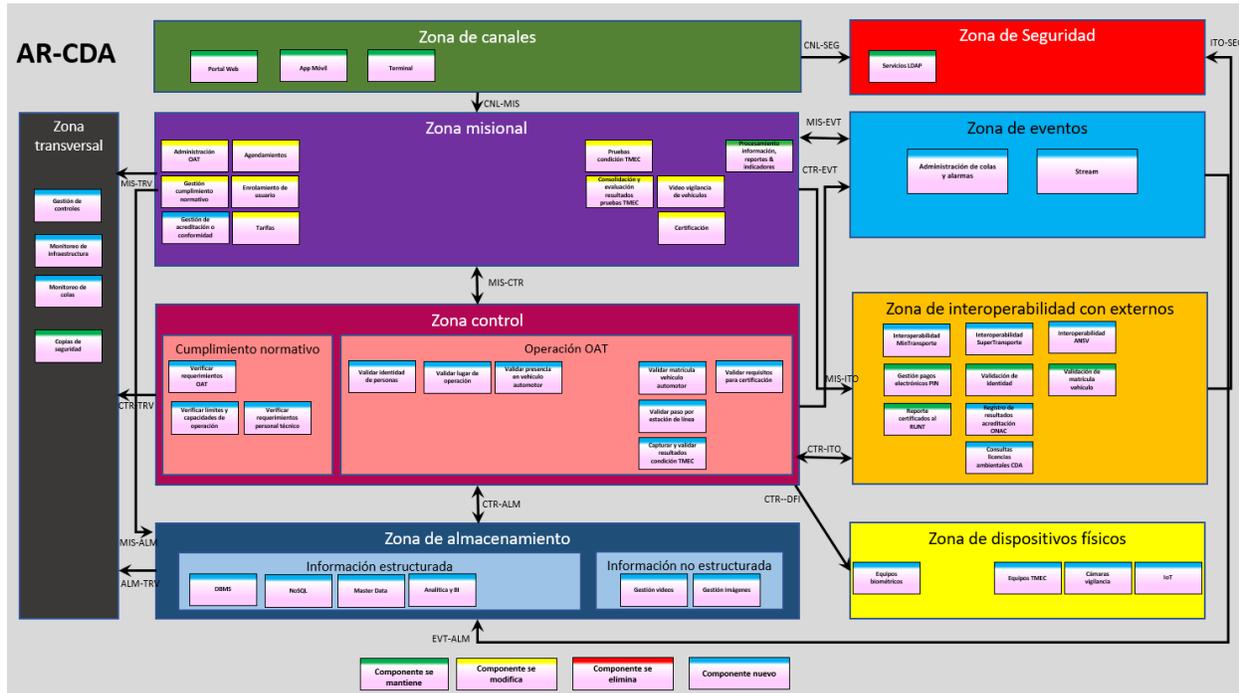


Fuente: Elaboración propia Grow Data 2021

En cuanto a los CIA (Véase la ilustración Arquitectura de referencia sistemas de información SICOV-CIA), se debe tener en cuenta en la arquitectura de referencia que es el único SICOV que presenta interoperación con el INPEC para los procesos de inscripción al RUNT y con el SIMIT para los procesos de disminución del valor a pagar por las infracciones cometidas por los usuarios. A parte de lo anterior, la arquitectura de referencia para los CIA es similar a la de los CEA en lo que tiene que ver con clases teóricas. Como en los casos anteriores, la interoperabilidad con la SuperTransporte requiere de componentes de cuya implementación se derive el cumplimiento de las necesidades establecidas para la ejecución de sus responsabilidades. En cuanto a los componentes de la zona de dispositivos físicos, están presentes los biométricos, las cámaras de vigilancia y los equipos IoT.

5.1.1.7 Arquitectura de referencia para los sistemas de información del SICOV-CDA federado

Ilustración 10 Arquitectura de referencia sistemas de información SICOV-CDA



Fuente: Elaboración propia Grow Data 2021

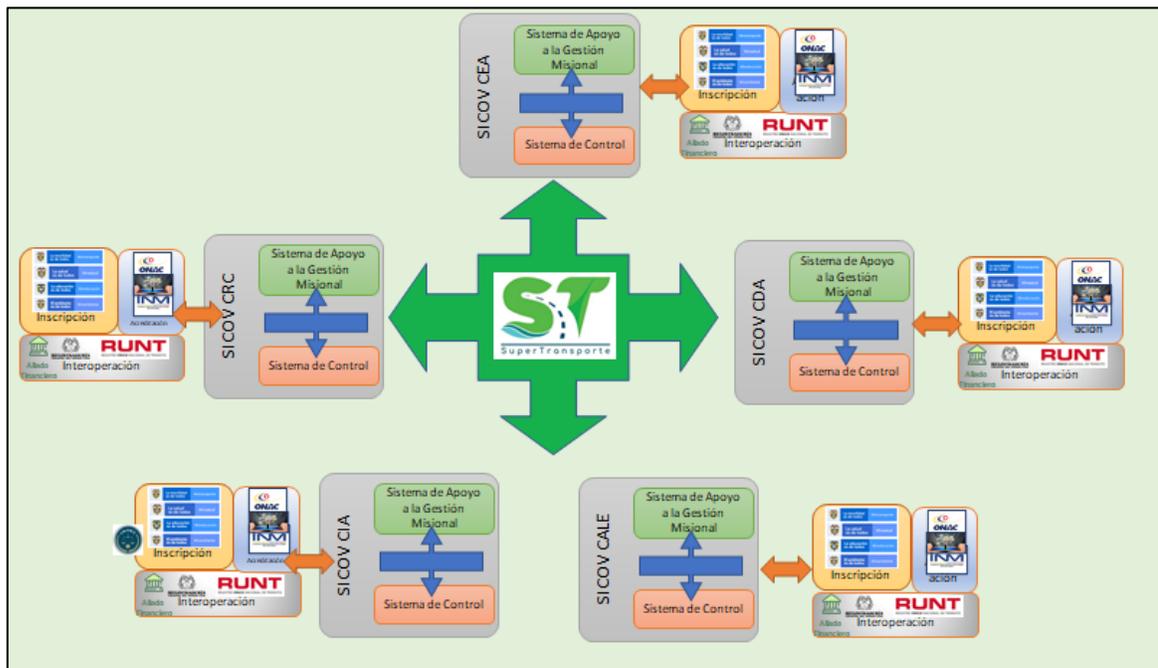
En el caso de la arquitectura de referencia para los CDA (Véase la ilustración Arquitectura de referencia sistemas de información SICOV-CDA) se debe tener en cuenta que en la zona de dispositivos los únicos que se excluyen con respecto al modelo centralizado, son los equipos médicos. Es importante resaltar que este es el único tipo de OAT que evalúa vehículos automotores y no personas, por lo tanto, es el que mayor diferencia presenta frente al modelo centralizado.

La arquitectura de referencia para el SICOV-CDA tiene un énfasis fundamental en la implementación de componentes en la zona misional, así como en la zona de control específicos.

Los componentes en la zona de almacenamiento para la información no estructurada, son de especial importancia para este tipo de OAT, dado que las acciones de vigilancia se fundamentan principalmente en el componente de video vigilancia.

5.1.2 Diagrama de interoperabilidad de los sistemas o aplicaciones modelo federado

Ilustración 11 Diagrama de interoperabilidad SICOV federado TO BE



Fuente: Elaboración propia Grow Data 2021

Al igual que para el modelo centralizado, la interoperabilidad representa un factor crítico para el SICOV, debido a la alta dependencia con los actores del sistema. En la Ilustración 11 Diagrama de interoperabilidad SICOV federado TO BE, se presenta de forma gráfica las interoperabilidades identificadas. A simple vista se puede observar como las interoperabilidades se deben implementar hasta 5 veces, una para cada SICOV. El diagrama de interoperabilidad propuesto coloca a la SuperTransporte en el centro de los cinco SICOV, teniendo en cuenta que, desde el punto de vista de vigilancia y control, la SuperTransporte debe actuar sobre todos los OAT y la mejor forma de realizarlo es mediante la consolidación de la información relevante de cada uno de ellos permitiendo tener una visión holística de todo el SICOV. Este modelo de interoperabilidad para el SICOV federado, implica por lo tanto que la SuperTransporte implemente las capacidades relacionadas con los procesos de recepción, transformación, consolidación y por supuesto gobierno de la información.

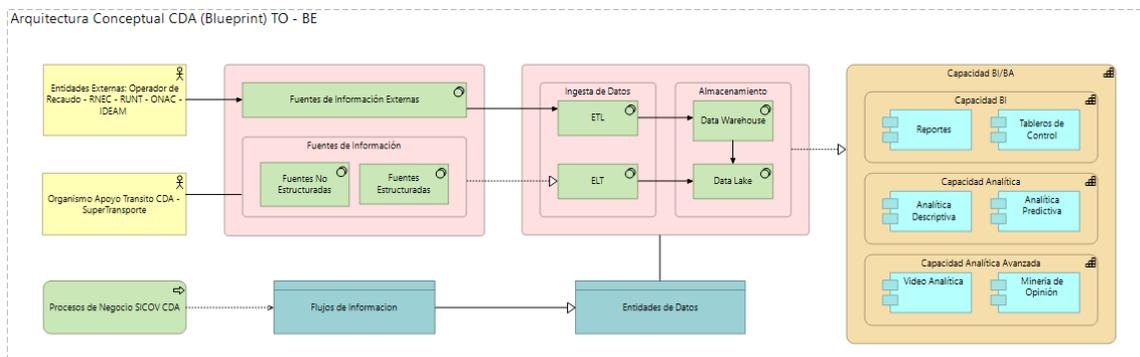
5.2 Arquitectura de Datos Modelo Federado

Teniendo como punto de partida el estado actual de la arquitectura de datos del sistema SICOV y que esta debe ser un puente entre la estrategia empresarial y la ejecución de tecnología, se plantea la siguiente arquitectura de datos TO BE para cada una de los OAT (CRC – CEA – CIA – CDA – CALE)

5.2.1 Arquitectura Conceptual TO BE - CDA

La arquitectura conceptual de datos TO BE del sistema SICOV para el Organismo de Apoyo al Tránsito – CDA (Centro de Diagnóstico Automotor) está conformada por los siguientes componentes como se presenta en la Ilustración 12. Arquitectura Conceptual TOBE - CDA.

Ilustración 12. Arquitectura Conceptual TOBE - CDA



Fuente: Elaboración propia Grow Data 2021

5.2.1.1 Entidades

Organizaciones que de forma directa e indirecta deben generar datos hacia el sistema SICOV. Estas se encuentran clasificadas en dos:

- o Entidades externas: Conformadas por
 - Operador de recaudo
 - RNEC
 - RUNT
 - ONAC

- IDEAM
 - Entidades internas: Conformadas por
 - CDA
 - SuperTransporte

Estas entidades que dependen de la naturaleza de la información generan datos estructurados y no estructurados según las necesidades de información (diario, mensual o semestral).

5.2.1.2 Fuentes de Información

Conformada por las diferentes estructuras de datos que deben ser generadas por parte del CDA. Estas se clasifican en fuentes de datos externas, que son datos estructurados en formato xml o json, generados por las entidades externas.

Por otro lado, tenemos las fuentes estructuradas y fuentes no estructuradas; las primeras son generadas por el CDA en formato xml o json y son los datos resultantes de la ejecución de los diferentes procesos del sistema SICOV.

La segunda son los datos no estructurados, conformados en su totalidad por videos de monitoreo a los vehículos automotores que acceden al centro de diagnóstico automotor. También se plantea tener una fuente de datos adicional dada por los datos generados por las redes sociales.

5.2.1.3 Almacenamiento

Este componente no tiene cambio con relación al AS IS. Actualmente el sistema SICOV cuenta con diferentes bases datos y esta propuesta federada, posee de igual forma una colección de bases, con la diferencia del manejo de los datos de forma autónoma, heterogénea y cooperativa.

En la propuesta de un sistema federado, los encargados del CDA tienen acceso a la información por medio de una interfaz común sin que estos perciban que los datos son dirigidos a distintas bases de datos.

De igual forma, se plantea una estrategia de persistencia de datos conformada por dos componentes:

- Ingesta de Datos: Este componente presenta dos mecanismos: el primero es el ETL (extracción, transformación y carga), que permite llevar de forma óptima y eficiente los datos desde las fuentes externas del CDA como son (Operador de recaudo, RNEC, RUNT, ONAC, IDEAM) hasta la bodega de datos. Es importante aclarar que toda la información

ingestada en la bodega es estructurada y debe persistirse en dimensiones y tablas de hechos.

El segundo, es el ELT (Extracción, Carga y Transformación), muy similar al anterior, con la diferencia que se cargan los datos antes de realizar las transformaciones. Es importante aclarar que, este mecanismo permite almacenar información en el Data Lake como una estrategia de colecciones.

- Almacenamiento: Este componente está conformado por:
 - Data Warehouse: Es un proceso estructurado de métodos, técnicas y lineamientos y reglas de negocio que permitirán integrar y manejar las fuentes de datos externas con el propósito de obtener una vista consolidada y detallada del sistema SICOV en el CDA.
 - Data Lake. Es un repositorio de almacenamiento que contienen una gran cantidad de datos en bruto y permite gestionar datos históricos. A diferencia de un Data Warehouse que almacena datos estructurados, un data Lake utiliza una arquitectura plana que permite almacenar datos no estructurados de la operación del CDA que corresponden a los videos de monitoreo a los vehículos automotores.

