Documento de Definición de Arquitectura (ADD)

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 Transito (OAT).

CONTROL DE VERSIONES			
VERSIÓN	**FECHA**	**ELABORADO POR**	**MOTIVO**
0.1	21/10/2021	Mario Briceño / Guiovanni 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	Gerente de Proyectos	Mario Briceño Torres	30-12-2021
Ing. Guiovanni Serrano	Asesor Gerencia de proyectos		30-12-2021

Contenido

1 Introducción 18
2 Objetivo 18
3 Cumplimiento normativo 19
3.1 Aspectos normativos 19
3.2 Normas de Calidad 19
3.2.1 Normas de Calidad aplicables a CRC 20
3.2.2 Normas de Calidad – CDA 21
3.2.3 Normas de Calidad – CALE 22
3.2.4 Normas de Calidad – CIA 22
3.2.5 Normas de Calidad – CEA 23
4 Arquitectura actual AS IS 23
4.1 Arquitectura de negocio 23
4.1.1 Arquitectura de referencia 23
4.2 Arquitectura de sistemas de información AS IS 38
4.2.1 Arquitectura Conceptual (Blue Print) 39
4.2.2 Arquitectura de solución actual (AS-IS) 49
4.2.3 Catálogo de soluciones, sistemas y aplicativos (SICOV) 58
4.2.4 Catálogo de servicios de intercambio de información 60
4.2.5 Diagrama actual (AS-IS) de interoperabilidad de los sistemas o aplicaciones 61
4.3 Arquitectura de datos 63
4.3.1 Arquitectura Conceptual 63
4.4 Arquitectura de Infraestructura 79
4.4.1 Catálogo de Servicios de Tecnología 79
4.4.2 Catálogo de Componentes de Infraestructura 79
4.4.3 Arquitectura conceptual actual (AS- IS) (Blueprint) 80
4.4.4 Arquitectura de Solución 87
4.4.5 Diagramas de Despliegue 94
4.5 Arquitectura de seguridad actual 108

4.5.1 Contexto 108
4.5.2 Marco normativo 108
4.5.3 Enfoque 110
4.5.4 Estado actual (AS-IS) 112
5 Justificación del enfoque arquitectónico 124
5.1 Modelo de Intención 124
5.1.1 Preocupaciones para la arquitectura empresarial de SICOV 124
5.2 Controles 132
5.2.1 Uso del sistema vial por vehículos automotores en Colombia 132
5.2.2 El control 135
5.2.3 El papel del SICOV en el sistema de tránsito en Colombia 137
5.2.4 Instrumentos para el apoyo al control 137
5.3 Principios 138
5.3.1 Negocio 139
5.3.2 Datos 142
5.3.3 Sistemas Información 146
5.3.4 Tecnología 152
5.4 Objetivos 159
5.5 Mapa de capacidades 160
6 Arquitectura objetivo TO BE 168
6.1 Arquitectura de negocio 168
6.1.1 Arquitectura de Estado Futuro (TOBE) 168
6.2 Arquitectura de sistemas de información TO-BE 254
6.2.1 Arquitectura conceptual para el modelo centralizado 254
6.2.2 Arquitectura de solución objetivo para el modelo centralizado 274
6.3 Arquitectura de Datos 295
6.3.1 Arquitectura Conceptual 295
6.4 Arquitectura de infraestructura 307
6.4.1 Arquitectura conceptual TO BE (Blueprint) 307
6.4.2 Arquitectura de solución 309

6.4.3 Diagramas de despliegue 314
6.4.4 Protocolos y Estándares 329
6.5 Arquitectura de seguridad 331
6.5.1 Protocolos, estándares y mejores prácticas 332
6.5.2 Arquitectura Conceptual 336
6.5.3 Controles de Seguridad 337
6.5.4 Arquitectura Objetivo 339
7 Anexos 345

Ilustraciones

Ilustración 1 - Ciclo de vida de un OAT 23
Ilustración 2 - Elementos de la Arquitectura de Negocio 26
Ilustración 3 - Elementos de la Arquitectura de Negocio 26
Ilustración 4 Proceso CRC Estado actual 27
Ilustración 5 Proceso CRC Estado actual 28
Ilustración 6 Proceso CDA Estado actual 29
Ilustración 7 Proceso CDA Estado actual 29
Ilustración 8 Proceso CEA Estado actual 30
Ilustración 9 Proceso CEA Estado actual 31
Ilustración 10 Proceso CIA Estado actual 31
Ilustración 11 Proceso CALE Estado actual 32
Ilustración 12 - Procedimiento - Aplicaciones CRC 36
Ilustración 13 - Procedimiento - Aplicaciones – CIA 36
Ilustración 14 - Procedimiento - Aplicaciones - CEA 37
Ilustración 15 - Procedimiento - Aplicaciones CDA 37
Ilustración 16 - Procedimiento - Aplicaciones CALE 38
Ilustración 17 Arquitectura conceptual SICOV (AS IS) 39
Ilustración 18 Mapa de zonas SICOV (AS IS) 40
Ilustración 19 Arquitectura de solución CRC 49
Ilustración 20 Arquitectura de solución CEA 52
Ilustración 21 Arquitectura de solución CDA 56
Ilustración 22 Diagrama de interoperabilidad del SICOV 61
Ilustración 23. Matriz procesos/Entidades de datos 67
Ilustración 24. Matriz Aplicaciones vs Entidades de datos 68
Ilustración 25. Flujo de información CRC As Is 69
Ilustración 26. Flujo de información CEA As Is 71
Ilustración 27. Flujo de información CDA As Is 71

Ilustración 28. Arquitectura Conceptual As Is 72
Ilustración 30. Diagrama de despliegue As Is 76
Ilustración 31. Arquitectura Conceptual Blue Print As Is 82
Ilustración 32. Arquitectura Solución actual CRC 89
Ilustración 33. Arquitectura Solución actual CEA 91
Ilustración 34. Arquitectura Solución actual CDA 93
Ilustración 35. Diagrama de despliegue homologado CRC - Olimpia 96
Ilustración 36. Diagrama de despliegue CRC – Consorcio SICOV CRC 98
Ilustración 37. Diagrama de despliegue CEA - Olimpia 100
Ilustración 38. Diagrama de despliegue CEA - SICOV CEA 102
Ilustración 39. Diagrama de despliegue CDA - Indra 104
Ilustración 40. Diagrama de despliegue CDA - Ci2 106
Ilustración 41 - Alcance del diagnóstico 111
Ilustración 42- Arquitectura de Seguridad actual 115
Ilustración 43. Avance Arquitectura Seguridad 118
Ilustración 44. Método de construcción de vistas a partir de las preocupaciones 124
Ilustración 45. Vista construida a partir de las preocupaciones 131
Ilustración 46 - Mapa de Capacidades 161
Ilustración 47 – Visión de arquitectura empresarial SICOV 168
Ilustración 48 – Modelo de interacción del SICOV con otras entidades 169
Ilustración 49 Diagrama conceptual SICOV 255
Ilustración 50 Arquitectura de referencia sistemas de información SICOV 257
Ilustración 51 Arquitectura de referencia componentes por zona SICOV 258
Ilustración 52 Arquitectura de referencia componentes zona canales 259
Ilustración 53 Arquitectura de referencia componentes zona de seguridad 260
Ilustración 54 Arquitectura de referencia componentes zona transversal 261
Ilustración 55 Arquitectura de referencia componentes zona misional 262
Ilustración 56 Arquitectura de referencia componentes zona de control 265

Ilustración 57 Arquitectura de referencia componentes zona interoperabilidad con externos 267
Ilustración 58 Arquitectura de referencia componentes zona de eventos 268
Ilustración 59 Arquitectura de referencia componentes zona de dispositivos físicos 269
Ilustración 60 Arquitectura de referencia componentes zona de almacenamiento 270
Ilustración 61 Modelo operativo recomendado para el SICOV 274
Ilustración 62 Estructura de control para el SICOV 276
Ilustración 63 Arquitectura de solución SICOV 278
Ilustración 64 Arquitectura de solución componentes zona canales 279
Ilustración 65 Arquitectura de solución componentes zona de seguridad 280
Ilustración 66 Arquitectura de solución componentes zona transversal 280
Ilustración 67 Arquitectura de solución componentes zona misional 281
Ilustración 68 Arquitectura de solución componentes zona de control 285
Ilustración 69 Arquitectura de solución componentes zona interoperabilidad con externos 286
Ilustración 70 Arquitectura de solución componentes zona de eventos 287
Ilustración 71 Arquitectura de solución componentes zona de dispositivos físicos 288
Ilustración 72 Arquitectura de solución componentes zona de almacenamiento 289
Ilustración 73 Diagrama de interoperabilidad SICOV TO BE 290
Ilustración 74. Catálogo entidades de datos ToBe 295
Ilustración 75. Flujo de información CRC To Be 298
Ilustración 76. Flujo de información CEA To Be 298
Ilustración 77. Flujo de información CDA To Be 299
Ilustración 78. Flujo de información CIA To Be 299
Ilustración 79. Flujo de información CALE To Be 300
Ilustración 80. Arquitectura Conceptual To Be 301
Ilustración 81. Diagrama de despliegue To Be 305
Ilustración 82. Arquitectura Conceptual Blue Print To Be 308
Ilustración 83. Arquitectura de Solución To Be 311

Ilustración 84. Diagrama de despliegue To-Be CRC 315
Ilustración 85. Diagrama de despliegue To Be CEA 318
Ilustración 86. Diagrama de despliegue To Be CDA 321
Ilustración 87. Diagrama de despliegue To Be CALE 324
Ilustración 88. Diagrama de despliegue To Be CIA 327
Ilustración 89. Vista Lineamientos vs SGSI (AS IS – TO BE) 332
Ilustración 90. Estándares aplicables en seguridad de la información 333
Ilustración 91. Vista Arquitectura General Seguridad – SICOV.....336
Ilustración 92. Vista Arquitectura Seguridad – Controles - SICOV 337
Ilustración 93. Vista Arquitectura Seguridad – Detallada - SICOV 344