5.2.1.4 Procesos de Negocio, Flujos y Entidades de Datos

Estos componentes tienen como objetivo identificar las diferentes entidades de datos que conforman el sistema SICOV en el CDA. Inicialmente se identifican y contextualizan los procesos de negocio de los Centros de Diagnóstico Automotor, los cuales se encuentran descritos y diseñados en el dominio de negocio; estos procesos son insumos para el diagrama de flujos de datos del CDA, el cual se encuentra en la sección de diagramas del TO BE en la arquitectura de datos, donde se puede apreciar cómo deben interactúan con las diferentes entidades de datos y las bases de datos del CDA.

Finalmente, se debe generar los catálogos de entidades de datos. Es importante aclarar, que el catálogo de entidades de datos es un documento vivo que evoluciona en el tiempo y debe ser continuamente alimentada por cambios en los procesos, normativa y necesidades alrededor de los datos.

5.2.1.5 Capacidad BI/BA

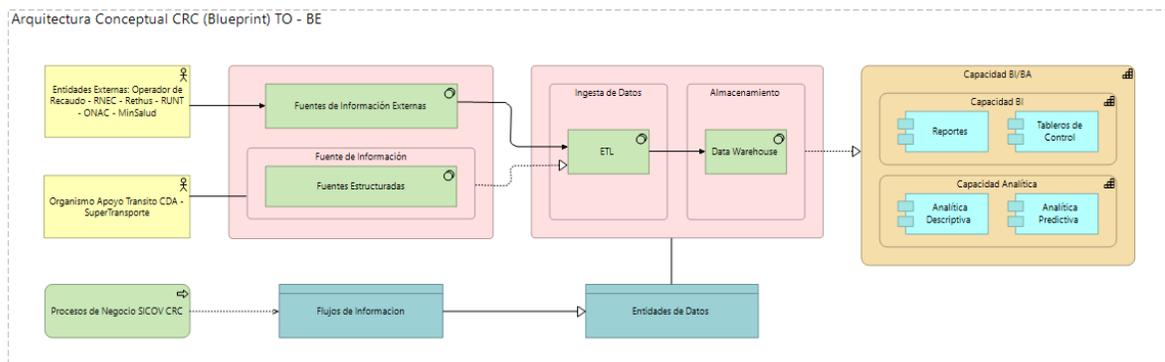
Este componente en términos de capacidad está conformado por tres componentes:

- **Capacidad BI:** Estrategia de inteligencia de negocios, que permita generar reportes, alertas y tableros de control donde se puedan apreciar diferentes indicadores que permitan medir la gestión y control del sistema SICOV del CDA.
- **Capacidad Analítica:** Estrategia de analítica tradicional que permita realizar modelos para descubrir información y poder tomar decisiones a partir de estos. Por ejemplo, algoritmos para predecir los posibles vehículos automotores que probablemente no pasaran la revisión tecno-mecánica.
- **Capacidad Analítica Avanzada:** Estrategia de analítica avanzada basada en modelos y técnicas de inteligencia artificial que permitan realizar video analítica y minería de opinión. La primera se propone para tener una herramienta que apoye el control y vigilancia de un vehículo automotor cuando se encuentra en proceso de obtener certificación tecno-mecánica al interior de un CDA. La segunda es basada en análisis de sentimiento a partir de redes sociales, para poder captar las opiniones de los usuarios de los CDA y tomar acciones de mejoras.

5.2.2 Arquitectura Conceptual TO BE - CRC

La arquitectura conceptual de datos TO BE del sistema SICOV para el Organismo de Apoyo al Tránsito – CRC (Centros de Reconocimiento de Conductores) está conformada por los siguientes componentes como se presenta en la Ilustración 13. Arquitectura Conceptual TOBE - CRC.

Ilustración 13. Arquitectura Conceptual TOBE - CRC



Fuente: Elaboración propia Grow Data 2021

5.2.2.1 Entidades

Organizaciones que de forma directa e indirecta deben generar datos hacia el sistema SICOV. Estas se encuentran clasificadas en dos:

- Entidades externas: Conformadas por
 - Operador de recaudo
 - RNEC
 - ReTHUS
 - RUNT
 - ONAC
 - MinSalud

- Entidades internas: Conformadas por
 - CRC
 - SuperTransporte

Estas entidades que dependen de la naturaleza de la información generan datos estructurados según las necesidades de información (diario, mensual o semestral).

5.2.2.2 Fuentes de Información

Conformada por las diferentes estructuras de datos que deben ser generadas por parte del CRC. Estas se clasifican en fuentes de datos externas, que son datos estructurados en formato xml o json, generados por las entidades externas.

Por otro lado, tenemos las fuentes estructuradas las cuales son generadas por el CRC en formato xml o json y son los datos resultantes de la ejecución de los diferentes procesos del sistema SICOV.

5.2.2.3 Almacenamiento

Este componente no tiene cambio con relación al AS IS. Actualmente el sistema SICOV cuenta con diferentes bases de datos y esta propuesta federada posee de igual forma una colección de bases de datos, con la diferencia del manejo de los datos de forma autónoma, heterogénea y cooperativa.

En la propuesta de un sistema federado, los encargados del CRC tienen acceso a la información por medio de una interfaz común sin que estos perciban que los datos son dirigidos a distintas bases de datos.

De igual forma se plantea una estrategia de persistencia de datos conformada por dos componentes:

- **Ingesta de Datos:** Este componente presenta el ETL (extracción, transformación y carga), que permite llevar de forma óptima y eficiente los datos desde las fuentes externas del CRC como son (Operador de recaudo, RNEC, ReTHUS, RUNT, ONAC, MinSalud) hasta la bodega de datos. Es importante aclarar que toda la información ingestada en la bodega es estructurada y debe persistirse en dimensiones y tablas de hechos.

Almacenamiento: Este componente está conformado por Data Warehouse: Es un proceso estructurado de métodos, técnicas y lineamientos y reglas de negocio que permitirán integrar y manejar las fuentes de datos externas con el propósito de obtener una vista consolidada y detallada del sistema SICOV en el CRC.

5.2.2.4 Procesos de Negocio, Flujos y Entidades de Datos

Estos componentes tienen como objetivo identificar las diferentes entidades de datos que conforman el sistema SICOV en el CRC. Inicialmente se identifican y contextualizan los procesos de negocio de los Centros de Reconocimiento de Conductores los cuales se encuentran descritos y diseñados en el dominio de negocio; estos procesos son insumos para el diagrama de flujos de datos del CRC, el cual se encuentra en la sección de diagramas del TO BE en la arquitectura de datos, donde se puede apreciar cómo deben interactuar con las diferentes entidades de datos y las bases de datos del CRC.

Finalmente, se debe generar los catálogos de entidades de datos. Es importante aclarar, que el catálogo de entidades de datos es un documento vivo que evoluciona en el tiempo y debe ser continuamente alimentada por cambios en los procesos, normativa y necesidades alrededor de los datos.

5.2.2.5 Capacidad BI/BA

Este componente en términos de capacidad está conformado por dos componentes:

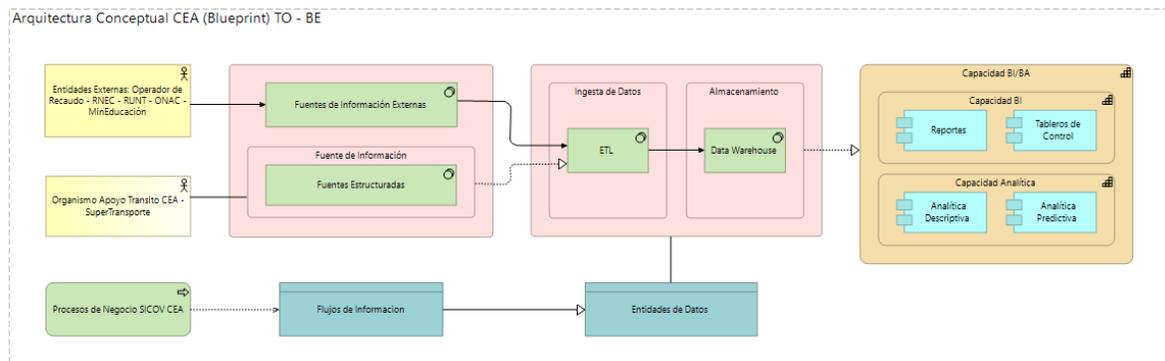
- **Capacidad BI:** Estrategia de inteligencia de negocios, que permita generar reportes, alertas y tableros de control donde se puedan apreciar diferentes indicadores que permitan medir la gestión y control del sistema SICOV del CRC.
- **Capacidad Analítica:** Estrategia de analítica tradicional que permita realizar modelos para descubrir información y poder tomar decisiones a partir de estos. Por ejemplo, algoritmos para predecir el número de solicitudes de exámenes de reconocimiento en un periodo de tiempo determinado.

5.2.3 Arquitectura Conceptual TO BE - CEA

La arquitectura conceptual de datos TO BE del sistema SICOV para el Organismo de Apoyo al Tránsito – CEA (Centros de Enseñanza Automovilística) está conformada por los siguientes componentes como se presenta en la

Ilustración 14. Arquitectura Conceptual TOBE - CEA.

Ilustración 14. Arquitectura Conceptual TOBE - CEA



Fuente: Elaboración propia Grow Data 2021

5.2.3.1 Entidades

Organizaciones que de forma directa e indirecta deben generar datos hacia el sistema SICOV. Estas se encuentran clasificadas en dos:

- Entidades externas: Conformadas por
 - Operador de recaudo
 - RNEC
 - RUNT
 - ONAC
 - MinEducación
- Entidades internas: Conformadas por
 - CEA
 - SuperTransporte

Estas entidades que dependen de la naturaleza de la información generan datos estructurados según las necesidades de información (diario, mensual o semestral).

5.2.3.2 Fuentes de Información

Conformada por las diferentes estructuras de datos que deben ser generadas por parte del CEA. Estas se clasifican en fuentes de datos externas, que son datos estructurados en formato xml o json, generados por las entidades externas.

Por otro lado, tenemos las fuentes estructuradas las cuales son generadas por el CEA en formato xml o json y son los datos resultantes de la ejecución de los diferentes procesos del sistema SICOV.

5.2.3.3 Almacenamiento

Este componente no tiene cambio con relación al AS IS. Actualmente el sistema SICOV cuenta con diferentes bases de datos y esta propuesta federada posee de igual forma una colección de bases; con la diferencia del manejo de los datos de forma autónoma, heterogénea y cooperativa.

En la propuesta de un sistema federado los encargados del CEA tienen acceso a la información por medio de una interfaz común sin que estos perciban que los datos son dirigidos a distintas bases de datos.

De igual forma se plantea una estrategia de persistencia de datos conformada por dos componentes:

- **Ingesta de Datos:** Este componente presenta el ETL (extracción, transformación y carga), que permite llevar de forma óptima y eficiente los datos desde las fuentes externas del CEA como son (Operador de recaudo, RNEC, RUNT, ONAC, MinEducación) hasta la bodega de datos. Es importante aclarar que toda la información ingestada en la bodega es estructurada y debe persistirse en dimensiones y tablas de hechos.

Almacenamiento: Este componente está conformado por Data Warehouse: Es un proceso estructurado de métodos, técnicas y lineamientos y reglas de negocio que permitirán integrar y manejar las fuentes de datos externas con el propósito de obtener una vista consolidada y detallada del sistema SICOV en el CEA.

5.2.3.4 Procesos de Negocio, Flujos y Entidades de Datos

Estos componentes tienen como objetivo identificar las diferentes entidades de datos que conforman el sistema SICOV en el CEA. Inicialmente se identifican y contextualizan los

procesos de negocio de los Centros de Enseñanza Automovilística los cuales se encuentran descritos y diseñados en el dominio de negocio; estos procesos son insumos para el diagrama de flujos de datos del CEA el cual se encuentra en la sección de diagramas del TO BE en la arquitectura de datos, donde se puede apreciar cómo deben interactúan con las diferentes entidades de datos y las bases de datos del CEA.

Finalmente, se debe generar los catálogos de entidades de datos. Es importante aclarar, que el catálogo de entidades de datos es un documento vivo que evoluciona en el tiempo y debe ser continuamente alimentada por cambios en los procesos, normativa y necesidades alrededor de los datos.

5.2.3.5 Capacidad BI/BA

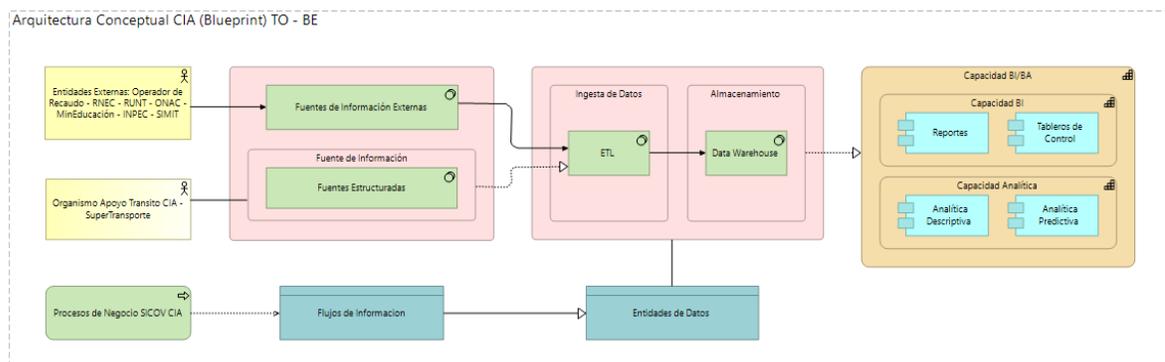
Este componente en términos de capacidad está conformado por dos componentes:

- **Capacidad BI:** Estrategia de inteligencia de negocios, que permita generar reportes, alertas y tableros de control donde se puedan apreciar diferentes indicadores que permitan medir la gestión y control del sistema SICOV del CEA.
- **Capacidad Analítica:** Estrategia de analítica tradicional que permita realizar modelos para descubrir información y poder tomar decisiones a partir de estos. Por ejemplo, algoritmos para predecir el número de solicitudes de licencia de conducción en un periodo de tiempo determinado.

5.2.4 Arquitectura Conceptual TO BE - CIA

La arquitectura conceptual de datos TO BE del sistema SICOV para el Organismo de Apoyo al Tránsito – CIA (Centros Integrales de Atención) está conformada por los siguientes componentes como se presenta en la Ilustración 15. Arquitectura Conceptual TOBE - CIA.

Ilustración 15. Arquitectura Conceptual TOBE - CIA



Fuente: Elaboración propia Grow Data 2021

5.2.4.1 Entidades

Organizaciones que de forma directa e indirecta deben generar datos hacia el sistema SICOV. Estas se encuentran clasificadas en dos:

- Entidades externas: Conformadas por
 - Operador de recaudo
 - RNEC
 - RUNT
 - ONAC
 - MinEducación
 - INPEC
 - SIMIT
- Entidades internas: Conformadas por
 - CIA
 - SuperTransporte

Estas entidades que dependen de la naturaleza de la información generan datos estructurados según las necesidades de información (diario, mensual o semestral).

5.2.4.2 Fuentes de Información

Conformada por las diferentes estructuras de datos que deben ser generadas por parte del CIA. Estas se clasifican en fuentes de datos externas, que son datos estructurados en formato xml o json, generados por las entidades externas.

Por otro lado, tenemos las fuentes estructuradas las cuales son generadas por el CIA en formato xml o json y son los datos resultantes de la ejecución de los diferentes procesos del sistema SICOV.

5.2.4.3 Almacenamiento

Esta propuesta federada posee una colección de bases; con el manejo de los datos de forma autónoma, heterogénea y cooperativa.

En la propuesta de un sistema federado los encargados del CIA tienen acceso a la información por medio de una interfaz común sin que estos perciban que los datos son dirigidos a distintas bases de datos.

De igual forma se plantea una estrategia de persistencia de datos conformada por dos componentes:

- **Ingesta de Datos:** Este componente presenta el ETL (extracción, transformación y carga), que permite llevar de forma óptima y eficiente los datos desde las fuentes externas del CIA como son (Operador de recaudo, RNEC, RUNT, ONAC, MinEducación, INPEC, SIMIT) hasta la bodega de datos. Es importante aclarar que toda la información ingestada en la bodega es estructurada y debe persistirse en dimensiones y tablas de hechos.

Almacenamiento: Este componente está conformado por Data Warehouse, es un proceso estructurado de métodos, técnicas y lineamientos y reglas de negocio que permitirán integrar y manejar las fuentes de datos externas con el propósito de obtener una vista consolidada y detallada del sistema SICOV en el CIA.

5.2.4.4 Procesos de Negocio, Flujos y Entidades de Datos

Estos componentes tienen como objetivo identificar las diferentes entidades de datos que conforman el sistema SICOV en el CIA. Inicialmente se identifican y contextualizan los procesos de negocio de los Centros Integrales de Atención los cuales se encuentran descritos y diseñados en el dominio de negocio; estos procesos son insumos para el diagrama de flujos de datos del CIA el cual se encuentra en la sección de diagramas del TO BE en la arquitectura de datos, donde se puede apreciar cómo deben interactúan con las diferentes entidades de datos y las bases de datos del CIA.

Finalmente, se debe generar los catálogos de entidades de datos. Es importante aclarar, que el catálogo de entidades de datos es un documento vivo que evoluciona en el tiempo y debe ser continuamente alimentada por cambios en los procesos, normativa y necesidades alrededor de los datos.

5.2.4.5 Capacidad BI/BA

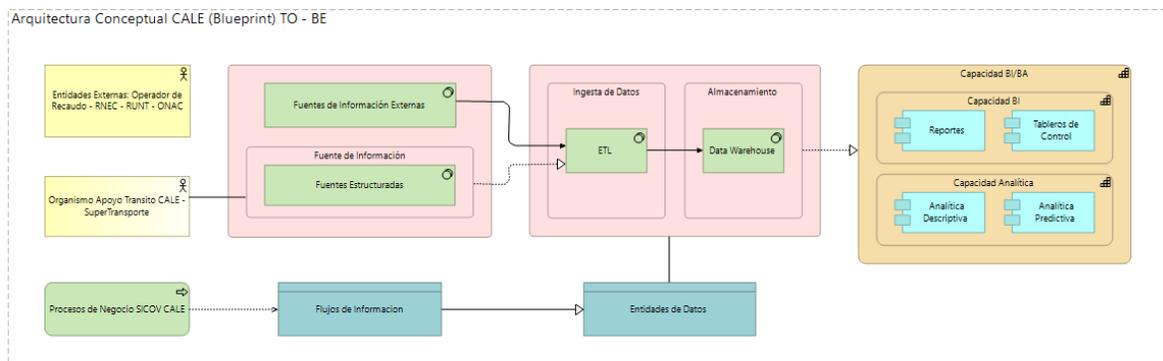
Este componente en términos de capacidad está conformado por dos componentes:

- **Capacidad BI:** Estrategia de inteligencia de negocios, que permita generar reportes, alertas y tableros de control donde se puedan apreciar diferentes indicadores que permitan medir la gestión y control del sistema SICOV del CIA.
- **Capacidad Analítica:** Estrategia de analítica tradicional que permita realizar modelos para descubrir información y poder tomar decisiones a partir de estos. Por ejemplo, algoritmos para predecir el número de infractores que solicitan los servicios del CIA en un periodo de tiempo determinado.

5.2.5 Arquitectura Conceptual TO BE - CALE

La arquitectura conceptual de datos TO BE del sistema SICOV para el Organismo de Apoyo al Tránsito – CALE (Centros de Apoyo logístico de Evaluación) está conformada por los siguientes componentes como se presenta en la Ilustración 16. Arquitectura Conceptual TOBE - CALE.

Ilustración 16. Arquitectura Conceptual TOBE - CALE



Fuente: Elaboración propia Grow Data 2021

5.2.5.1 Entidades

Organizaciones que de forma directa e indirecta deben generar datos hacia el sistema SICOV. Estas se encuentran clasificadas en dos:

- Entidades externas: Conformadas por
 - Operador de recaudo
 - RNEC
 - RUNT
 - ONAC

- Entidades internas: Conformadas por
 - CALE
 - SuperTransporte

Estas entidades que dependen de la naturaleza de la información generan datos estructurados según las necesidades de información (diario, mensual o semestral).

5.2.5.2 Fuentes de Información

Conformada por las diferentes estructuras de datos que deben ser generadas por parte del CALE. Estas se clasifican en fuentes de datos externas, que son datos estructurados en formato xml o json, generados por las entidades externas.

Por otro lado, tenemos las fuentes estructuradas las cuales son generadas por el CALE en formato xml o json y son los datos resultantes de la ejecución de los diferentes procesos del sistema SICOV.

5.2.5.3 Almacenamiento

Esta propuesta federada posee una colección de bases; con el manejo de los datos de forma autónoma, heterogénea y cooperativa.

En la propuesta de un sistema federado los encargados del CALE tienen acceso a la información por medio de una interfaz común sin que estos perciban que los datos son dirigidos a distintas bases de datos.

De igual forma se plantea una estrategia de persistencia de datos conformada por dos componentes:

- **Ingesta de Datos:** Este componente presenta el ETL (extracción, transformación y carga), que permite llevar de forma óptima y eficiente los datos desde las fuentes externas del CALE como son (Operador de recaudo, RNEC, RUNT, ONAC) hasta la bodega de datos. Es importante aclarar que toda la información ingestada en la bodega es estructurada y debe persistirse en dimensiones y tablas de hechos.

Almacenamiento: Este componente está conformado por Data Warehouse: Es un proceso estructurado de métodos, técnicas y lineamientos y reglas de negocio que permitirán integrar y manejar las fuentes de datos externas con el propósito de obtener una vista consolidada y detallada del sistema SICOV en el CALE.

5.2.5.4 Procesos de Negocio, Flujos y Entidades de Datos

Estos componentes tienen como objetivo identificar las diferentes entidades de datos que conforman el sistema SICOV en el CALE. Inicialmente se identifican y contextualizan los procesos de negocio de los Centros de Apoyo logístico de Evaluación los cuales se encuentran descritos y diseñados en el dominio de negocio; estos procesos son insumos para el diagrama de flujos de datos del CALE el cual se encuentra en la sección de diagramas del TO BE en la arquitectura de datos, donde se puede apreciar cómo deben interactúan con las diferentes entidades de datos y las bases de datos del CALE.

Finalmente, se debe generar los catálogos de entidades de datos. Es importante aclarar, que el catálogo de entidades de datos es un documento vivo que evoluciona en el tiempo y debe ser continuamente alimentada por cambios en los procesos, normativa y necesidades alrededor de los datos.

5.2.5.5 Capacidad BI/BA

Este componente en términos de capacidad está conformado por dos componentes:

- **Capacidad BI:** Estrategia de inteligencia de negocios, que permita generar reportes, alertas y tableros de control donde se puedan apreciar diferentes indicadores que permitan medir la gestión y control del sistema SICOV del CALE.
- **Capacidad Analítica:** Estrategia de analítica tradicional que permita realizar modelos para descubrir información y poder tomar decisiones a partir de estos. Por ejemplo, algoritmos para predecir el número de solicitudes para evaluación de los exámenes teórico y práctico para la licencia de conducción en un periodo de tiempo determinado.

6 Modelo Propuesto – Esquema Centralizado

Para la estructuración del esquema a proponer, es necesario traer a colación las principales preocupaciones de la entidad respecto del sistema de control y vigilancia:

6.1 Principales preocupaciones

Dentro del desarrollo de la arquitectura de negocio y de T.I. un aspecto que impulsa las decisiones a nivel de estructuración y enfoque es el Modelo de Intención, siendo las preocupaciones uno de los principales impulsores. A continuación, se describen algunas de las principales preocupaciones:

- Falta de integración entre los sistemas de información de los homologados, lo que genera inconsistencias en la prestación de los servicios por parte de los OAT. Esta integración permitiría la validación de requisitos técnicos como el número de horas máximas por instructor (240 horas) en todo el SICOV CEA, independiente de quien es el homologado.
- Tener la garantía que el concesionario u homologado de SICOV, según el modelo de autorización que defina la ST, incorpore en el tiempo mejoras y evolución.

- Establecimiento de estándares y lineamientos para que independiente del proveedor del sistema, existan las mismas funcionalidades, reportes y validaciones en el SICOV.
- Crear un marco de interoperabilidad unificado para el intercambio de información entre los diferentes actores del sistema SICOV: Superintendencia, homologados, OAT, RUNT, Registraduría, Migración Colombia, Ministerio de Transporte y Salud, ANSV, ONAC y autoridades de apoyo al tránsito (secretarías de tránsito).
- Formalizar y estandarizar el reporte de información, indicadores y estadísticas hacia la Supertransporte.
- Mejorar la experiencia de usuario tanto para los OAT como para los ciudadanos de tal forma que se reporte en qué etapa o estado se encuentra el trámite. Por ejemplo, resultados de pruebas CRC, en los CEA conocer las horas de clase tomadas y las que faltan.
- Generar conjuntos de datos abiertos, publicarlos en el Portal de Datos Abiertos y definir estrategias para incentivar su uso teniendo como fuente el SICOV.

Para mayor detalle de las preocupaciones asociadas al Modelo de Intención, consultar el Documento de Definición de Arquitectura – ADD; Capítulo 5 Justificación del enfoque arquitectónico.

6.2 Controles

En un sistema, el control se refiere a las medidas o acciones tomadas para gestionar los riesgos y aumentar la probabilidad de alcanzar los objetivos y metas establecidos.

Por su parte, el autocontrol es el ejercicio mediante el cual cada participante controla su trabajo, detecta desviaciones en la ejecución de este y plantea y efectúa correctivos, de tal forma que se propicie la obtención de los resultados esperados.

Dado que, si bien los sistemas de información apoyan de una forma muy eficiente a la operación de las entidades, no puede verse como la solución de todos los problemas, es necesario identificar y fomentar comportamientos que potencien los resultados que una herramienta informática puede ofrecer. Un sistema de información por mejor que este sea si no se usa, no podrá generar los beneficios esperados. Es por esto por lo que el concepto del autocontrol se busca implementar de la mejor forma en la nueva estructura de SICOV.

El enfoque del concepto del autocontrol dentro de SICOV, se ha definido como el ejercicio mediante el cual los principales actores garantizan el control de sus propias acciones,

detectan desviaciones y efectúan correctivos necesarios para propiciar el logro de contar con un sistema de tránsito lo más seguro posible para todos los participantes.

El principal aspecto que afecta directamente este grupo de participantes en el sistema de tránsito es la cultura ciudadana. Sin embargo, esta puede ser influenciada y modificada con base en divulgación generalizada de estadísticas que muestren la relación existente entre los certificados obtenidos como resultado de acciones irregulares del aspirante, conductor o propietario y demás actores.