Tablas

Tabla 1. Servicios de Negocio 35
Tabla 2 Caracterización de conectores Arquitectura de Referencia 45
Tabla 3. Guía catálogo dominios de información 64
Tabla 4. Guía catálogo entidades de datos 65
Tabla 5. Guía matriz procesos vs entidades de datos 66
Tabla 6. Guía matriz aplicaciones vs entidades de datos 67
Tabla 7. Servicios Tecnológicos OAT 79
Tabla 8. Componentes Lógicos OAT 80
Tabla 9. Normatividad aplicable en Seguridad y privacidad de la información 110
Tabla 10. Niveles de madurez 112
Tabla 11. Principios de negocio 142
Tabla 12. Principios de Información 146
Tabla 13. Principios de Sistemas de Información 151
Tabla 14. Principios de Tecnología 159
Tabla 15 - Capacidades 162
Tabla 16 Servicios de intercambio de información SICOV TO BE 292

SIGLAS

En este documento se usan las siglas con las que se conocen y se referencian diferentes elementos relacionados con el Sistema de Control y Vigilancia SICOV y se presentan a continuación:

ANS - Acuerdo de Nivel de Servicios

ANSV - Agencia Nacional de Seguridad Vial

CALE - Centro de Apoyo Logístico de Evaluación

CC - Cédula de Ciudadanía

CDA - Centro de Diagnóstico Automotriz

CEA - Centro de Enseñanza Automovilística

CIA - Centro Integral de Atención al Infractor

CRC - Centro de Reconocimiento de Conductores

GPS - Sistema de Posicionamiento Global

IP - Internet Protocol (Denota una dirección en Internet)

IOT - Internet de las cosas

MinEducación - Ministerio de Educación

MinSalud - Ministerio de Salud

MinTransporte - Ministerio de Transporte

NTC - Norma Técnica Colombiana

PIN - Número de Identificación de Proceso

OAT - Organismo de Apoyo al Transito

ONAC - Organismo Nacional de Acreditación y Certificación

REP - Registro Especial de Prestadores de Salud

RETHUS - Registro Único de Talento Humano en Salud

RNEC - Registraduría Nacional del Estado Civil

RUNT - Registro Único Nacional de Tránsito

SI - Sistemas de Información

SICOV - Sistema de Control y Vigilancia

ST - Superintendencia de Transporte

TI - Tecnología de Información

TIC - Tecnología de Información y Comunicaciones

TOGAF - The Open Group Architecture Framework

GLOSARIO

- Accesibilidad: Es una característica deseable en las páginas web e interfaces gráficas de los sistemas de información que consiste en la posibilidad que tiene un usuario de acceder a un sitio web y navegar en él, sin importar que cuente con algún tipo de discapacidad.

- Activo: Cualquier cosa que tenga valor para la organización. Existen diversos tipos de activos en una organización como: información, software, programas de computador, físicos como los computadores, servicios, la gente y sus aptitudes, habilidades, y experiencia, intangibles como Reputación o Imagen.

- Activo de Información: En relación con la privacidad de la información, se refiere al activo que contiene información pública que el sujeto obligado genere, obtenga, adquiera, transforme o controle en su calidad de tal.

- ADD: sigla en inglés que significa "Documento de diseño de Arquitectura Empresarial".

- App Code: Entorno de desarrollo integrado para el diseño de aplicaciones.

- Arquitectura empresarial: Es una práctica estratégica que consiste en analizar integralmente las entidades desde diferentes perspectivas o dimensiones, con el propósito de obtener, evaluar y diagnosticar su estado actual y establecer la transformación necesaria. El objetivo es generar valor a través de las Tecnologías de la Información para que se ayude a materializar la visión de la entidad. Cuando se desarrolla en conjunto para grupos de instituciones públicas, permite además asegurar una coherencia global, que resulta estratégica para promover el desarrollo del país.

- Artefacto: Es un producto tangible resultante del proceso de diseño y desarrollo de software o arquitectura empresarial. Ejemplos de artefactos son: diagramas de casos de uso, catálogos de sistemas de información, infraestructura tecnológica, mapas de información, entre otros.

- Back Office: (término en inglés) Es el conjunto de tareas, actividades, puestos y procedimientos administrativos de la entidad u organización encaminados a dar apoyo y soporte a la gestión de la misma. Estas operaciones o procesos no tienen que ver directamente con los ciudadano o grupos de interés externos. Los servicios de back office son procedimientos internos que se realizan antes o después de la interacción con el ciudadano o grupo de interés externo. El back office incluye toda la infraestructura para soportar el Front Office.

- Cadena de trámites: A partir de las necesidades identificadas por los ciudadanos se genera un contacto ciudadano-Estado que se resuelve mediante la ejecución de trámites. La relación que se establece entre estos trámites en función de los requisitos exigidos para su realización, los cuales se cumplen a través de otros trámites o servicios prestados por otras entidades, genera las cadenas de trámites. Esta relación puede darse intra e intersectorial, ya sea entre entidades del Estado o con particulares que desempeñan funciones administrativas.

- CALE: Los Centros de Apoyo Logístico para la Evaluación CALE serán considerados como organismos de apoyo, en los términos del parágrafo 1° del artículo 3° de la Ley 769 de 2002. Son competentes para realizar los exámenes teórico y práctico de conducción.

- CDA: Los Centros de Diagnóstico Automotor, comúnmente llamados CDA, son organizaciones dedicadas al examen técnico – mecánico y a la revisión de control ambiental de emisión de gases de los vehículos automotores (Motos, Automóviles, Servicio Público, Transporte de Carga) en Colombia.

- CEA: Todo Centro de Enseñanza Automovilística, es un establecimiento docente de naturaleza pública, privada o mixta, que tenga como actividad permanente la instrucción de personas que aspiren a obtener el certificado de capacitación en conducción, o instructores en conducción.

- CIA: El artículo segundo del Código Nacional de Tránsito define a los CIA como establecimientos donde se prestará el servicio de escuela y casa cárcel para la rehabilitación de los infractores a las normas del Código Nacional de Tránsito.

- CRC: La Resolución 1555 del 2005, artículo 3º establece que los Centros de Reconocimiento de Conductores son prestadores de servicios de salud, habilitados en el sistema único de habilitación del sistema obligatorio de garantía de calidad de la atención de salud, de conformidad con la reglamentación vigente o la que expida de manera particular para estos efectos el Ministerio de la Protección Social. Dichos Centros deberán registrarse en el Registro Único Nacional de Tránsito RUNT, cuando éste entre en funcionamiento, los aprobados por el Ministerio de Transporte, los encuentra en la página www.mintransporte.gov.co.

- Capacidad: Es una habilidad que debe tener una institución para poder cumplir con la misión y los objetivos que se propone. Se entiende que se tiene la capacidad cuando se posee procesos, infraestructura y talento humano con las competencias requeridas para prestar los servicios que debe proveer.

- Ciudad o territorio inteligente: Aquella que tiene una visión holística de sí misma, y en la cual sus procesos estratégicos y la provisión de servicios urbanos se basan en la promoción del desarrollo sostenible y la innovación, y en el uso y aprovechamiento de las TIC, con el propósito de aumentar la calidad de vida de los ciudadanos.

- Confidencialidad: Se refiere a que la información solo puede ser conocida por individuos autorizados.

- Continuidad de negocio: Proceso general de gestión que identifica amenazas potenciales a una organización y el impacto que se podría causar a la operación de negocio que en caso de materializarse. La gestión de la continuidad del negocio provee un marco de trabajo para la construcción de la resiliencia organizacional, con capacidad de respuesta efectiva que salvaguarde los intereses de las partes interesadas, reputación, marca y actividades de creación de valor.

- Datos abiertos: Son aquellos datos primarios o sin procesar, que se encuentran en formatos estándar e interoperables que facilitan su acceso y reutilización, los cuales están bajo la custodia de las entidades públicas o privadas que cumplen con funciones públicas y que son puestos a disposición de cualquier ciudadano, de forma libre y sin restricciones, con el fin de que terceros puedan reutilizarlos y crear servicios derivados de los mismos.

- Disponibilidad de la información: Se refiere a la seguridad que la información puede ser recuperada en el momento que se necesite, esto es, evitar su pérdida o bloqueo, bien sea por ataque doloso, mala operación accidental o situaciones fortuitas o de fuerza mayor.

- Estado abierto: Es una modalidad de gestión pública más transparente, sujeta a rendición de cuentas, participativa y colaborativa, entre Estado y sociedad civil, donde el Estado hace posible una comunicación fluida y una interacción de doble vía entre gobierno y ciudadanía; dispone canales de diálogo e interacción, así como información para los ciudadanos con el fin de aprovechar su potencial contribución al proceso de gestión y la ciudadanía aprovecha la apertura de esos nuevos canales participativos, podrá colaborar activamente con la gestión de gobierno, promoviendo de este modo una verdadera democracia. El Estado no solo hace referencia a la rama ejecutiva, sino a la rama legislativa, judicial y órganos de control.

- Estándar: Es un conjunto de características y requisitos que se toman como referencia o modelo y son de uso repetitivo y uniforme. Para que sea un estándar debe haber sido construido a través de consenso y refleja la experiencia y las mejores prácticas en un área en particular. Son esquemas de cumplimiento para las entidades e implican uniformidad y normalización.

- Front office: (término en inglés) Son todas las actividades, proceso, puestos y procedimientos de la entidad u organización que están en contacto y directamente relacionadas con el ciudadano o grupos de interés externos a ella.

- Gestión de T.I.: Es una práctica, que permite operar, innovar, administrar, desarrollar y usar apropiadamente las tecnologías de la información (TI). A través de la gestión de TI, se opera e implementa todo lo definido por el gobierno de TI. La gestión de T.I. permite a una organización optimizar los recursos, mejorar los procesos de negocio y de comunicación y aplicar las mejores prácticas.

- Gobierno Digital: De forma general, consiste en el uso de las tecnologías digitales como parte integral de las estrategias de modernización de los gobiernos para

crear valor público. Esto depende de un ecosistema de actores gubernamentales, ONGs, empresas, asociaciones ciudadanas e individuos que dan soporte a la producción de y acceso a datos, servicios y contenido a través de interacciones con el gobierno. En Colombia, Gobierno Digital es la política pública liderada por el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), que tiene como objetivo "Promover el uso y aprovechamiento de las tecnologías de la información y las comunicaciones para consolidar un Estado y ciudadanos competitivos, proactivos, e innovadores, que generen valor público en un entorno de confianza digital".