El autocontrol se basa en la implementación de controles que de una forma eficiente y en la mayoría de los casos, de forma inmediata, impida o alerte de un comportamiento no alineado a los conceptos de "operación normal". El hacer visible este tipo de controles mitigará la tendencia de querer evitar el cumplimiento normativo a través de ofrecimientos, dadas o fraudes.

El cumplimiento de este objetivo se facilita a través de la creación e implementación de un SICOV con una operación centralizada, de tal forma que, este modelo brinde la estructura tecnológica y procedimental apropiada para la creación de controles transversales, validaciones que requieren de una integración entre OAT.

A continuación, se describen algunos controles que aprovechan el modelo centralizado:

- Repositorio centralizado, seguro y respaldado:
 - Almacenar y custodiar en medios digitales los certificados y los FUR de las revisiones efectuadas.
 - Resultados de auditorías.
 - CEA – material de cursos, material de apoyo.
 - Cuestionarios y materia de pruebas teóricas
 - Documentos y evidencias de las labores de registro (y su aprobación) que deben realizar los diferentes actores.
- Validaciones transversales:
 - El instructor no podrá ser programado en cursos diferentes a la misma fecha y hora.
 - El instructor podrá trabajar en varios OAT siempre y cuando no sobrepase 240 horas mensuales.
 - Intentos de validación / aprobación de un trámite en diferentes OAT.
- Acreditación:
 - Validación de la acreditación de los diferentes actores que así lo requieren.
 - Evidencias y soportes de las acreditaciones.
 - Trazabilidad.

6.3 Análisis tecnológico del esquema centralizado

Teniendo en cuenta el objetivo de definir el modelo de operación más apropiado para la Entidad, adicional a la información recolectada relativa a la operación, la cual fue proporcionada por la SuperTransporte, los actuales homologados, CONFEOG y los OAT visitados, se incluyen aspectos a nivel de tendencias mundiales en torno a la implementación y operación de servicios tecnológicos.

Para este aspecto, se consultan tendencias y recomendaciones realizadas por los fabricantes líderes a nivel de tecnología y marcos de trabajo reconocidos a nivel mundial y que fueran aplicables a SICOV, describiendo a continuación los aspectos analizados y que a la postre sustentan que el modelo centralizado es el más apropiado.

6.3.1 Gestión Integral de Servicios basados en tecnología

Una de las principales preocupaciones de los líderes y responsables de la gestión de servicios en donde el componente tecnológico es considerado como crítico dado la muy alta dependencia de la operación sobre la tecnología, y de forma especial, los responsables de la gestión de estas plataformas tecnológicas buscan lograr un equilibrio óptimo de los siguientes aspectos:

- **Optimización de recursos¹:**

A través de la optimización de la infraestructura tecnológica se busca inicialmente una disminución en los costos de implementación de los servicios de T.I., de tal forma que al tener menor cantidad de equipos, menor cantidad de licencias y menor cantidad de herramientas de diferentes fabricantes para hacer la misma tarea/actividad.

- **Aumento de la productividad**

Debido a que la administración se lleva a cabo de forma centralizada, los protocolos de gestión que se establezcan (políticas, controles, criterios de uso), se aplican de forma transversal a las diferentes partes, se simplifica y se estandarizada la gestión, lo cual conlleva al aumento de la productividad del personal de TI.

Adicionalmente, servicios que integran una gran diversidad de plataformas, fabricantes, estándares aumenta la complejidad en la operación, dado que los procesos de integración se dificultan y las iniciativas de mejoramiento se ven muchas veces impedida

¹ <https://docs.microsoft.com/es-es/azure/cost-management-billing/scope-level/overview-azure-hybrid-benefit-scope>

dado que las complicaciones a nivel de integración y estabilización son tan altas que se prefiere dejar de lado la mejora a implementarla.

Estándares para la gestión de servicios de tecnología como ITIL² busca a través de la optimización de la infraestructura brindar más enfoque en los procesos y servicios, que en la infraestructura. Dejar de lado la reactividad y pasar a un enfoque preventivo y proactivo. A través de los servicios tecnológicos brindar apoyo efectivo y que este se traduzca en mejores servicios operativos / misionales, con un enfoque en el cliente. Para el caso de SICOV todo esto es facilitado a través de una operación centralizadas. Esto no implica que estos objetivos no se puedan lograr bajo un modelo federado, pero su logro si requerirá de mayores inversiones, recursos y una gestión de operaciones más compleja.

- **Aumento de la seguridad³**

El análisis de seguridad de los sistemas y la infraestructura en un esquema centralizado será más rápido y eficiente, ya que no existe la necesidad de ir sitio por sitio (se aumenta la complejidad si dichas infraestructuras están distribuidas en diferentes sedes/zonas geográficas y/o en diferentes proveedores), para poder examinar errores o fallas en los sistemas.

A nivel de seguridad, actualmente la tendencia más fuerte es Secure Access Service Edge (SASE)⁴ la cual busca centralizar la gestión de la seguridad a través de plataformas de este tipo. El éxito y facilidad de implementación es directamente proporcional a la cantidad de fabricantes y plataformas. De hecho, SASE se apoya en SDWAN tendencias que de igual forma busca centralizar la gestión de servicios de comunicación.

6.3.2 Riesgos asociados al modelo centralizado

Independiente al modelo de gestión de servicios que se implemente los riesgos asociados a la tecnología siempre estarán presentes, la diferencia la marca cuál modelo permite una mejor gestión de riesgos, definición del plan de tratamiento e implementación de controles.

Los principales riesgos asociados la gestión servicios de tecnología son los de disponibilidad, capacidad, seguridad y desempeño. Bajo un modelo centralizado el diseño de protecciones y controles permite llevar a estos riesgos a una valoración de riesgo residual

² [ITSM - IT Service Management Information General Information](#)

³ https://www.cisco.com/c/es_mx/products/security/what-is-sase-secure-access-service-edge.html?dtid=osscdc000283#~descripcion-general-de-sase

⁴ [Gartner Blog Network](#)

que permita operar dentro de unos niveles adecuados. A continuación, se escribe los mecanismos por los cuales el modelo centralizado facilita la gestión de estos riesgos.

- **Disponibilidad** ⁵

En el momento de diseñar e implementar una infraestructura tecnológica centralizada se pueden generar varios puntos de fallo los cuales en caso de materializarse un riesgo podrían generar la indisponibilidad de SICOV. Sin embargo, este riesgo puede ser mitigado de una forma muy eficiente a través de la virtualización de sus componentes, y su gestión a través de orquestadores⁶, balanceadores de carga elementos de infraestructura que de forma automática detecte una falla y realice un procedimiento de recuperación del servicio ya bien sea en el CPD primario o en el CPD de Secundario.

- **Seguridad** ⁷

Uno de los grandes retos de la gestión de la seguridad es la cobertura a nivel de elementos, componentes y servicios de la infraestructura tecnológica. El tener un modelo centralizado facilita la gestión de la seguridad dado que a través de una sola plataforma (por ejemplo, SUSE) se puede brindar completa cobertura a nivel de seguridad y potencia el análisis de cada una de sus capas: red, datos, aplicaciones, servicios, nube. Otro aspecto que evidencia la ventaja de tener un modelo centralizado son los equipos de seguridad perimetral (Firewall, AntiDDos, entre otros.) es que su implementación bajo este modelo se simplifica dado que la implementación de un solo elemento ofrece la protección requerida. Bajo un modelo federado, se requiere

En un modelo federado, implementar una capa transversal a nivel de seguridad, se dificulta dado que se requiere un equipo / plataforma por cada concesionario, dispersando los esfuerzos y dificultando el análisis integral de SICOV como por ejemplo el que se realiza a través de plataformas SIEM a nivel de correlación de eventos.

- **Capacidad y Desempeño** ⁸

A nivel de capacidad de desempeño, los ambientes centralizados ofrecen una gran ventaja a nivel de optimizar la infraestructura tecnológica dado que al tener en una sola ubicación (física o virtual) en donde operan los elementos que soportan dicha infraestructura, los tiempos de respuesta se ven favorecidos al evitar el tiempo adicional

⁵ [Novedades en los servicios de cloud de VMware | ES](#)

⁶ [Aprovechamiento de contenedores y orquestadores | Microsoft Docs](#)

⁷ [ISO 27001 Shared Services blueprint sample overview - Azure Blueprints | Microsoft Docs](#)

⁸ [Embracing hybrid multicloud—Storage edition \(asicamericas.com\)](#)

("overhead") que requieren las transacciones al tener que transportarse los datos entre diferentes componentes y entre diferentes locaciones.

Adicionalmente, las actuales tecnologías para la gestión de servicios de T.I. ofrecen capacidad flexible a nivel de recursos de procesamiento, memoria, almacenamiento o comunicaciones. Al tener un centro de recursos (Resource pooling) gestionado a través de orquestadores, hipervisores o plataformas de gestión de recursos, se podrá asignar en tiempo real recursos basados en la demanda de servicios velando porque las prioridades definidas a nivel de servicios siempre cuenten con los recursos mínimos de operación. En modelos de menor tamaño no se puede explotar de igual forma estas características de computación flexible o al menos no con la misma relación costo beneficio.

6.3.3 Centros de Datos definidos por software ⁹

Dentro del modelo de gestión de SICOV se mencionan los Centros de Procesamiento de Datos. Es necesario resaltar que este es un concepto genérico y extraído de la normatividad y requerimientos exigidos actualmente dentro de la operación del Sistema de Control y Vigilancia. Este concepto se asocia al servicio de Data Center el cual dentro del modelo propuesto podrá ser implementado en las instalaciones físicas del concesionario o a través de un proveedor de estos servicios.

La implementación de los servicios de tecnología se basa en estos centros de procesamiento de datos, pero deben ser gestionados a través del enfoque de "nube privada de servicios" haciendo compatible estos dos conceptos. La actual tendencia es la de crear centros de procesamiento virtuales (VDC Virtual Data Center) centros de datos definidos por software, brindando de esta forma la utilización de una infraestructura totalmente virtualizada y el control a través de plataformas que gestionan los servicios de esta nube de una forma integral.

6.4 Estructura conceptual del Modelo Centralizado

El modelo propuesto para la entidad es basado en una estructura centralizada en donde confluyan los diferentes actores y se soporte en una arquitectura acorde a este modelo. A continuación, se presenta gráficamente el modelo conceptual de estructura propuesta:

Ilustración 17 - Modelo Propuesto SICOV Centralizado

⁹ [Centro de datos definido por software \(SDDC\) para nubes híbridas y privadas | VMware | CO](#)



Fuente: Elaboración propia Grow Data 2021

En la parte superior se encuentran los OAT, sujetos a inspección, vigilancia y control por parte de la SuperTransporte es decir los CRC, los CEA, los CIA, los CALE y los CDA. De acuerdo con el modelo propuesto, el cual es detallado en el documento ADD – Documento de Definición de Arquitectura, cada uno de los OAT tendrá una interacción directa con el sistema de apoyo a la gestión misional del SICOV que le servirá de apoyo en la ejecución de actividades de sus procesos operativos.

En cada actividad, procedimiento o proceso del OAT que se identifique un punto de control, se establece una interoperabilidad con el sistema de control del SIVOC, de tal forma que se pueda verificar el cumplimiento del aspecto a controlar, cualquiera que sea su índole y siempre y cuando se pueda implementar por medio de elementos tecnológicos que permitan realizar la actividad de control de manera automática.

Por lo tanto, cualquier acción de control que requiera de la participación de un tercero por medio de interoperabilidad (como la RNEC, el RUNT o cualquier otro) será realizada directamente por el sistema de control. Las acciones de recibo de datos de equipos biométricos, equipos médicos para evaluación de personas, verificación de agudeza visual, prácticas de conducción o equipos técnicos para evaluación de vehículos automotores, serán realizadas a través del sistema de control del SICOV.



De otra parte, las acciones de verificación de cumplimiento normativo, tanto para la inscripción inicial en el RUNT para poder operar, así como la verificación del cumplimiento de las condiciones que le permitan mantener dicha condición durante la operación, serán realizadas por el sistema de control del SICOV.

Finalmente, la SuperTransporte como actor principal en el ecosistema del SICOV, tendrá una relación en sentido doble, una como receptor de toda la información que requiera para dar cumplimiento a sus obligaciones y responsabilidades y la otra como ente regulador y administrador de las acciones de control de forma dinámica en el tiempo.

6.5 Arquitectura de Referencia del Modelo Centralizado

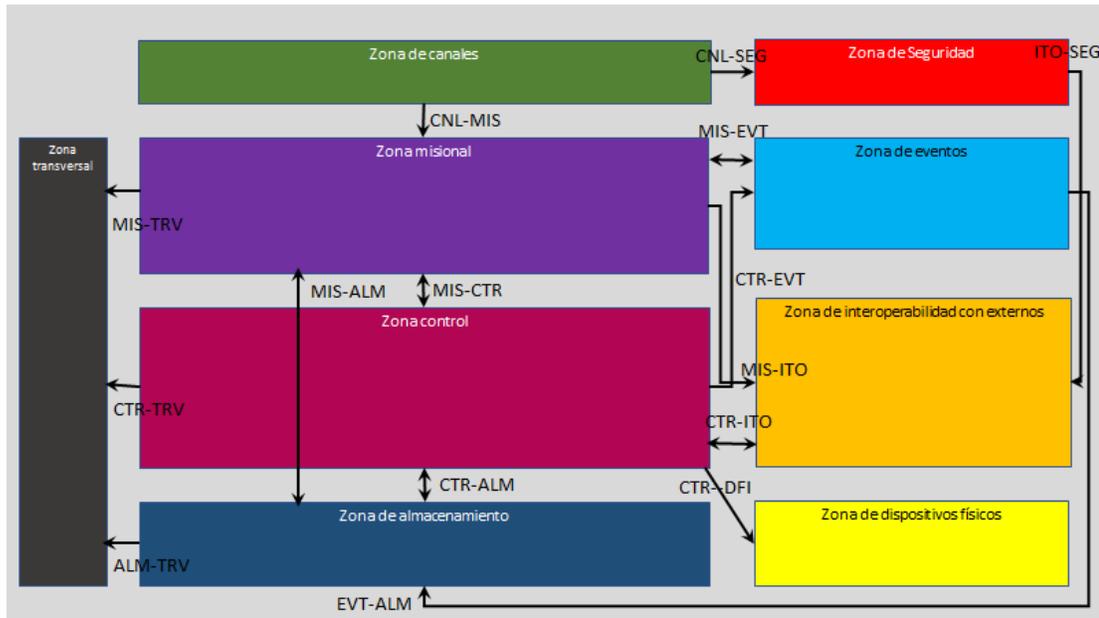
La arquitectura de referencia tiene como propósito orientar los procesos de construcción de arquitecturas de solución que atiendan preocupaciones específicas de interesados y den respuesta a requerimientos concretos.

La arquitectura de referencia para los sistemas de información del SICOV se diseñó teniendo en cuenta las siguientes consideraciones:

- Delimitar las responsabilidades entre el sistema de gestión misional (SGM) y el Sistema de Control del SICOV
- El sistema de control actúa en cada punto de control identificado en los procesos y procedimientos misionales de los OAT
- El SICOV deberá automatización de los controles, mejorando la calidad y oportunidad de la información
- El sistema de control deberá ofrecer mayor flexibilidad en la incorporación, modificación o eliminación de controles

En la siguiente imagen, se presenta de forma gráfica la arquitectura para el modelo centralizado para SICOV.

Ilustración 18 – Arquitectura de referencia modelo centralizado



Fuente: Elaboración propia Grow Data 2021

En la anterior Ilustración se presenta de forma gráfica los principales componentes de cada una de las zonas definidas en la arquitectura de referencia. A continuación, se describen cada una de las zonas que conforman la arquitectura definida para el modelo centralizado.

El presente documento toma las definiciones realizadas dentro del Documento de Definición de Arquitectura – ADD y para mayor detalle a nivel de Arquitectura Conceptual o Arquitectura de Solución del Modelo Centralizado puede consultar dicho documento y sus anexos.

6.5.1 Zona de canales

La zona de canales contiene los componentes requeridos para permitir el acceso de los usuarios del SICOV a las diferentes prestaciones funcionales disponibles.

En esta zona pueden encontrarse portales corporativos, apps móviles e incluso sistemas PQRS para la ciudadanía en general.



6.5.2 Zona de seguridad

En la zona de seguridad se encuentran los componentes encargados proveer servicios de autorización, autenticación que controla y centraliza el acceso a las demás funcionalidades como por ejemplo servicios LDAP.

6.5.3 Zona transversal

En la zona transversal se encuentran los componentes o agrupaciones de servicios utilitarios de interés común, por ejemplo, monitoreo de infraestructura y colas, gestión de auditoría y logs, gestión de backups.

6.5.4 Zona misional

La zona misional contiene los componentes requeridos para soportar la operación misional de los OAT, como el reconocimiento de conductores, la enseñanza de conducción, el diagnóstico automotor y emisión de contaminantes, el apoyo logístico para la evaluación y los cursos de reeducación de infractores de las normas de tránsito.

6.5.5 Zona control

En la zona de control se encuentran todos los componentes necesarios para implementar controles automatizados sobre las actividades operativas del OAT que tienen incidencia directa en los resultados del certificado que emite el OAT. También se encuentran los componentes necesarios para verificar que el OAT cumple con los aspectos normativos que los regulan desde la autorización de operación del Mintransporte y la subsiguiente inscripción en el RUNT, así como la verificación de que se mantienen las condiciones que dieron origen a la autorización para operar durante toda la operación del OAT.

6.5.6 Zona de interoperabilidad

La zona de interoperabilidad está integrada por las capacidades tecnológicas que permiten el intercambio de datos y la interoperabilidad entre el SICOV y los sistemas de otros actores o terceros, que permitan mejorar los procesos de intercambio de datos de manera estándar

6.5.7 Zona de eventos

La zona de eventos tiene como objetivo consolidar los componentes y servicios que le permitan al SICOV implementar servicios de colas en modelo publicador suscriptor.

La zona de eventos contiene los componentes permiten la integración asíncrona entre los componentes misionales y los componentes de control de tal forma que la operación del OAT no se vea afectada por aspectos tecnológicos del SICOV.

- El componente de administración de colas y alarmas permite implementar eventos entre publicador y suscriptor para la interoperación entre la zona misional y la zona de controles.
- El componente de stream permite procesar alarmas en tiempo real generadas en el procesamiento de las colas.

6.5.8 Zona de dispositivos físicos

La zona de dispositivos físicos tiene un propósito muy específico en el SICOV y se origina en la necesidad de controlar la forma como los datos obtenidos en por los diferentes dispositivos de evaluación y medición son transmitidos a los componentes del sistema de gestión contenidos en la zona misional, garantizando que no se producen alteración, modificación o distorsión durante la transmisión. Algunos componentes de esta zona son los que permiten integración (drivers) con dispositivos para realizar validaciones biométricas para el reconocimiento de personas, dispositivos para evaluación de condiciones físicas o psicológicas de las personas o dispositivos para determinar el estado técnico mecánico de los vehículos automotores. También puede contener componentes para la obtención y procesamiento de imágenes y videos provenientes de cámaras que registren los procesos físicos en los OAT.

En la medida que la tecnología libere y haga disponibles dispositivos IoT con capacidad lógica y de interoperación, en esta zona se ubicarán los componentes que permitan su incorporación en el SICOV.

6.5.9 Zona de almacenamiento

La zona de almacenamiento contiene los componentes que habiliten la gestión del almacenamiento de los datos del SICOV.

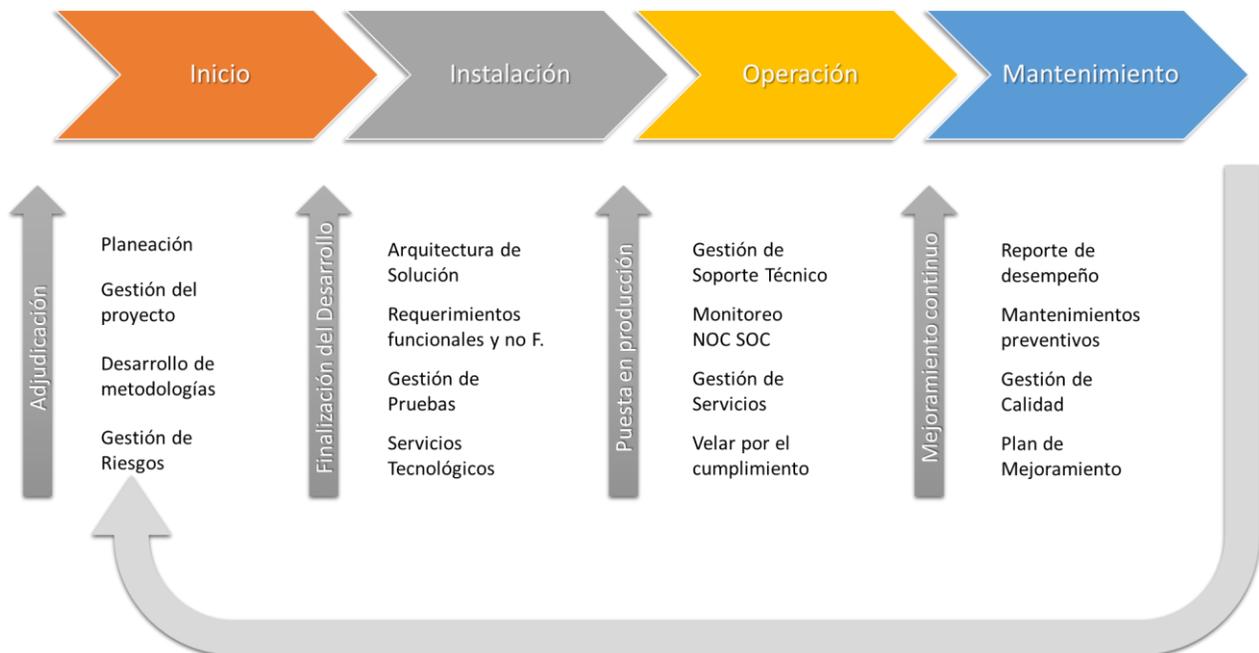
7 Instalación, Implementación, Operación y Mantenimiento

7.1 Plazos de ejecución

El plazo de la concesión es de diez (10) años a partir de su adjudicación en donde en la fase de inicio se deberán hacer todas aquellas labores de planeación de nivel del proyecto (desarrollo e implementación de SICOV) y del servicio (planear las fases de operación servicio y mantenimiento).

La fase de instalación inicia una vez la fase de desarrollo haya finalizado y se pueda dar paso a las labores de pruebas de requerimientos funcionales y no funcionales. De igual forma, en esta fase se debe instalar y configurar todos los elementos de la infra estructura tecnológica que soporta a SICOV.

Ilustración 19 - Plazo de Ejecución



Fuente: Elaboración propia Grow Data 2021

La tercera fase es la de Operación del Servicio la cual inicia una vez se tenga la certificación que a nivel de calidad del software se cumple con todos los requerimientos, así como de la estabilización y óptimo funcionamiento de las plataformas tecnológicas. En esta fase arranca a operar los servicios de monitoreo NOC / SOC y el soporte técnico y funcional de SICOV.

De forma complementaria a la fase de operación, se encuentra la fase de mantenimiento en donde a través del análisis de los ANS e indicadores de gestión se podrán identificar los aspectos que deben ser mejorados y las oportunidades de mejora. Así mismo se deberán estructurar y ejecutar los planes de mantenimiento preventivo y correctivos a que haya lugar, siendo la gestión de calidad uno de los principales insumos para alimentar la información requerida en esta fase.

A continuación, se describen los requerimientos técnicos para etapas aquí mencionadas:

7.2 Requerimientos técnicos para el inicio

De forma inicial y entre el ámbito técnico de SICOV se requiere la definición y presentación por parte del concesionario la siguiente información:

- Cronograma de actividades detallando que incluya la fase de instalación y la ruta crítica de dicho plan de actividades.
- Matriz de riesgos detallando la valoración del riesgo a nivel de impacto y probabilidad, creando un plan de acción detallado para los riesgos altos y medios.
- Metodología de desarrollo del proyecto con la definición de hitos, objetivos y entregables de cada una de las etapas, así como los mecanismos de medición y control a nivel de avance.
- Crear el repositorio oficial del proyecto, donde se podrá hacer seguimiento del versionamiento de la documentación, se mantendrá actualizada la documentación técnica del sistema y se realizará la supervisión del proyecto, con los respectivos mecanismos de seguridad. La documentación deberá incluir como mínimo diccionarios de datos, vista de componentes lógicos, de despliegue físico y de desarrollo.
- Crear el procedimiento para la gestión de configuración del proyecto.
- Crear el procedimiento por medio del cual el concesionario mantendrá actualizada la documentación técnica del sistema.
- Desarrollar el plan de proyecto haciendo especial detalle en los entregables y sus criterios de aceptación, de tal manera que se defina y controle el alcance.
- Desarrollar el plan de comunicaciones ente los actores del proyecto.
- Desarrollar el plan de calidad del proyecto.
- Presentación del grupo base del proyecto según los perfiles definidos.

- Presentar la metodología para el desarrollo del software, así como las herramientas asociadas a esta labor.
- Instalar y configurar las herramientas para administración del código fuente y sus versiones
- Plan de implementación
- Plan de contingencia
- Plan de transferencia de conocimiento técnico y funcional
- Plan de capacitación
- Plan de migración de datos
- Plan de integración
- Plan de estabilización
- Plan para la gestión de la configuración del software, que indique como mínimo su línea base y el conjunto de actividades a desarrollar para gestionar los cambios a lo largo del ciclo de vida.
 - Identificación de las versiones adecuadas de los elementos de configuración con que trabajar.
 - Gestión de las versiones de los sistemas, considerando no solo software sino también documentación.
 - Control de los cambios producidos en el software y en su documentación incluyendo la gestión de las peticiones que dan lugar a estos cambios:
 - Peticiones de cambio en requisitos y errores en el software.
 - Identificación de los responsables de gestionar las peticiones, asignando prioridad a las mismas y asignándolas a personas.
 - Garantizar la integridad, completitud y corrección de las distintas líneas base generadas.
- Desarrollar el plan detallado de interoperabilidad y garantizar las condiciones técnicas administrativas y jurídicas para la operación de dicho plan.
- Guía para el desarrollo seguro de software. El cual incluye la realización de validaciones de seguridad continua del proyecto en construcción, desde su fase inicial hasta la culminación del proyecto.

7.3 Requerimientos técnicos para la instalación – implementación

La fase de instalación e implementación de SICOV supone la finalización de la fase de desarrollo del software, durante la cual se incluyó su especificación y diseño detallado. Independiente al ciclo de vida utilizado en el desarrollo del software, la instalación inicia con la fase de pruebas y termina con su paso a producción. Dentro de esta fase se contemplan los siguientes requerimientos:

- Certificación por parte del concesionario de la finalización de la fase de desarrollo indicando que se cumplen con todos los conceptos de calidad definidos, así como la

realización de las pruebas unitarias, integrales, funcionales y de desempeño, la corrección de los incidentes identificados durante las pruebas de aceptación y la estabilización del sistema.