- Gobierno de Arquitectura Empresarial: Es una práctica orientada a establecer instancias de decisión, alinear los procesos institucionales o de negocio con los procesos, recursos y estrategias de TI, para agregar valor a las organizaciones y apoyar el cumplimiento de sus objetivos estratégicos. El gobierno de Arquitectura empresarial gestiona y controla los riesgos, mide el desempeño de la arquitectura, define políticas de arquitectura, gestiona la evolución y cambios sobre los artefactos o productos de la arquitectura. El gobierno de la arquitectura es parte del gobierno corporativo o empresarial.

- Innovación abierta: Es un método específico para adelantar procesos de innovación, en el cual se distribuyen las tareas entre actores internos y externos de una organización, para la comprensión de problemáticas, generación de ideas o desarrollo de soluciones.

- Integridad: Se refiere a la garantía de que una información no ha sido alterada, borrada, reordenada, copiada, etc., bien durante el proceso de transmisión o en su propio equipo de origen.

- Lineamiento: Es una directriz o disposición obligatoria para efecto de este documento que debe ser implementada por las entidades públicas para el desarrollo de la política de gobierno digital. Los lineamientos pueden ser a través de estándares, guías, recomendaciones o buenas prácticas.

- Manual de Gobierno Digital: Documento que define los lineamientos, estándares y acciones a ejecutar por parte de los sujetos obligados de la Política de Gobierno Digital en Colombia, el cual es elaborado y publicado por el Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), en coordinación con el Departamento Nacional de Planeación (DNP).

- Marco de interoperabilidad: Es el conjunto de principios, políticas y recomendaciones que busca facilitar y optimizar la colaboración entre

organizaciones privadas y entidades del Estado para intercambiar información y conocimiento, en el marco de los procesos de negocio, con el propósito de facilitar la entrega de servicios a ciudadanos, empresas y a otras entidades para intercambiar información, aporte de documentos y datos en línea.

- Metadatos: Son entidades de datos que incluyen información de otros datos; es decir permiten tener información de procesos, reglas de negocio, estructuras, sistemas, aplicaciones y restricciones.

- OAT: Organismos de apoyo a las autoridades de tránsito. Están definidos en la legislación vigente mediante cinco tipos de OAT como son: CALE, CDA, CEA, CIA y CRC.

- Servicios ciudadanos digitales: Es el conjunto de servicios que brindan capacidades y eficiencias para optimizar y facilitar el adecuado acceso de los usuarios a la administración pública a través de medios electrónicos. Estos servicios se clasifican en básicos y especiales.

- Sistema de Gestión Documental Electrónico de Archivo (SGDEA): Es una herramienta informática destinada a la gestión de documentos electrónicos de archivo. También se puede utilizar en la gestión de documentos de archivo tradicionales.

- SICOV: Sistema de Control y Vigilancia reglamentario al que están sujetos los organismos de Apoyo a las Autoridades de Transito (OAT).

- Tecnologías digitales: Son herramientas, sistemas, dispositivos y recursos electrónicos que generan, almacenan o procesan datos en forma de bits (0 y 1). Estos incluyen redes sociales, juegos y aplicaciones en línea, multimedia, aplicaciones de productividad, computación en la nube, sistemas interoperables, dispositivos móviles, entre otros.

- Trámite: Conjunto o serie de pasos o acciones reguladas por el Estado, que deben efectuar los usuarios para adquirir un derecho o cumplir con una obligación prevista o autorizada por la ley. El trámite se inicia cuando ese particular activa el aparato público a través de una petición o solicitud expresa y termina (como trámite) cuando la administración pública se pronuncia sobre este, aceptando o denegando la solicitud.

- Transformación digital: Es un proceso de reinvención o modificación en la estrategia o modelo del negocio, que responde a necesidades de supervivencia de las organizaciones y se apoya en el uso de Tecnologías de la Información y las Comunicaciones.

- Usabilidad: Es un anglicismo que apareció hace algunos años, que significa facilidad de uso. Desde la Norma ISO 9241-11 (1998), usabilidad se define como "El grado en que un producto puede ser usado por determinados usuarios para lograr sus propósitos con eficacia, eficiencia y satisfacción en un contexto de uso específico".

- Valor público: Se relaciona con la garantía de derechos, la satisfacción de necesidades y la prestación de servicios de calidad. Por ello, somos conscientes que no sólo es hacer uso de las tecnologías, sino cómo las tecnologías ayudan a resolver problemas reales. Este sería el fin último del uso de los medios digitales en la relación del Estado y el ciudadano.

1 Introducción

En este documento se presentan los elementos que describen la arquitectura empresarial actual y objetivo del sistema SICOV. Inicialmente se presenta la arquitectura actual (AS- IS) que resulta del análisis y procesamiento de la información obtenida de la Supertransporte, los operadores homologados, Confeorg, ONAC y de las visitas a algunos OAT que operan en la actualidad.

Luego se presentan los mismos elementos correspondientes a la arquitectura empresarial Objetivo (TO -BE) del sistema SICOV, que soportarán el modelo operativo propuesto que resulta de la ejecución del proyecto.

Este documento denominado Documento de Definición de la Arquitectura (por sus siglas en ingles ADD- Architecture Definition Document) consolida la descripción de la arquitectura empresarial que corresponde al principal entregable de la etapa 3 del proyecto denominada "Evaluar y proponer".

2 Objetivo

Basados en Marco de Referencia de Arquitectura Empresarial del Estado y el marco de trabajo de TOGAF, el objetivo del Documento de Definición de Arquitectura es el de ser

el centralizador de los principales artefactos desarrollados para describir la Arquitectura Actual (AS-IS) y la Arquitectura Objetivo (TO-BE) de SICOV.

3 Cumplimiento normativo

3.1 Aspectos normativos

Dentro de la fase de estudio y diagnóstico se desarrollan las actividades propias de los componentes técnicos, tecnológicos, financieros y jurídicos, identificando en este último documento la centralización y compendio de todo lo relacionado con la normatividad vigente y aplicable a SICOV, encontrando en detalle los siguientes temas desarrollados:

- Marco regulatorio relacionado con la operación de los Organismos de Apoyo a las Autoridades de Transito (OAT)
- Normas expedidas por el Ministerio de Transporte
- Normas de carácter legal que contienen disposiciones relacionadas con el Sistema de Control y Vigilancia SICOV de la Superintendencia de Transporte
- Actos Administrativos emitidos por la Superintendencia de Transporte para la implementación de los actuales sistemas de control y vigilancia

Dentro del Sistema de Información de Control y Vigilancia – SICOV, adicional a los aspectos normativos se identifican estándares de calidad que apoyan los diferentes ámbitos de la implementación, puesta en marcha y operación de SICOV las cuales se describen en los siguientes numerales.

3.2 Normas de Calidad

Dentro de la operación de SICOV, se identifican 5 tipos de OAT los cuales tienen formalmente establecido procedimientos de evaluación basados en estándares de calidad.

Dichos procedimientos toman como elemento de valoración el cumplimiento de estándares internaciones con el fin de establecer criterios objetivos y cuantificables para determinar si efectivamente se está cumpliendo aspectos que por su naturaleza deben ser analizados y valorados.

Los aspectos evaluados bajo las recomendaciones y controles asociados a estándares internacionales basados en la familia de las normas ISO 17000 para la acreditación de Organismos de inspección y ensayo, adicionalmente, Organismos que realizan

certificación de personas. Estas acreditaciones inician con los procesos de habilitación de los OAT y posteriormente serán evaluados de forma periódica para de esta forma mantener la habilitación. Estas valoraciones las realiza el ONAC quien tiene como objetos: a) proveer los servicios de acreditación a los organismos de evaluación de la conformidad para acreditar su competencia, b) ejercer como autoridad de monitoreo en buenas prácticas de laboratorio de la Organización para la Cooperación y el Desarrollo Económico (OCDE) y c) desempeñar las funciones de Organismo Nacional de Acreditación de Colombia.

3.2.1 Normas de Calidad aplicables a CRC

La acreditación de los Centros de Reconocimiento de Conductores- CRC, les permite demostrar su competencia e imparcialidad, como organismos evaluadores de la conformidad, para certificar la aptitud física, mental y de coordinación motriz para los aspirantes y conductores de vehículos automotores, con base en los requisitos técnicos, legales y reglamentarios.

Para el cumplimiento de estos objetivos, se cuenta con el documento de Criterios Específicos de Acreditación – Trazabilidad Metrológica dentro del cual se describen las siguientes normas de calidad, la cuales, entre otros requisitos, apoyan los procesos de valoración de los CRC:

- ISO/IEC 17025: 2017 "Requisitos generales para la competencia de laboratorios de ensayo y calibración"
- ISO/IEC 17024: 2012 "Evaluación de la conformidad. Requisitos generales para los organismos que realizan certificación de personas"
- ISO 15189: 2012 "Laboratorios Clínicos: Requisitos particulares para la calidad y la competencia"
- ILAC P10:01/2013 "Policy on traceability of measurements results"
- ISO 17511:2003, In vitro diagnostic medical devices -- Measurement of quantities in biological samples

La aplicación de la Norma ISO/IEC 17025:2017. Se enfoca especialmente en comprobar que:

- El laboratorio debe establecer y mantener la trazabilidad metrológica de los resultados de sus mediciones por medio de una cadena ininterrumpida y documentada de calibraciones, cada una de las cuales contribuye a la incertidumbre de medición, vinculándose con la referencia apropiada.
- El uso de materiales de referencia certificados
- Registros de selección, verificación y validación de métodos

- Evaluación de la incertidumbre de medición
- Documentación y evidencia del control metrológico de equipos
- Documentación y evidencia de la trazabilidad metrológica
- Documentación e implementación del aseguramiento de la validez de los resultados
- Documentación y evidencia de la competencia del personal
- Documentación y evidencia de la adecuación de las instalaciones y sus condiciones ambientales
- Registros de auditorías internas del laboratorio de calibración
- Requisitos aplicables de la ISO 17511:2015, Reactivos para diagnóstico in vitro.