- Entrega de toda la documentación técnica, aprobada por la SuperTransporte, sobre la cual se basó el desarrollo del software:
 - Arquitectura detallada de solución.
 - Inventario requerimientos funcionales y no funcionales.
 - Prototipos, flujogramas, etc.
 - Casos de uso detallados o los artefactos que hagan sus veces según la metodología seleccionada.
 - Casos de prueba definidos o los artefactos que hagan sus veces según la metodología seleccionada.
 - Documentos de diseño: diagrama de clases, diagramas de secuencia, diagramas de interacción, prototipos y demás documentación que haga parte de la fase de diseño.
 - Plan de pruebas funcionales.
 - Dimensionamiento de la infraestructura tecnológica y plan de capacidad.
 - Matriz de trazabilidad de cada uno de los requerimientos solicitados.
 - Informes con el resultado de las pruebas.
 - Manuales técnicos, instalación, configuración y de usuario.
- Pruebas no funcionales:
 - Plan de pruebas de desempeño del software.
 - Plan de pruebas a nivel de cargas y estrés.
 - Plan de recuperación del software.
 - Pruebas a nivel de seguridad.
 - Pruebas de integración – interoperabilidad.
 - Informe con el cumplimiento de los requerimiento técnicos y no funcionales.
- Implementación de ambientes de pruebas, preproducción, capacitación y operación
- Certificación del licenciamiento de todo el software que interviene en la operación de SICOV.
- Ejecución del plan de prueba con certificación de la completitud a cabalidad de la ejecución satisfactoria del plan y del logro del nivel de calidad requerido para pasar a producción.
- Ejecución del plan de pruebas no funcionales con la certificación de la completitud a cabalidad de estos requerimientos logrando el nivel de calidad requerido a nivel de infraestructura para soportar el paso a producción.
- Generación Las pruebas y la respectiva certificación que indique que se cumplen a cabalidad todos los requerimientos mínimos funcionales para el paso a producción.
- Desarrollo, entrega, validación y aceptación de la documentación técnica de SICOV:
 - Manuales de usuario, manuales técnicos, manuales de administración y . manuales de mantenimiento.
 - Documentación de soporte y manejo de incidentes para la mesa de servicios.

- Ejecución de la capacitación funcional y técnica a las áreas técnicas de administración y de soporte.
- Diseñar presentar y validar el plan de despliegue para SICOV.
- (Recomendable) Antes del paso a producción realizar una prueba piloto en la cual se opere con transacciones reales y se genere un informe el cual retroalimente a los diferentes instancias técnicas y operacionales de SICOV.
- Creación del plan de Gobierno de datos en donde se incluya como mínimo, plan de calidad de datos, plan para la generación de informes, plan de estructuración de datos maestros,
- Realizar la parametrización de la configuración del sistema, de acuerdo con la línea base definida. Deberá incluir la creación de cuentas de usuario, roles y demás aspectos sobre la autenticación y autorización de usuarios del sistema,

Realización de la migración de datos de acuerdo con lo establecido en el Plan de Migración presentado como requisito técnico para el inicio.

7.4 Requerimientos técnicos para la operación y mantenimiento

- Medir y reportar cada uno de los ANS (Acuerdo de Nivele de Servicio) definidos, así como los indicadores de gestión.
- Realizar la gestión de los procesos (administración, medición, fortalecimiento a través del mejoramiento continuo) involucrados dentro de SICOV. Para ello, se requerirá una(s) herramienta(s) ALM que incluya el control de versiones, funciones de gestión de los requisitos, estimación y planificación de proyectos, gestión del código fuente y gestión de las pruebas que apoyen los procesos de gestión de necesidades, desarrollo de Software, gestión de riesgos, gestión de pruebas, seguimiento de problemas y defectos y gestión del cambio.
- Realizar el Gobierno de datos según el plan definido a través del marco de trabajo Data Management (DAMA).
- Realizar la gestión de los servicios de T.I. a través del marco de trabajo ITIL y poseer una herramienta de software que soporte el modelo de gestión
- Realizar el Gobierno la arquitectura de SICOV a través del marco de trabajo TOGAF y los lineamientos indicados por el Ministerio de las Tecnologías y comunicaciones de Colombia (MINTIC) en el Marco de Arquitectura Empresarial MAE en su versión más reciente Incluyendo el control de cambios y la actualización de la documentación de la descripción de las arquitecturas tanto de referencia como de solución en sus dominios.
- Realizar el Gobierno de SICOV a través del marco de trabajo COBIT.
- Implementar y gestionar la seguridad de SICOV:
 - Gestión periódica de vulnerabilidades.
 - Análisis proactivo de amenazas.

- Identificación de patrones de comportamiento normales con el fin de identificar actividades sospechosas o inusuales.
- Realizar pruebas de continuidad del servicio.
- verificar la implementación y efectividad de los controles de seguridad propuestos.
- Definir y gestionar la estrategia de Protección de Datos personales.
- Garantizar la disponibilidad y el acceso a la información requerida para las auditorías que se programen.
- Realizar auditorías internas y a los OAT para verificar el cumplimiento de los requisitos normativos vigentes.
- Crear, programar y hacer seguimiento a los planes de acción derivados de las auditorías ejecutadas.
- Realizar el diseño e implementación de los reportes requeridos para la identificación y análisis del desempeño de la operación.
- Realizar las jornadas de capacitación y transferencia de conocimiento de forma periódica a todos los perfiles involucrados en la gestión de SICOV y de forma especial al personal nuevo.
- Implementar y administrar una herramienta para la gestión de PQRS garantizando su disponibilidad y la gestión oportuna de los requerimientos recibidos por este medio.
- Garantizar que el personal de la mesa de servicio cuenta con la preparación y conocimiento requerido.
- Garantizar que el personal del servicio de monitoreo (NOC / SOC) cuenta con la preparación y conocimiento requerido.
- Garantizar que el personal para el apoyo en la operación cuenta con la preparación y conocimiento requerido.
- Garantizar que la cantidad y disponibilidad del personal requerido en las diferentes áreas de gestión de SICOV es el requerido.
- Realizar mediciones en todo momento de la infraestructura y componentes de software (registros de auditoría) propia de SICOV para identificar y/o proyectar posibles fallos asociados a su estabilidad (o de acuerdo con el plan de estabilización) o necesidades a nivel de crecimiento funcional o de la plataforma tecnológica que soporta la operación.
- Todo cambio sin excepción derivado de fallos o mejoras detectadas deberá ser procesado de acuerdo con lo definido en el plan para la gestión de la configuración.
- Realizar el proceso de copias de seguridad diario incremental tanto para las bases de datos, servidores, documentación y código fuente de los sistemas de información de acuerdo con su versionamiento. Las copias de seguridad a las bases de datos deben ser preferiblemente realizados a través de software especializado para el respaldo de este tipo de información, que permita administrarse y configurarse de manera centralizada mediante una interface gráfica intuitiva. Las copias de seguridad deben ser almacenados de manera segura salvaguardándolas de posible hurto, daño total o parcial y/o adulteración de la información. Las copias de seguridad se deben almacenar por un tiempo mínimo de acuerdo a la normatividad

establecida por el Ministerio de las Tecnologías de la Información y Comunicaciones de Colombia. Se debe realizar pruebas de recuperación a través de simulacros en servidores de prueba, por lo menos una vez al mes. Garantizar que la capacidad en todo momento cumple y excede los requerimientos operación hace sobre la plataforma tecnológica en este sentido.

- Velar porque la disponibilidad de los servicios asociados a SICOV cumple y exceden los niveles definidos.

7.5 Parámetros, metas de control y desempeño

7.5.1 Acuerdos de niveles de servicio

Una organización que no tiene Acuerdos de Niveles de Servicio implementados envía un mensaje muy peligroso a sus clientes y proveedores: el servicio se presta lo mejor que se puede y por ende, el cliente puede pedir incondicionalmente lo que necesite, cuando lo necesite y de la forma que lo necesite. De igual forma, los proveedores podrán entregar el servicio contratado bajo el supuesto del mejor esfuerzo y si se presentan fallas o errores, se “tratarán” de subsanar lo más pronto que se pueda.

Cuando una organización tiene implementados fuertes procedimientos de gestión de niveles de servicio y estos alineados a la gestión de contratos y proveedores, se envía un fuerte mensaje:

- A sus clientes: Entendemos exactamente las necesidades de su negocio y el impacto que los servicios que les prestamos generan sobre su operación, por ende “nos comprometemos” a ofrecer un servicio bajo unas condiciones mínimas de calidad que aseguren y generen valor a su operación.
- De igual forma, a los proveedores se les envía un mensaje en el cual se les hace notar que el servicio a recibir debe tener unas condiciones mínimas de operación y calidad, las cuales se estarán monitoreando para velar por su cumplimiento.

La gestión de niveles de servicios deberá tener como principal objetivo el de “asegurar que todos los servicios (actuales y futuros) cuentan con una definición de niveles de servicios y que estos compromisos son alcanzables, medibles y verificables”.

De igual forma, se deberán tener en cuenta las siguientes responsabilidades asociadas con la gestión de niveles de servicio:

- Monitorear, medir, reportar y revisar los niveles de servicio.
- Instigar el mejoramiento continuo de los servicios.
- Monitorear y mejorar la satisfacción de los usuarios.

- Asegurar que los niveles de servicio sean provistos dentro de un Costo / Beneficio adecuado.

7.5.1.1 Alineación Proveedores – Servicios

Para la prestación de un servicio el cual está soportado, en gran medida por componentes tecnológicos como lo es el caso de SICOV, es necesario establecer de forma inicial los acuerdos que a nivel de servicio se plantean para que, de esta forma, se identifiquen y deleguen las respectivas responsabilidades a nivel de cumplimiento. Estos compromisos en forma general son:

- **Disponibilidad:** porcentaje mínimo de operación de los servicios.
- **Continuidad:** en caso de presentarse una falla de alto impacto o de índole catastrófica, tiempo de recuperación del servicio en un ambiente de contingencia.
- **Soporte Técnico:** Indicadores asociado al desempeño de las responsabilidades mesa de servicios.
- **Desempeño:** Tiempos de respuesta asociados a las transacciones / operaciones de SICOV.
- **Perfiles del personal:** Cumplimiento y mantenimiento del personal mínimo exigido a nivel contractual.

En detalle los ANS sugeridos, para la fase de instalación, implementación, operación y mantenimiento, son los siguientes:

ID	ANSDIP01
Categoría	Disponibilidad
Nombre	Disponibilidad de SICOV
Descripción	Tiempo ininterrumpido de operación de SICOV entendido como plataforma tecnológica incluyendo todos sus componentes.
Objetivo / Meta	99% del tiempo acordado – 7x24
Frecuencia de medición	Mensual
Rango cumplimiento	>= 99% No se descuenta

	<p><99% y >=96,5% se descuenta el 0,35% del Ingreso por trámites del Mes</p> <p><965% y >=93,5% se descuenta el 0,5% del Ingreso por trámites del Mes</p>
Fórmula de cálculo	<p>DS = Disponibilidad de SICOV</p> <p>TTD = Total tiempo de disponibilidad (total de horas del mes)</p> <p>TCS = Tiempo de caída del SICOV.</p> <p>Fórmula: $DS = (TTD - TCS) / TTD * 100$</p>
Excepciones	<ol style="list-style-type: none"> 1. La variación de la disponibilidad de los servicios de SICOV, cuando por solicitud formal expresa de la SuperTransporte. 2. Cuando las ventanas de mantenimiento sean aprobadas por la Superintendencia. 3. Otros factores indirectos que afecten el servicio, tales como: mantenimientos programados, reinicios programados, problemas, o causas atribuibles a un tercero (RNEC, RUNT, SuperTransporte).

ID	ANSDIP02
Categoría	Disponibilidad
Nombre	Disponibilidad del servicio de monitoreo
Descripción	Tiempo ininterrumpido de operación del NOC / SOC entendido como el software de monitoreo y todos los elementos incluidos en dicha labor.
Objetivo / Meta	99% del tiempo acordado – 7x24
Frecuencia de medición	Mensual
Rango de cumplimiento	<p>>= 99% No se descuenta</p> <p><99% y >=96,5% se descuenta el 0,35% del Ingreso por trámites del Mes</p> <p><965% y >=93,5% se descuenta el 0,5% del Ingreso por trámites del Mes</p>
Fórmula de cálculo	<p>DSM = Disponibilidad del Servicio de Monitoreo</p> <p>TTD = Total tiempo de disponibilidad (total de horas del mes)</p>



	TCSM = Tiempo de caída del Servicio de Monitoreo. Fórmula: $DSM = (TTD - TCSM) / TTD * 100$
Excepciones	<ol style="list-style-type: none"> 1. La variación de la disponibilidad de los servicios de monitoreo, cuando por solicitud formal expresa de la SuperTransporte. 2. Cuando las ventanas de mantenimiento sean aprobadas por la Superintendencia.

ID	ANSDIP03						
Categoría	Disponibilidad						
Nombre	Disponibilidad de la Mesa de Servicios						
Descripción	Tiempo ininterrumpido de operación de la mesa de servicios entendiendo los que canales de comunicación y la plataforma de atención son los elementos incluidos dentro del ANS.						
Objetivo / Meta	99% del tiempo acordado – 7x24						
Frecuencia de medición	Mensual						
Rango de cumplimiento	<table> <tr> <td>>= 99%</td> <td>No se descuenta</td> </tr> <tr> <td><99% y >=96,5%</td> <td>se descuenta el 0,35% del Ingreso por trámites del Mes</td> </tr> <tr> <td><965% y >=93,5%</td> <td>se descuenta el 0,5% del Ingreso por trámites del Mes</td> </tr> </table>	>= 99%	No se descuenta	<99% y >=96,5%	se descuenta el 0,35% del Ingreso por trámites del Mes	<965% y >=93,5%	se descuenta el 0,5% del Ingreso por trámites del Mes
>= 99%	No se descuenta						
<99% y >=96,5%	se descuenta el 0,35% del Ingreso por trámites del Mes						
<965% y >=93,5%	se descuenta el 0,5% del Ingreso por trámites del Mes						
Fórmula de cálculo	DMS = Disponibilidad de la Mesa de Servicio TTD = Total tiempo de disponibilidad (total de horas del mes) TCMS = Tiempo de caída de la Mesa de Servicio. Fórmula: $DMS = (TTD - TCMS) / TTD * 100$						

ID	ANSCON01
Categoría	Continuidad
Nombre	Recuperación del servicio

Descripción	Tiempo de recuperación del servicio de SICOV en un ambiente de contingencia debido a una falla catastrófica del ambiente primario.	
Objetivo / Meta	4 horas	
Frecuencia de medición	Mensual	
Rango de cumplimiento	<= 4 horas	No se descuenta
	>4 horas y <=4,5 horas	se descuenta el 0,35% del Ingreso por trámites del Mes
	>4,5 horas y <=5 horas	se descuenta el 0,5% del Ingreso por trámites del Mes
Fórmula de cálculo	TRS = Tiempo Total de Recuperación del Servicio	

ID	ANSCON02	
Categoría	Continuidad	
Nombre	Punto de Recuperación	
Descripción	Tiempo máximo permitido de pérdida de información	
Objetivo / Meta	Inferior a 5 minutos	
Frecuencia de medición	Mensual	
Rango de cumplimiento	<= 5 minutos	No se descuenta
	>5 minutos y <=5,5 minutos	se descuenta el 0,35% del Ingreso por trámites del Mes
	>5,5 minutos y <=6 minutos	se descuenta el 0,5% del Ingreso por trámites del Mes
Fórmula de cálculo	TPR = Tiempo Total de perdida de información	

ID	ANSSOP01	
Categoría	Soporte Técnico – Mesa de Servicios	
Nombre	Tiempo medio de espera	
Descripción	Tiempo promedio que un usuario debe esperar hasta ser atendido por un analista de la mesa.	



Objetivo / Meta	Menor a 120 segundos	
Frecuencia de medición	Mensual	
Rango de cumplimiento	<= 120 segundos	No se descuenta
	>120 seg y <=150 seg	se descuenta el 0,35% del Ingreso por trámites del Mes
	>150 seg y <=180 seg	se descuenta el 0,5% del Ingreso por trámites del Mes
Fórmula de cálculo	TME = Tiempo Medio de espera para la Mesa de Servicio	

ID	ANSSOP02	
Categoría	Soporte Técnico – Mesa de Servicios	
Nombre	Tasa de abandono	
Descripción	Cantidad de llamadas abandonadas por no atención o por demora en la misma	
Objetivo / Meta	Menor a 5% del total de llamadas	
Frecuencia de medición	Mensual	
Rango de cumplimiento	<= 5%	No se descuenta
	>5% y <= 6%	se descuenta el 0,35% del Ingreso por trámites del Mes
	>6% y <= 7%	se descuenta el 0,5% del Ingreso por trámites del Mes

ID	ANSSOP03	
Categoría	Soporte Técnico – Mesa de Servicios	
Nombre	Registro de casos	
Descripción	Cantidad de casos registrados respecto de las llamadas recibidas	
Objetivo / Meta	99.99%	

ID	ANSSOP04	
-----------	----------	--



Categoría	Soporte Técnico – Mesa de Servicios
Nombre	Tiempo de resolución
Descripción	Tiempo máximo para resolver un caso de soporte registrado en la mesa de servicios según su criticidad.
Objetivo / Meta	Crítico: 4 horas Alto: 8 horas Medio: 16 horas Bajo: 32 horas Casos escalados a terceros: Mejor esfuerzo.

ID	ANSDES01
Categoría	Desempeño
Nombre	Cantidad de transacciones
Descripción	Cantidad de transacciones realizadas sobre la cantidad de transacciones que fueron exitosas. Una transacción no exitosa se considera la operación que por demoras en su procesamiento generó error, tiempo de espera superado o cancelado automáticamente por la plataforma por demoras / problemas en su ejecución.
Objetivo / Meta	Superior al 99.8%

ID	ANSDES02
Categoría	Desempeño
Nombre	Replica de transacciones
Descripción	Replica de las transacciones e información crítica para la operación a un ambiente de réplica para el aseguramiento de la información.
Objetivo / Meta	99.99%

ID	ANSADM01
Categoría	Administrativos



Nombre	Personal base
Descripción	Presentación y mantenimiento del personal mínimo requerido para la operación.
Objetivo / Meta	Al inicio del contrato: Presentación del grupo de trabajo al momento del inicio oficial del contrato. En la operación: Mantenimiento del grupo completo de trabajo aprobado oficialmente. Cambios: el reemplazo de personal debe tomar como máximo 8 días hábiles

7.5.2 Análisis de la Gestión

La gestión de concesionario deberá medirse de forma objetiva a través de los ANS establecidos formalmente. Adicionalmente se deberá considerar como uno de los principales indicadores de gestión los niveles de satisfacción del cliente y los niveles de calidad en la prestación del servicio.

Los niveles de satisfacción del cliente deben ser interpretados a través de encuestas que periódicamente se recomiendan sean aplicadas y analizados sus respectivos resultados. El nivel de satisfacción del usuario debe ser superior al 80%.

De igual forma la calidad en la prestación del servicio en una forma básica puede ser medida a través del porcentaje de resolución de casos en primer nivel y el tiempo promedio para resolver un caso (agrupado por criticidad).

A nivel de gestión, el concesionario deberá ser medido por el nivel de cumplimiento de los ANS, el nivel de satisfacción del cliente y la calidad en la prestación del servicio. Como parte del mejoramiento continuo y como resultado del análisis periódico (mensual) del desempeño del servicio, se deberán estructurar planes de acción enfocados a la mitigación o solución de los aspectos que así lo requieran.

8 Aspectos Técnicos Contractuales

8.1 Perfiles técnicos de las empresas – análisis del sector

8.1.1 Perspectivas del sector

La actividad económica está dividida en sectores económicos diferentes, donde cada sector hace referencia a una parte de la actividad económica, cuyos elementos tienen características comunes, guardan una unidad y se diferencian de otras agrupaciones. Su división se realiza de acuerdo con los procesos de productos o servicios que ocurren al interior de cada uno de ellos.

Según la división de la economía clásica, los sectores de la economía son los siguientes:

- Sector primario o sector agropecuario.
- Sector secundario o sector Industrial.
- Sector terciario o sector de servicios.

El presente estudio se clasifica en el sector terciario o sector de servicios; incluye aquellas actividades que no producen una mercancía (producto tangible) en sí, pero que son necesarias para el funcionamiento de la economía del país. Como ejemplos de ello tenemos el comercio, los restaurantes, los hoteles, el transporte, los servicios financieros, las comunicaciones, los servicios de educación, los servicios profesionales, científicas y técnicas, administrativas, servicios de Gobierno, entre otras.

Las empresas de servicios son aquellas creadas cuyo objeto principal es de proveer a los clientes y/o usuarios un servicio, mediante el desarrollo de una actividad intangible. Tiene como fin satisfacer al cliente en el cumplimiento de una necesidad concreta hacia un individuo sea persona natural o jurídica.

En el sector de prestación de servicios profesionales se clasifica en cada actividad profesional, tecnológica y/o técnica en: conectividad, redes y telecomunicaciones, construcción, transporte, educación, cultura, turismo, salud, ambiental, vigilancia entre otros.

La mayoría de las empresas de prestación de servicios se tiene como objeto principal: asesorías, diseños, consultorías, interventorías donde el producto a entregar es intangible, pero sirve para estructurar, planear, controlar, supervisar un proyecto o un bien material que se necesita.

Las empresas de presentación de servicios pueden ser privada, público; en este sector económico se encuentran servicios de auditorías fiscal, de mantenimiento y servicios administrativos o generales; asesoramiento técnico, financiero, jurídico, servicios de educación, servicios de comunicaciones, transporte, recreación, turismo etc. Estos son administradas o lideradas por diversidad de profesionales independientes como ingenieros, abogados, administradores entre otros.

8.1.2 Evolución del subsector de servicios de tecnologías de la información tic

En Colombia en el 2010 la Comisión regulación de comunicaciones -CRC, realizó una revisión del estado y evolución del sector de las TIC en el país; donde se evidenció que el sector creció y recibe mayores ingresos de derivados de los servicios de telefonía móvil y fija, donde se dio el crecimiento de dos empresas de proveedores más grandes del país.

En el plan vive Digital 2010-2014, se buscó la conectividad del país, facilitando el acceso a internet y banda ancha en estratos bajos, por lo que se define la intervención de proyectos para la estructuración de una infraestructura del ecosistema digital que permita la evolución de los servicios a nivel nacional¹⁰.

El aumento del consumo de servicios de telecomunicaciones por parte de los ciudadanos a nivel nacional y el nuevo desarrollo de estrategias para ampliar las coberturas mediante tecnologías como la fibra óptica, influye en el crecimiento de la cobertura de las Tecnologías de la información y las comunicaciones (TIC), y en el PIB.

Así mismo la industria de software que hace referencia a las licencias de sistemas informáticos en empresas y entidades públicas, aplicaciones de software, los servicios de consultoría especializadas en TI (tecnología de la información), la cual se refiere a los servicios de gestión de procesos empresariales, soporte, diseño y desarrollo de tecnología de la información (TI) para aplicaciones, programas, sistemas de control y vigilancia, servicios de alojamiento, entre otras actividades económicas.

Por lo anterior, las TIC son el apoyo a las necesidades que evidencia la economía para los usos específicos de las redes de comunicaciones y los bienes TIC; en el que empresas y entidades las utilizan como instrumentos de gestión, planificación, implementación de tecnologías y políticas de cero papel, seguimiento, control y vigilancia en los diferentes procesos.

Durante los últimos años en el sector de las Tecnologías de la información (TI) en Colombia, se han desarrollado servicios completos de manejo remoto de infraestructura, así como el desarrollo y mantenimiento de aplicaciones software para distintas empresas de diferentes sectores económicos.

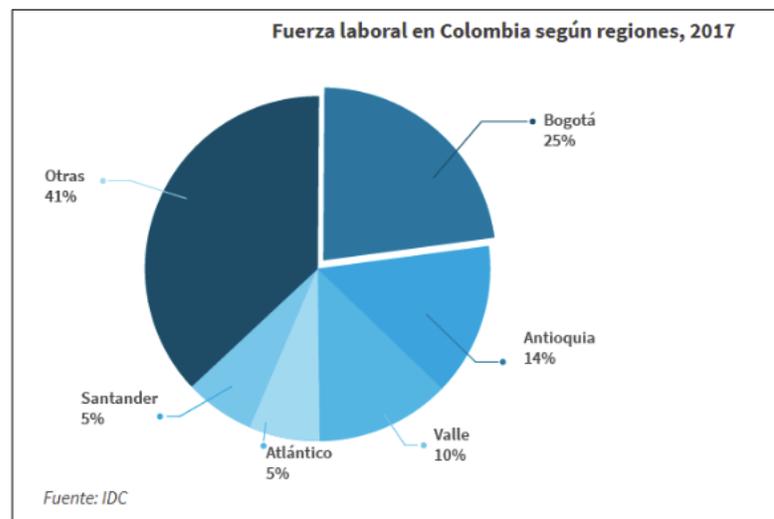
10 https://colombiatic.mintic.gov.co/679/articles-14305_panoranatic.pdf
(mintic.gov.co) - 24/08/2021.

articles-14305_panoranatic.pdf

El incremento del recurso humano capacitado y la infraestructura tecnológica de primera calidad se ha reconocido por las grandes multinacionales y empresas han escogido a Bogotá como plataforma offshore para atender los mercados externos¹¹.

Donde la fuerza laboral en las regiones estadística en el 2017; se establece de la siguiente manera: Bogotá 25%, Antioquia 14%, Valle 10%, Atlántico 5%, Santander 5% y otras del 41%, como se muestra en la gráfica datos suministrados en informe de IDC.

Ilustración 20 - fuerza laboral en Colombia - 2017



De acuerdo con documento presentado panorama la tecnología de información y comunicación (TIC)¹², el comportamiento macroeconómico del sector de la tecnología de información y comunicación TIC en Colombia (MINTIC, 2015), se presenta la cadena de valor del sector de las TIC así:

- La infraestructura que soporta la utilización de los servicios y productos.
- La fabricación y/o venta de los bienes TIC.

¹¹ <https://es.investinbogota.org/sectores-de-inversion/la-industria-de-ti-en-bogota-24/08/2021>.