3.2.2 Normas de Calidad – CDA

La acreditación, además de ser una condición para operar como OAT, es un medio para que los Centros de Diagnóstico Automotor - CDA[1] demuestren su competencia mediante el cumplimiento de los requisitos de imparcialidad, instalaciones, personal, equipos, métodos y procedimientos descritos en las Normas Técnicas Colombianas adoptadas por el Ministerio de Transporte.

Para el cumplimiento de estos objetivos, se cuenta con el documento "Criterios Específicos de Acreditación para Centros de Diagnóstico Automotor - NORMA ISO/IEC 17020:2012" dentro del cual se invocan las siguientes normas:

- NTC 4231:2012, Procedimientos de evaluación y características de los equipos de flujo parcial necesarios para medir las emisiones de humo generadas por las fuentes móviles accionadas con ciclo diésel. Método de aceleración libre.
- NTC 4983:2012, Calidad del aire. Evaluación de gases de escape de vehículos automotores que operan con ciclo Otto. Método de ensayo en marcha mínima (ralentí) y velocidad crucero; y especificaciones para los equipos empleados en esta evaluación.
- NTC 5375:2012, Revisión Técnico-mecánica y de emisiones contaminantes en vehículos automotores.
- NTC 5365:2012, Calidad del aire. Evaluación de gases de escape de motocicletas, motociclos, moto-triciclos, motocarros y cuatrimotos, accionados tanto con gas o gasolina (motor de cuatro tiempos) como con mezcla gasolina aceite (motor de dos tiempos). Método de ensayo en marcha mínima (ralentí) y especificaciones para los equipos empleados en esta evaluación.
- NTC 5385:2011, Centros de Diagnóstico Automotor. Especificaciones del servicio.

[1] Tomado de: CDA Centros de Diagnóstico Automotor — ONAC

- NTC 6218 Revisión técnico mecánica y de emisiones contaminantes en vehículos automotores cuatrimotos, moto triciclos y cuadriciclos
- NTC 6282 Revisión técnico mecánica y de emisiones contaminantes en vehículos automotores tipo ciclomotor y tricimoto

Estas normas se convierten en parámetros de evaluación objetiva de la competencia y cumplimiento del OAT respecto de los requerimientos mínimos de calidad. Para establecer el nivel de cumplimiento sin dejar lugar a dudas se deben evidenciar los resultados a través del aporte de la siguiente información:

- Resultados satisfactorios en los exámenes y determinaciones,
- El resultado satisfactorio en exámenes de informes, entrevistas, inspecciones simuladas y otras evaluaciones de desempeño.
- El resultado satisfactorio de las evaluaciones independientes para confirmar los resultados de las inspecciones.
- El resultado satisfactorio del trabajo supervisado y la formación.
- La ausencia de apelaciones o quejas legítimas.
- Los resultados satisfactorios de atestiguamiento por un organismo competente, por ejemplo, un organismo de certificación para las personas.
- Cualquier otra información que el organismo considere pertinente

3.2.3 Normas de Calidad – CALE

La Resolución 1349 de 2017 Ministerio de Transporte establece en su artículo 2:

Artículo 2°. Centros de Apoyo Logístico de Evaluación (CALE). Serán competentes para realizar los exámenes teórico y práctico de conducción de que trata la presente resolución, los organismos de apoyo que se denominarán Centros de Apoyo Logístico de Evaluación - CALE, debidamente habilitados por el Ministerio de Transporte, los que deberán contar con la certificación en la **norma técnica en seguridad de la información ISO 27001**, o la norma que la modifique o sustituya, la cual deberá mantenerse para poder realizar las pruebas.

Podrán habilitarse como CALE las personas jurídicas debidamente constituidas y registradas en el registro mercantil, que incluyan en su objeto social la realización de exámenes teórico y práctico para la obtención de la licencia de conducción, igualmente, las universidades públicas o privadas y el Servicio Nacional de Aprendizaje (SENA).

3.2.4 Normas de Calidad – CIA

La resolución 003204 de MinTransporte, en su artículo 4, establece que los CIA deben mantener la certificación en la **norma ISO 9001** expedido por un organismo de certificación acreditado en el subsistema nacional de calidad.

3.2.5 Normas de Calidad – CEA

La resolución 003245 del MinTransporte establece en su artículo 8 que los CEA deberán obtener el certificado de conformidad otorgado por un organismo de certificación acreditado con la **norma ISO IEC Guía 65** o su equivalente **GTC 38**.

4 Arquitectura actual AS IS

4.1 Arquitectura de negocio

4.1.1 Arquitectura de referencia

Ciclo de vida de un OAT

En la Ilustración 1, se presenta el ciclo de vida de un OAT. El ciclo inicia cuando el inversionista toma la decisión de operar un OAT para ofrecer el servicio al público. En esta etapa, se deberá cumplir con todos los requisitos exigidos por la ley para poder comenzar a operar. Cada OAT tiene requisitos específicos y deben interactuar con otras entidades y organismos que le permiten demostrar el cumplimiento del requisito, algunas de esas organizaciones son: el ONAC, el Ministerio de Salud, el Ministerio de Educación, entre otros.

Ilustración 1 - Ciclo de vida de un OAT

Fuente: Elaboración propia Grow Data 2021

Una vez el aspirante a convertirse en un OAT ha cumplido con todos los requisitos, debe realizar el siguiente paso que consiste en tramitar ante el RUNT su registro como OAT. Una vez finalizado este trámite, el OAT recibe su identificador denominado ID RUNT y a partir de ese momento tiene autorización para iniciar la operación y prestar servicio al público. Esto dado que una sociedad (NIT) puede tener más de un establecimiento registrado (por esto no se puede identificar únicamente con el NIT).

Después de iniciar la operación, el OAT deberá demostrar el cumplimiento de todos los requisitos establecidos por la normatividad aplicable. En el momento en que se presente un incumplimiento en los términos previstos, y este sea demostrado, el OAT será suspendido y no podrá operar ni prestar servicio al público. Esta suspensión permanecerá hasta que demuestre según lo previsto en las normas vigentes, haber resuelto el incumplimiento presentado. En este caso podrá reiniciar la operación y ofrecer sus servicios al público.

El OAT podrá operar de manera indefinida hasta que ocurra una de las siguientes situaciones: i) el inversionista decide cerrar por voluntad propia o ii) se presente una situación de incumplimiento de los requisitos normativos y estos no son resueltos por el OAT de acuerdo con las normas vigentes.

<u>El SICOV y su papel en el ciclo de vida del OAT</u>

Teniendo en cuenta que para que un certificado generado por un OAT sea válido, este solamente puede ser emitido en el momento en que el OAT cuente con su autorización de operación vigente. Por lo tanto, es imperativo que dicha autorización refleje con precisión el estado real del OAT.

Durante la etapa de montaje del OAT, el cumplimiento de cada requisito es verificado por diferentes actores y dicha verificación puede ser realizada y registrada formalmente de forma manual o automática, siempre y cuando se cumpla con la normatividad vigente. Por lo tanto, el papel del SICOV en este paso, consiste en apoyar la verificación del cumplimiento de los requisitos para que el OAT pueda entrar en operación.

Mientras el OAT mantenga vigente la autorización para operar, el SICOV deberá soportar los procesos requeridos para garantizar que todos los elementos que intervienen en la generación de un certificado expedido por un OAT reflejen de manera fiel y precisa la realidad. Algunos ejemplos de estos elementos se enumeran a continuación:

- Equipos técnicos de apoyo para realizar pruebas médicas.
- Equipos técnicos de apoyo para determinar las condiciones de un vehículo
- Cumplimiento de requisitos del personal humano que interviene en el proceso de evaluación, enseñanza o certificación entre otros.
- Elementos que permitan demostrar que el OAT presta sus servicios en la locación geográfica autorizada.

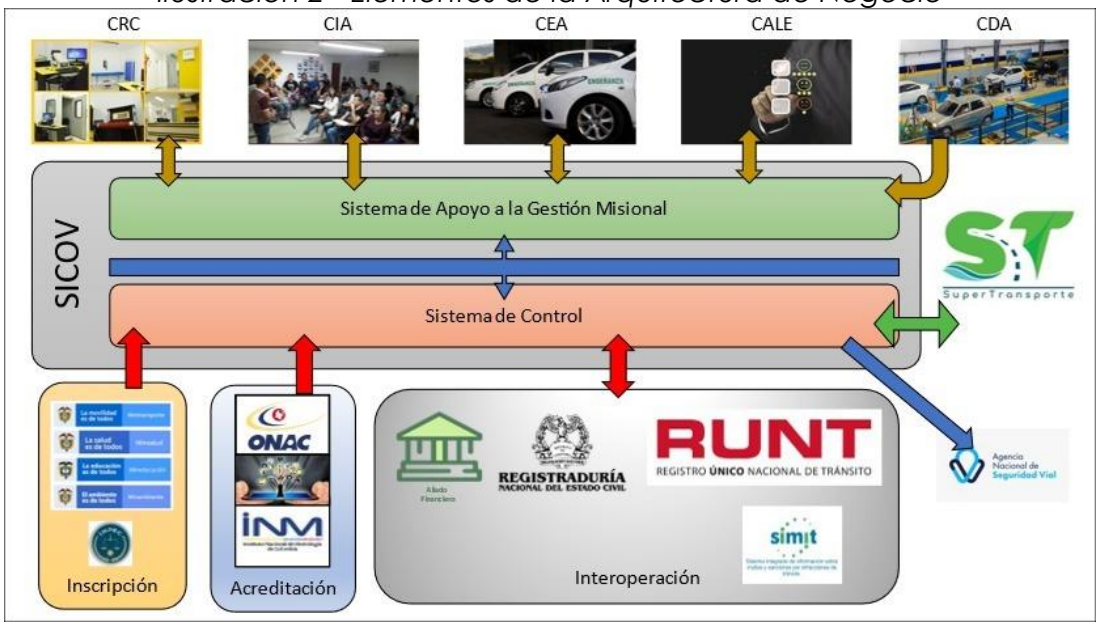
Durante la operación del OAT, el SICOV también deberá soportar los procesos que permitan identificar posibles irregularidades en la operación del OAT, así como la generación de la información necesaria para realizar las acciones normativas que debe realizar la ST.

Finalmente, el SIVOC también deberá soportar los procesos que permitan determinar que un OAT en estado de suspendido ha ejecutado satisfactoriamente las acciones requeridas para dar cumplimiento al plan de mejoras a las faltas que ocasionaron su suspensión. En caso de que esto no ocurra, el SICOV deberá garantizar que el OAT cerrado definitivamente no preste más servicios al público.

Entorno de interacción del SICOV

El sistema de control y vigilancia SICOV tiene una serie de interacciones con diferentes entidades del Estado Colombiano como se puede ver en la ilustración 2:

Ilustración 2 - Elementos de la Arquitectura de Negocio

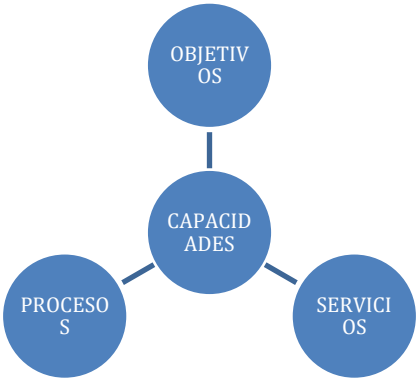


Fuente: Elaboración propia Grow Data 2021

<u>Diseño de la arquitectura en su estado actual</u>

Siguiendo este ciclo establecido la arquitectura de negocio se define de acuerdo con los elementos identificados en el metamodelo[2] de Arquitectura Empresarial como son: objetivos, capacidades, procesos y servicios.

Ilustración 3 - Elementos de la Arquitectura de Negocio



[2] Anexo 2 Metodología consultoría SICOV numeral 14.1

Fuente: Elaboración propia Grow Data 2021

Las capacidades y los objetivos se mostrarán más adelante en el capítulo 5 de modelo motivacional de este mismo documento.

A continuación, se describen estos componentes desde la arquitectura de negocio actual.

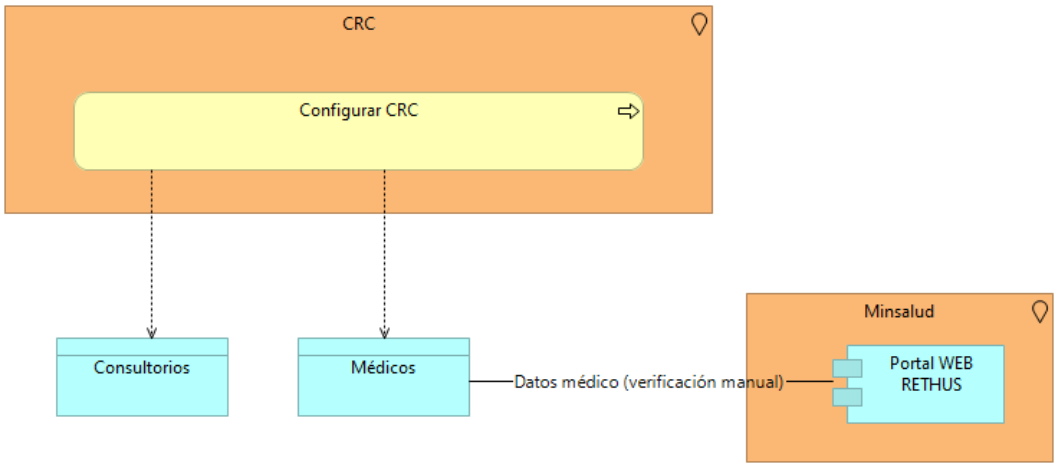
4.1.1.1 Procesos y unidades organizacionales

Los procesos de negocio también son otra perspectiva (al igual que las capacidades de negocio) que definen el comportamiento, pero en este caso especificando el "cómo" (cómo es hecha la actividad). Los procesos de negocio son contenedores que encapsulan la lógica de la operación del negocio en la forma de procesos, actividades, roles, entradas, salidas, recursos necesarios. Para la arquitectura actual (AS-IS), de acuerdo con la catalogación existente en el repositorio de Arquitectura, se identifica el Proceso de Negocio con los subprocesos o procedimientos, para finalizar con las actividades que los componen.

A continuación, se presentan los procesos actuales por cada uno de los tipos de OAT:

<u>PARA CRC</u>

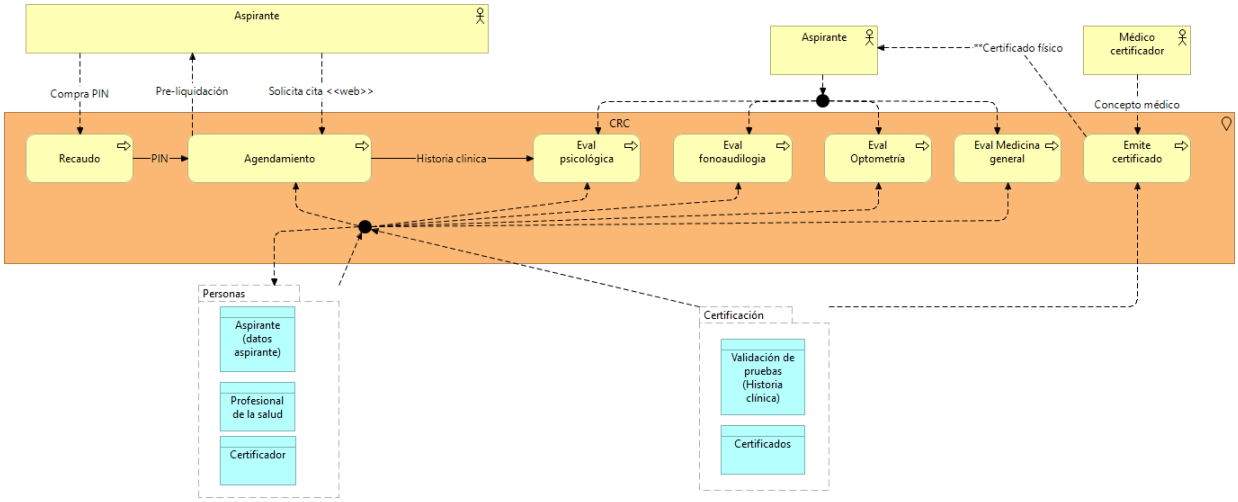
Ilustración 4 Proceso CRC Estado actual



Fuente: Elaboración propia Grow Data 2021

Iniciando el proceso (ver ilustración 4) para el CRC lo que se realiza es el registro y configuración del CRC en el SICOV, registrando los consultorios y lo médicos especialistas que prestan el servicio previa verificación con el sistema RETHUS para garantizar que estos especialistas médicos cumplan con los requisitos establecidos por MinSalud como entidad reguladora del sector salud.

Ilustración 5 Proceso CRC Estado actual

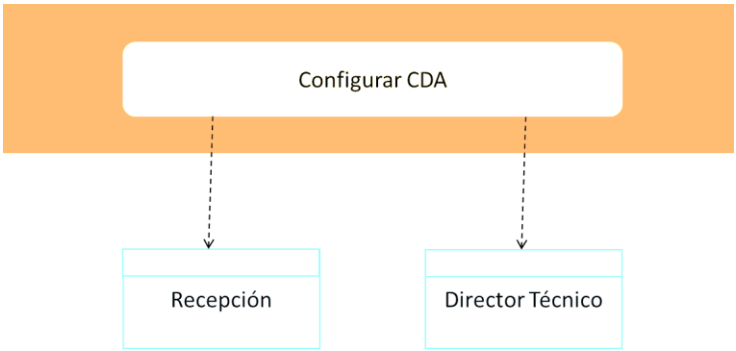


Fuente: Elaboración propia Grow Data 2021

Posteriormente, como se muestra en la ilustración 5, se realiza el registro del aspirante mediante la verificación del PIN de recaudo y el agendamiento respectivo, una vez cumplidos estos pasos se procede con la realización de los distintos exámenes médicos por especialidad: optometría, fonoaudiología, psicología y evaluación de medicina general. Si no hay elementos de juicio que impidan que una persona pueda conducir un vehículo se expide el certificado de aptitud con las anotaciones que haya lugar, como por ejemplo el uso de lentes oftálmicos para conducir.

PARA CDA

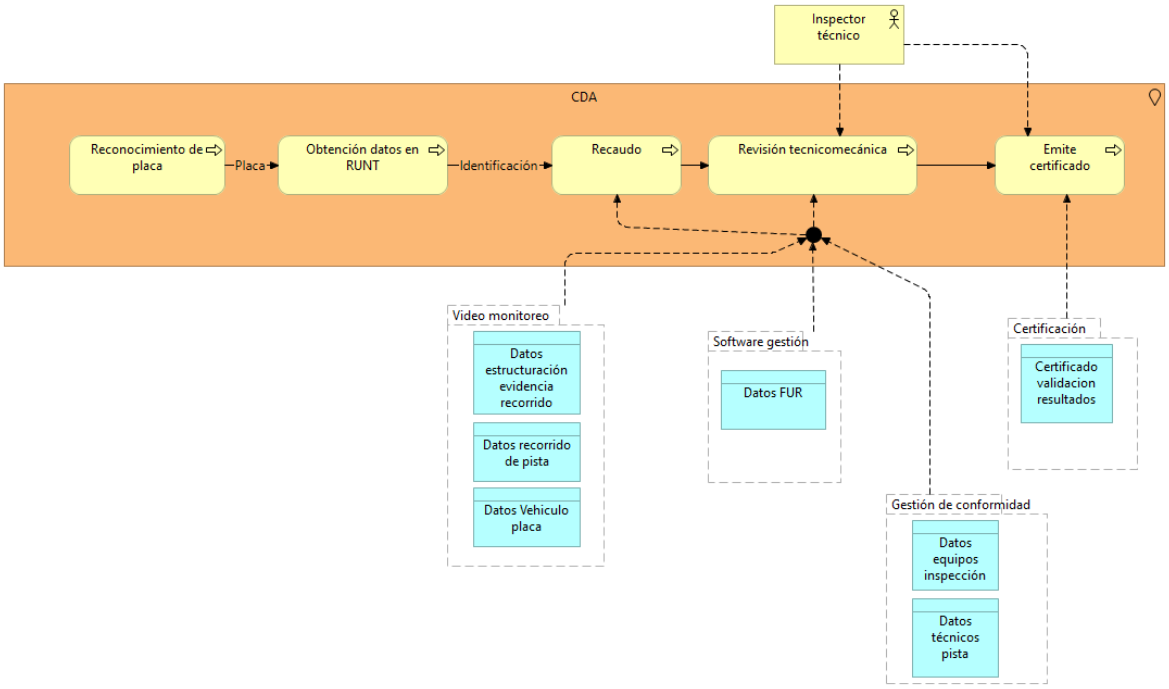
Ilustración 6 Proceso CDA Estado actual



Fuente: Elaboración propia Grow Data 2021

Iniciando el proceso (ver ilustración 6) para el CDA lo que se realiza es el registro y configuración del CDA en el SICOV, registrando el usuario de recepción que es la primera interacción con el cliente y el Director Técnico que soporta toda la operación del CDA.