¹² Comportamiento Macroeconómico del sector TIC en Colombia (MINTIC 2015)



- La producción de los servicios de telecomunicaciones, donde el servicio de internet comienza a ser el punto de surgimiento de una nueva industria.
- La industria de las plataformas digitales. Toda la cadena de valor tiene como componente transversal el conjunto de actividades.
- Investigación, desarrollo e innovación necesarios para la continua evolución del sector.

Mediante Acuerdo marco de Software empresarial Colombia Compra eficiente¹³ agrupó en tres (3) grandes grupos:

Software de propósito general: se clasifican los softwares de ofimática, CRM, ERP, base de datos entre otros.

Desarrollo de software a la medida: Una vez realizada la revisión de la posibilidad de que exista en el mercado un software que atienda su necesidad, si dicha herramienta no se encuentra en el mercado el cliente puede recurrir a este tipo de software para la atención de su necesidad.

Fábrica de Software: Como en el caso anterior si en el mercado un cliente evidencia que no existe un software que pueda atender su necesidad, y el cliente no cuenta con un presupuesto para poner un proyecto de desarrollo en funcionamiento, puede recurrir a este tipo de software, el cual reutiliza código previamente escrito con el fin de atender las necesidades específicas del destinatario final, teniendo en cuenta que, a diferencia del software a la medida, este no tiene en cuenta todo el ciclo de vida del software.

La mayoría de los productos generales del mercado en la prestación de servicios TIC pertenece a la industria del software donde hace referencia a licencias, sistemas informáticos paquete de aplicaciones de software, redes tecnológicas, basados en investigación en ingeniería, investigación y tecnología.

13

https://colombiacompra.gov.co/sites/cce_public/files/cce_documents/guia_de_buenas_practicas_software_ver1_Logo_01.pdf

El mercado para las entidades estatales se enfocan en el desarrollo de proyectos de modernización, servicios de TI para dar cumplimiento a los proceso misionales con el fin de capturar, procesar, almacenar y distribuir la información generado en cada uno de los procedimientos que hagan parte del gobierno en concordancia con el plan nacional de gobierno y estrategias, que tienen como finalidad la estructuración de un estado más eficiente, transparente y participativo gracias a los avances y servicios al implementar las tecnologías de la información y comunicaciones (TIC).

8.1.3 Composición del sector TIC en Colombia

La cadena de valor del sector de las Tecnologías de la información y comunicaciones (TIC); se destacaba principalmente por la infraestructura, que provee el acceso a los servicios de telecomunicaciones y comunicaciones, el auge de contenidos y uso de aplicativos de software específicos donde la industria TI, tenía una proporción pequeña del mercado.

Desde el 2018 a la fecha, se observa un sector TIC evolucionado, donde las metas de la política del cuatrienio 2018 - 2022 se han venido cumpliendo y donde aparecen términos como la transformación digital (economía digital), explotación de datos e inteligencia artificial para ofrecer nuevos retos en el mercado.

Debido a esta transformación presentada por el sector y con el fin de hacer una mejor medición del crecimiento de este dentro del Producto Interno Bruto del país, se adicionó a la cadena de valor el componente de la industria de las plataformas digitales que emerge de la economía digital.

Así las cosas, dicha cadena está integrada actualmente por los siguientes componentes:

- Fabricación y/o Venta de bienes TIC.
- Producción de servicios de telecomunicaciones.
- Infraestructura que soporta los servicios
- Investigación, desarrollo e innovación - I+D+i

La producción de los productos y servicios TIC se encuentran: servicios y redes de telecomunicaciones: servicios de telefonía fija, móvil, transmisión de datos, internet, correos y postales, radio y televisión, entre otros.

Así mismo, se encuentra la industria de software que hace referencia a licencias, sistemas informáticos, paquetes de software de aplicaciones.

Los servicios de servicios en TI (tecnología e información) se refieren a los servicios de gestión de procesos empresariales, soporte, diseño y desarrollo de TI para aplicaciones, servicios de alojamiento (hosting), entre otros. Bajo este contexto, la infraestructura tecnológica ejerce un papel importante en cumplimiento de los objetivos y metas organizacionales, para el desarrollo del objeto a contratar.

8.1.4 Perfil técnico detallado

Clasificador de Bienes y Servicios de Naciones Unidas (UNSPSC)

Varias de las actividades del contrato se encuentran codificadas en el Clasificador de Bienes y Servicios de Naciones Unidas (UNSPSC) en los siguientes códigos

CLASIFICADOR DE BIENES Y SERVICIOS UNSPSC					
Grupo	Segmento	Familia	Clase	Producto	Descripción
(E) Servicios	81	11	15	00	Ingeniería de software o Hardware
(E) Servicios	81	11	16	00	Programadores de computador
(F) Servicios	81	11	17	00	Sistemas de manejo de información
(F) Servicios	81	11	18	00	Servicios de sistemas y administración de componentes de sistemas
(F) Servicios	81	11	20	00	Servicio de datos



CLASIFICADOR DE BIENES Y SERVICIOS UNSPSC					
Grupo	Segmento	Familia	Clase	Producto	Descripción
(F) Servicios	81	11	22	00	Mantenimiento y soporte de software
(F) Servicios	80	10	15	00	Servicios de consultoría de negocios y administración corporativa
(F) Servicios	80	10	16	00	Gerencia de proyectos

Experiencia específica

El Oferente deberá acreditar directamente las siguientes experiencias:

1. Experiencia en mínimo tres (3) y hasta seis (6) contratos cuyos valores (incluidas sus adiciones) sumen, como mínimo, el cuarenta por ciento (40%) valor de CAPEX del modelo financiero, con corte a diciembre de 2021 expresado en SMMLV y cuyo objeto u obligaciones consistan en: prestación, integración e interoperabilidad de servicios tecnológicos de información y comunicaciones y/o de Sistemas de Información que permitan realizar Transacciones. El plazo de ejecución de los contratos que se acrediten debe ser de mínimo seis (6) años, sumando los plazos individuales de cada uno (incluidas sus prórrogas).

El participante deberá acreditar en mínimo con tres (3) y hasta seis (6) contratos cuyo objeto u obligaciones consistan en la puesta en funcionamiento y/o operación de un sistema de gestión integral que implique las etapas de instalación, configuración, operación y soporte; el alcance debe involucrar la prestación de servicios de gestión de redes, aprovisionamiento de infraestructura, gestión de comunicaciones y procesamiento de datos, desarrollo de software, soluciones de centro alterno, mantenimiento de infraestructura y administración de licenciamiento de terceros, soporte de mesa de ayuda para acreditar esta experiencia, el participante deberá acreditar como cincuenta por ciento (50%) del valor de CAPEX del modelo financiero expresado en SMMLV.

2. Experiencia en mínimo tres (3) y hasta seis (6) contratos cuyos valores (incluidas sus adiciones) sumen el diez por ciento (10%) valor de CAPEX del modelo financiero, con corte a diciembre de 2021 expresado en SMMLV y cuyo objeto u obligaciones consistan en: la administración y operación de plataformas y/o servicios tecnológicos en nube pública o privada con un mínimo de 200.000 transacciones mensuales que involucren servicios a ciudadanos colombianos. El plazo de ejecución de los contratos que se acrediten debe ser de mínimo seis (6) años, sumando los plazos individuales de cada uno (incluidas sus prórrogas).

Para efectos de acreditar la experiencia, debe tenerse en cuenta que:

- Solo se tendrán en cuenta los siguientes contratos:
 - Concesión: ejecución Mínima de cuatro (4) años de ejecución, los cuales deberán ser certificados por la interventoría o la entidad estatal.
 - Otros tipos de contrato: se requerirá que se encuentren registrados en el RUP, y estar acompañados de la certificación expedido por la entidad contratante.

Solo se tendrán en cuenta contratos que se hayan ejecutado dentro de los diez (10) años anteriores a la Fecha de Cierre.

- La experiencia adquirida en Estructuras Plurales Anteriores se tendrá en cuenta, para efectos del cálculo del valor, en proporción a la participación al interior de esa estructura; y, en relación con el plazo, la totalidad del plazo de ejecución que lleve el contrato.
- En el evento se incluyan en "Experiencia general" más contratos de los admitidos, estos no se tendrán en cuenta.
- No se admiten las auto certificaciones de experiencia.
- El mismo contrato puede ser utilizado para acreditar varias experiencias, no obstante, es importante que este, al momento de realizar las verificaciones de los códigos UNSPSC en el RUP, coincidan con cada uno de los componentes requeridos.
- Experiencia específica en desarrollo

El Oferente deberá acreditar directamente experiencia en mínimo tres (3) y hasta seis (6) contratos cuyos valores (incluidas sus adiciones) sumen, como mínimo el veinte por ciento (20%) del valor de CAPEX del modelo financiero con corte de diciembre de 2021 y cuyo objeto u obligaciones comprendan el ciclo de vida de los Sistemas de Información, en particular, el análisis, el diseño, el desarrollo, la realización de pruebas, la implantación, la configuración, y la puesta en producción de aplicativos. El plazo de ejecución de los contratos que se acrediten debe ser de mínimo seis (6) años, sumando los plazos individuales de cada uno (incluidas sus prórrogas).

8.2 Perfiles de los profesionales claves

ITEM	NOMBRE DEL ROL	CANTIDAD	FORMACION	EXPERIENCIA
1	GERENTE DE PROYECTOS	1	Profesional de la Ingeniería, con especialización en Gerencia de Proyectos o afines. Certificación PMP (vigente) Certificación Scrum Máster	Diez años de experiencia profesional en proyectos TI y mínimo 3 proyectos de Arquitectura Empresarial en entidades del estado colombiano.
2	EXPERTO LIDER EN ARQUITECTURA	1	Profesional de la Ingeniería. Certificación Togaf Certified. Certificado Lean StartUp.	Cinco años de experiencia profesional en proyectos consultivos y mínimo 3 proyectos de Arquitectura Empresarial en entidades del estado colombiano.
3	LIDER EN ARQUITECTURA DE NEGOCIO SENIOR	1	Profesional de la Ingeniería, con especialización en áreas de la administración o la ingeniería. Certificación Togaf Certified.	Cinco años de experiencia profesional en proyectos consultivos y mínimo 3 proyectos de Arquitectura Empresarial en entidades del estado colombiano.
6	ARQUITECTO JUNIOR DE NEGOCIO	3	Profesional de la Ingeniería o la administración.	Dos años de experiencia profesional en proyectos consultivos y mínimo 1 proyectos de Arquitectura Empresarial en entidades del estado colombiano.
7	EXPERTO EN ARQUITECTURA DE DATOS E INFORMACION	1	Profesional de la Ingeniería de sistemas o electrónica y afines. Certificación Togaf Certified. Certificación SOA Profesional	Cinco años de experiencia profesional en proyectos TI y mínimo 3 proyectos de Arquitectura Empresarial en entidades del estado colombiano.
8	ARQUITECTO JUNIOR DE DATOS E INFORMACION	1	Profesional de la Ingeniería de sistemas o electrónica y afines. Certificación Togaf Certified.	Tres años de experiencia profesional en proyectos TI y mínimo 2 proyectos de Arquitectura Empresarial en entidades del estado colombiano.
9	INGENIERO APOYO DE DATOS E INFORMACION	3	Profesional de la Ingeniería de sistemas o electrónica y afines.	Dos años de experiencia profesional en proyectos TI.

ITEM	NOMBRE DEL ROL	CANTIDAD	FORMACION	EXPERIENCIA
10	EXPERTO EN ARQUITECTURA DE SISTEMAS DE INFORMACION	1	Profesional de la Ingeniería de sistemas o electrónica y afines, con especialización en construcción de software o afines. Certificación Togaf Certified.	Cinco años de experiencia profesional en proyectos TI y mínimo 3 proyectos de Arquitectura Empresarial en entidades del estado colombiano.
11	ARQUITECTO JUNIOR DE SISTEMAS DE INFORMACION	1	Profesional de la Ingeniería de sistemas o electrónica y afines. Certificación Togaf Certified.	Tres años de experiencia profesional en proyectos TI y mínimo 2 proyectos de Arquitectura Empresarial en entidades del estado colombiano.
12	INGENIERO APOYO DE SISTEMAS DE INFORMACION	1	Profesional de la Ingeniería de sistemas o electrónica y afines.	Dos años de experiencia profesional en proyectos TI.
13	EXPERTO EN ARQUITECTURA DE INFRAESTRUCTURA TECNOLÓGICA	1	Profesional de la Ingeniería de sistemas o electrónica y afines, con especialización en áreas de la ingeniería o la administración. Certificación Togaf Certified. Certificación Cobit V5. Certificación ITIL Expert.	Cinco años de experiencia profesional en proyectos TI y mínimo 3 proyectos de Arquitectura Empresarial en entidades del estado colombiano.
14	EXPERTO EN INFRAESTRUCTURA TECNOLÓGICA	2	Profesional de la Ingeniería de sistemas o electrónica y afines. Certificación ITIL Foundation.	Tres años de experiencia profesional en proyectos TI y mínimo 2 proyectos de Arquitectura Empresarial en entidades del estado colombiano.
15	INGENIERO APOYO INFRAESTRUCTURA TECNOLÓGICA	1	Profesional de la Ingeniería de sistemas o electrónica y afines.	Dos años de experiencia profesional en proyectos TI.
16	DOCUMENTADOR	2	Profesional en áreas de la administración o ingeniería.	Dos años de experiencia profesional en proyectos consultivos.
17	AUDITOR	1	Profesional de la Ingeniería, con especialización en áreas de la ingeniería o la administración. Certificación ISO 20000-1	Cinco años de experiencia profesional y mínimo 3 proyectos consultivos desempeñando actividades de auditor y/o garante de la calidad.