Ilustración 7 Proceso CDA Estado actual

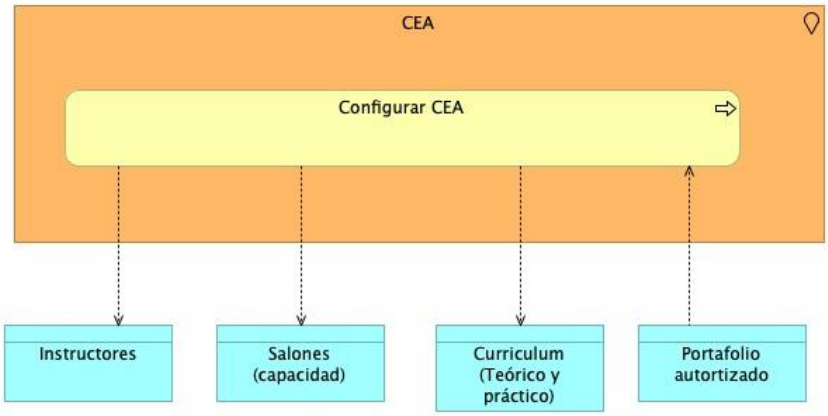


Fuente: Elaboración propia Grow Data 2021

Una vez cumplida esta etapa inicial de recepción del vehículo y verificación del PIN de recaudo se procede a realizar las pruebas en pista para los diferentes tipos de vehículo como se ve en la ilustración 7. Una vez validados los datos de las pruebas el Director Técnico verifica los resultados y si no hay inconvenientes se procede a expedir el certificado de emisión técnico mecánica y de gases.

PARA CEA

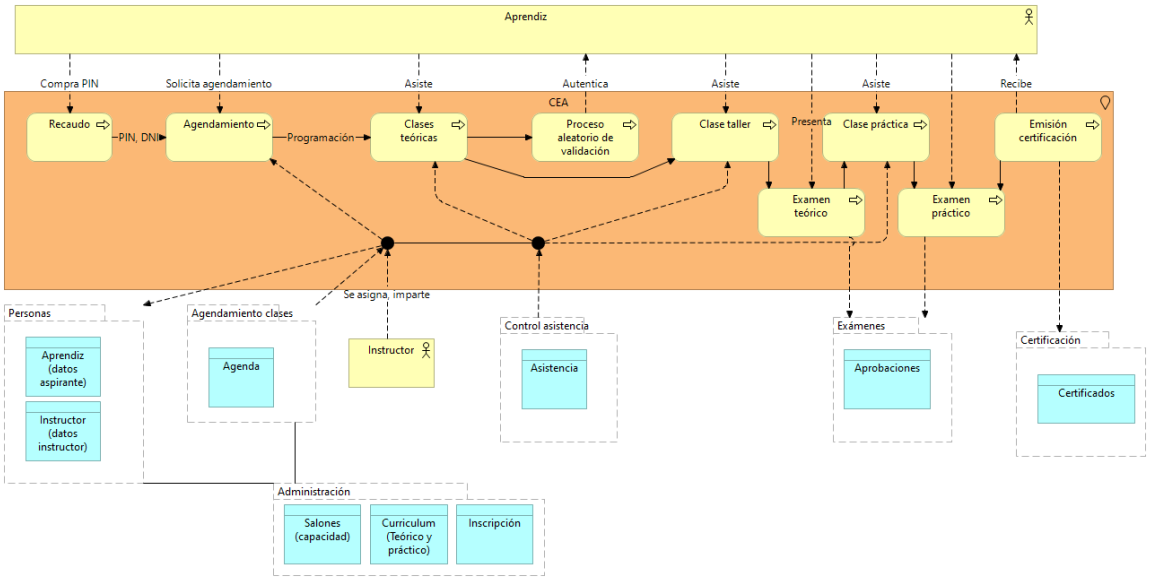
Ilustración 8 Proceso CEA Estado actual



Fuente: Elaboración propia Grow Data 2021

En la etapa inicial del proceso se procede a registrar el CEA en el SICOV, incluyendo instructores, salones y su capacidad de aprendices a atender, el currículo y contenidos de curso como se ve en la ilustración 8.

Ilustración 9 Proceso CEA Estado actual

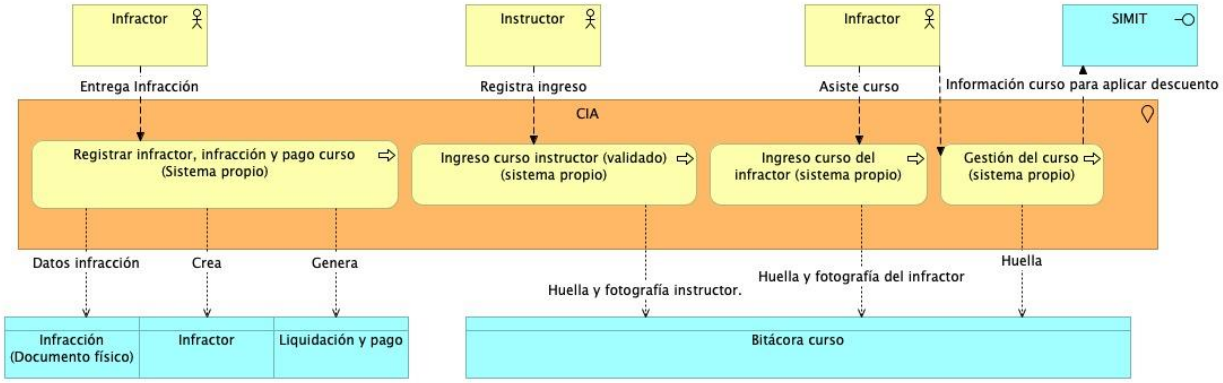


Fuente: Elaboración propia Grow Data 2021

Posteriormente, una vez se verifica el PIN de recaudo se procede con la prestación del servicio de formación en sus componentes teóricos y prácticos, finalizando con la aplicación de los exámenes y la emisión del certificado.

<u>PARA CIA</u>

Ilustración 10 Proceso CIA Estado actual

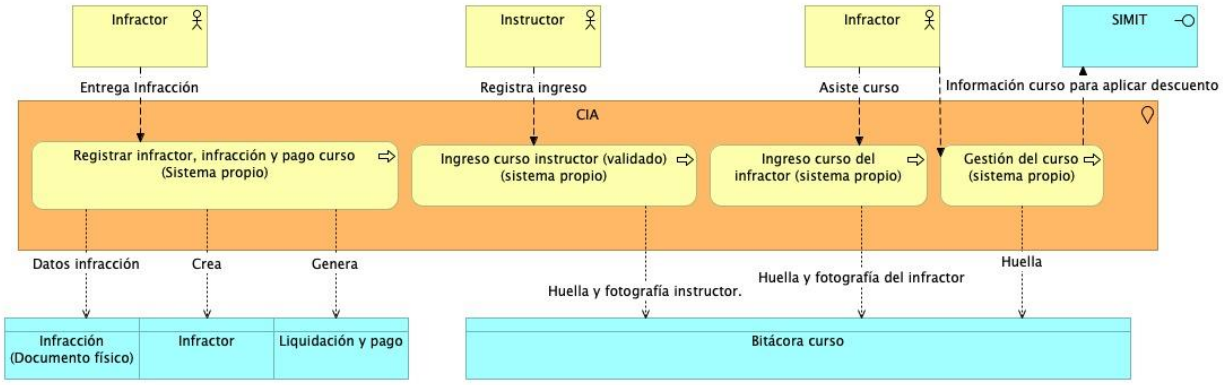


Fuente: Elaboración propia Grow Data 2021

El CIA no se encuentra en operación, lo expresado en este diagrama de proceso está definido por la legislación vigente para este tipo de OAT.

PARA CALE

Ilustración 11 Proceso CALE Estado actual



Fuente: Elaboración propia Grow Data 2021

El CALE no se encuentra en operación, lo expresado en este diagrama de proceso está definido por la legislación vigente para este tipo de OAT.

4.1.1.2 Servicios de negocio

Un servicio de negocio representa una vista externa de los servicios que una organización o unidad organizacional ofrece a sus clientes. Un servicio de negocio es realizado/soportado por procesos. Un servicio de negocio puede ser ejecutado por una función de negocio o directamente por un servicio de aplicación; sin embargo, lo correcto es modelarlo para que sea ejecutado desde un proceso de negocio. De ser necesario, se pueden descomponer los servicios de negocio en componentes más pequeños para darle mayor precisión a su flujo al igual que sucede con los procesos de negocio. Los servicios de negocio se registran en el catálogo de servicios de negocio con su nombre y descripción. A continuación, se lista los servicios de negocio identificados en la arquitectura actual:

SERVICIO	DESCRIPCIÓN
Análisis de la información de cliente	Este servicio permite el análisis de los clientes de la organización, así como la calificación de información de terceros en la relación con los clientes de la organización

SERVICIO	DESCRIPCIÓN
Gestión de relaciones con proveedores y asociados	Este servicio proporciona un marco para promover la colaboración efectiva entre una organización y sus proveedores y asociados, en particular los miembros de la cadena de suministro (por ejemplo, canal y alianzas, distribuidores, agentes, intermediarios y concesionarios), otros terceros que soportan las operaciones y la prestación de servicios a clientes de una organización; incluye la evaluación del desempeño de los proveedores y asociados, si es necesario
Retroalimentación del cliente	Este servicio se utiliza para recopilar, analizar y tramitar las observaciones y comentarios de los clientes de la Organización
Solicitud de Asistencia	Este servicio permite dar soporte al cliente en sitio o vía medios electrónicos (p.e. mesa de ayuda, servicios de asistencia remota, etc.)
Gestión de la Configuración	Este servicio controla los entornos de hardware y software, así como los documentos de una organización
Gestión de la Calidad	Este servicio determina el nivel en que un producto o servicio satisface los requisitos de los clientes.
Gestión de Riesgos	Este servicio apoya la identificación, análisis, evaluación y tratamiento de riesgos en lo que respecta a una meta, tarea, decisión a corto, mediano y largo plazo.
Digitalización de documentos y lectura OCR (reconocimiento óptico de caracteres)	Este servicio permite el soporte de la digitalización de documentos
Registro vinculación/asociación	Este servicio soporta la correlación entre los datos lógicos y conjuntos de información
Mapas / Referenciación Geoespacial / Sistemas de Información Geográfica / GPS	Este servicio proporciona la representación de la posición de la información a través de atributos como la elevación, latitud y longitud, y a través de coordenadas geográficas

SERVICIO	DESCRIPCIÓN
Intercambio de Datos	Este servicio soporta el intercambio de información entre múltiples sistemas o aplicaciones; incluye la verificación de los datos transmitidos que se recibieron inalterados
Auditoría	Este servicio soporta el examen y verificación de los registros para precisar el cumplimiento de los requisitos legales, éticos, contables y aplicables a la organización por entes externos o por entes internos.
Gestión Informática / Automatización	Este servicio soporta la identificación, actualización, distribución y sustitución de dispositivos físicos, incluyendo los servidores y equipos de sobremesa, que se utilizan para facilitar la prestación de productos y/o servicios, y actividades orientadas a procesos
Identificación y autenticación	Este servicio soporta la obtención de información sobre los usuarios que intentan iniciar sesión en un sistema o aplicación con fines de seguridad y la validación de los usuarios
Control de Acceso	Este servicio soporta la gestión de los permisos para iniciar sesión en una computadora, aplicación, servicio o red; incluye la gestión de usuarios y los privilegios de administración. Adicionalmente permite los controles de acceso físicos a las instalaciones de la organización
Respuesta a Incidentes	Este servicio proporciona respuesta activa y la remediación de un incidente de seguridad que ha permitido acceso no autorizado a un sistema de información
Protección de Virus	Este servicio proporciona el servicio antivirus para prevenir, detectar y remediar la infección de activos informáticos

SERVICIO	DESCRIPCIÓN
Correo electrónico (e-mail)	Este servicio soporta la transmisión de notas y mensajes a través de una red
Gestión de licencias	Este servicio soporta la adquisición, actualización y seguimiento de los contratos legales de uso y licenciamiento para los sistemas de software y aplicaciones
Sistemas de Control Remoto	Este servicio soporta el monitoreo, administración y uso de las aplicaciones y sistemas empresariales desde locaciones fuera del entorno del sistema.
Monitoreo de recursos del sistema	Este servicio soporta el equilibrio y la asignación de recursos de memoria, uso, espacio en disco y rendimiento de las computadoras y sus aplicaciones
Seguimiento de incidentes de TI	Este servicio soporta la recepción y seguimiento de las cuestiones y problemas notificados por los usuarios en el uso de los sistemas de TI, incluyendo las llamadas al servicio de asistencia (Help-Desk)

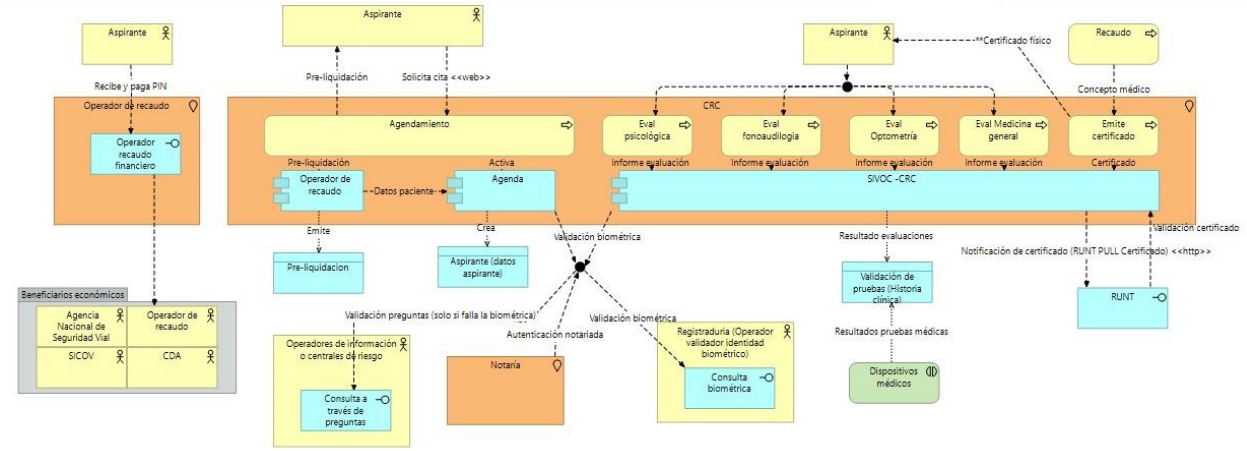
Tabla 1. Servicios de Negocio

Fuente: Elaboración propia Grow Data 2021

4.1.1.3 Matriz Procesos / Aplicaciones

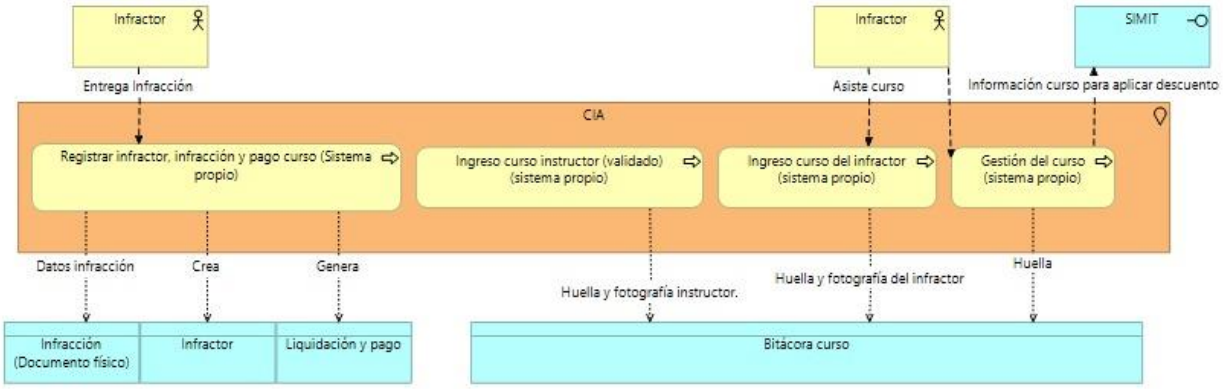
A continuación, se presenta la alineación de procesos versus aplicaciones en el estado actual, las descripciones de estas aplicaciones se encuentran en el Anexo "Catálogo de aplicativos SICOV". Adicionalmente, este tema se trata de manera extendida en el numeral 4.2.3 del presente documento.

Ilustración 12 - Procedimiento - Aplicaciones CRC



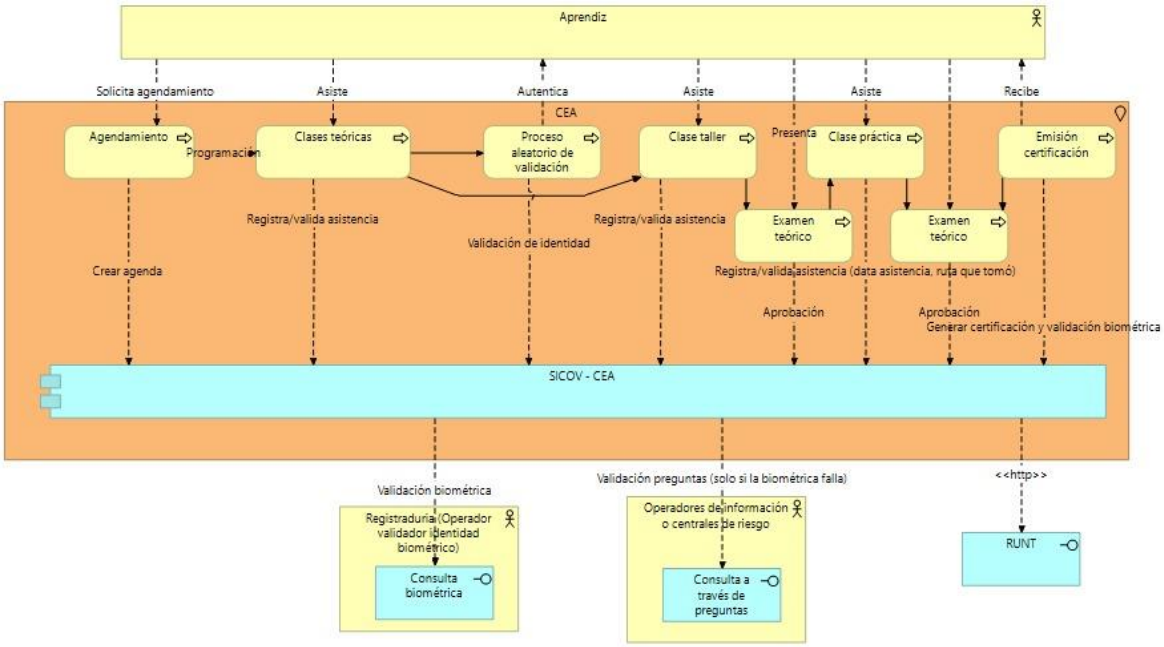
Fuente: Elaboración propia Grow Data 2021

Ilustración 13 - Procedimiento - Aplicaciones – CIA



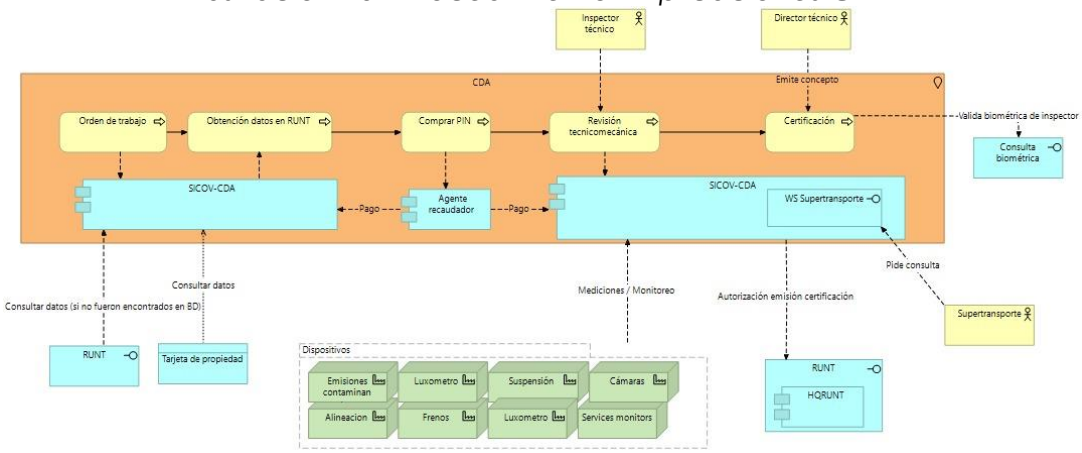
Fuente: Elaboración propia Grow Data 2021

Ilustración 14 - Procedimiento - Aplicaciones - CEA



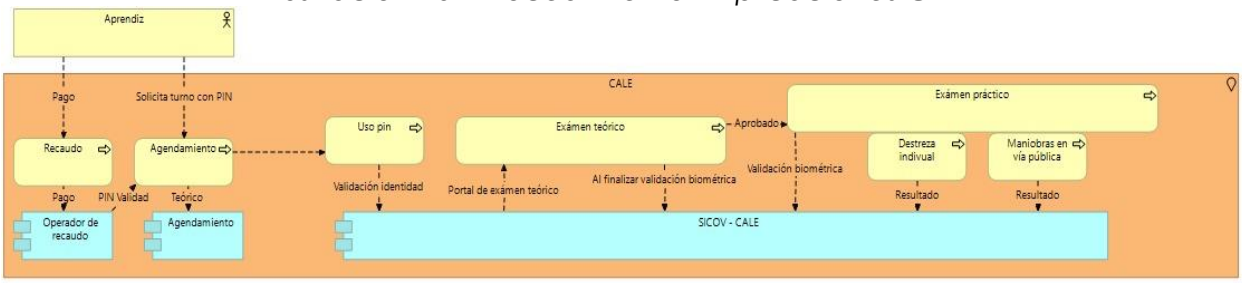
Fuente: Elaboración propia Grow Data 2021

Ilustración 15 - Procedimiento - Aplicaciones CDA



Fuente: Elaboración propia Grow Data 2021

Ilustración 16 - Procedimiento - Aplicaciones CALE



Fuente: Elaboración propia Grow Data 2021

4.1.1.4 Procesos / Entidades información

Este componente se detalla en la arquitectura de datos numeral 4.3.1.2.1. de este mismo documento.

4.2 Arquitectura de sistemas de información AS IS

La arquitectura de sistemas de información actual As-IS tiene como propósito, con base en la información recolectada en las actividades realizadas en la ejecución del contrato, establecer un modelo arquitectónico que represente adecuadamente los SICOV existentes. Lo anterior se justifica en el hecho de no contar con información primaria que permita determinar si los actuales homologados del SICOV realizaron algún ejercicio de arquitectura empresarial. El modelo arquitectónico podría ser usado como base para realizar un análisis de brecha con la arquitectura deseada TO-BE que se obtenga para soportar el nuevo modelo operativo que se produzca.
Observando los requerimientos establecidos en el anexo 1 del contrato 287 de 2021, el alcance de la arquitectura de sistemas de información incluye:

- Arquitectura conceptual (Blue print) de la arquitectura de sistemas de información actual con su respectivo análisis y descripción.
- Arquitectura solución actual con su respectivo análisis.
- Diagrama de interoperabilidad de los sistemas y/o aplicaciones actuales con su respectivo análisis y descripción.
- Catálogo de servicios de intercambio de información actual
- Catálogo de soluciones, sistemas y aplicativos actuales que conforman la solución actual que soporta la operación del actual SICOV

4.2.1 Arquitectura Conceptual (Blue Print)

La arquitectura conceptual tiene como propósito ilustrar con un nivel de abstracción alto (en forma de conceptos), la arquitectura de sistemas de información del SICOV, basándose en las soluciones encontradas en los homologados que operan actualmente

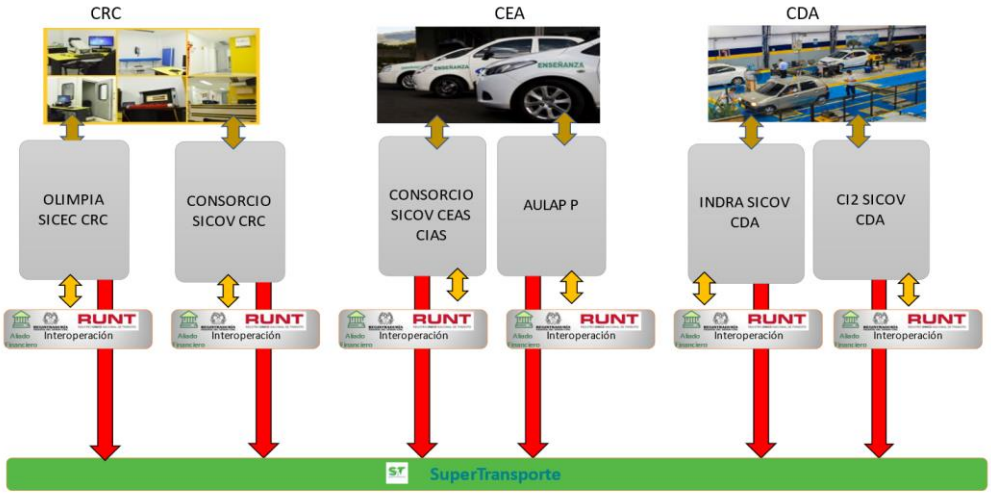


Ilustración 17 Arquitectura conceptual SICOV (AS IS)

Fuente: Elaboración propia Grow Data 2021

Se encuentran operando soluciones SICOV para tres tipos de OAT, los CRC, los CEA y los CDA. Para los CIA no se encuentran soluciones SICOV mientras que los CALE no han entrado en operación aun por lo tanto no existe SICOV.

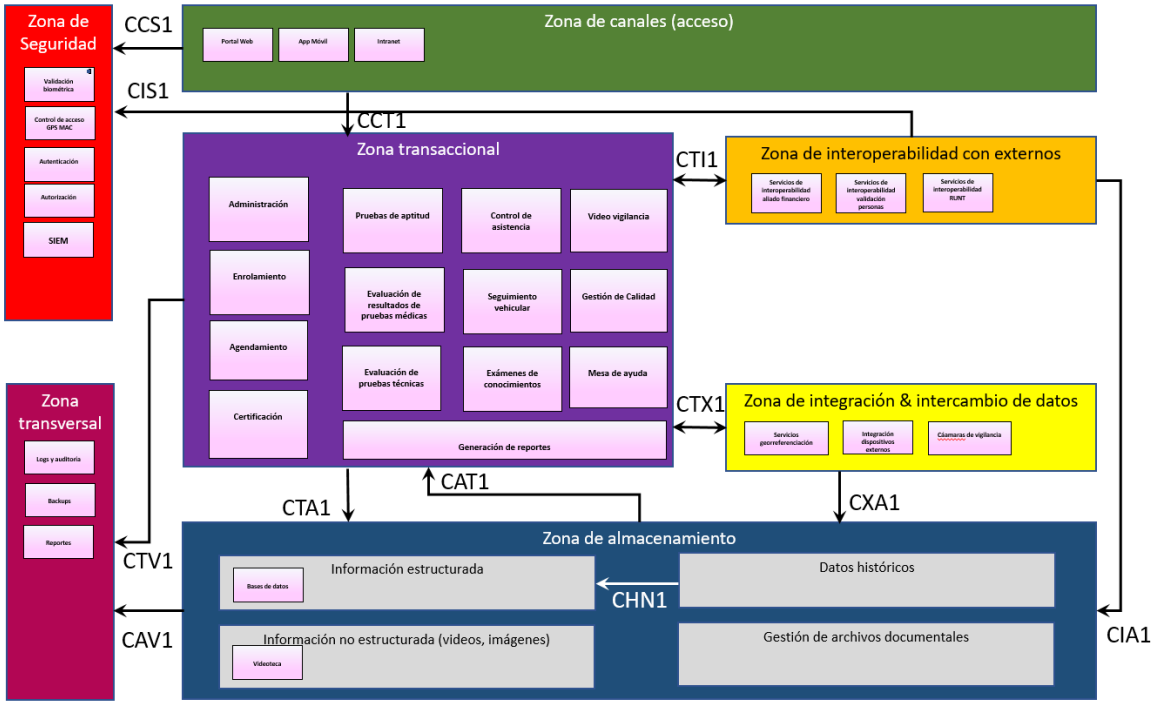
Con el propósito de describir y analizar la arquitectura del SICOV, se elaboró un diagrama con zonas y componentes que presenta los aspectos relevantes inferidos de las soluciones encontradas.

4.2.1.1 Diagrama zonas

.

Con base en la recomendación de MinTIC para estructurar y organizar la arquitectura de sistemas de información, a continuación, se presenta el mapa de zonas que ilustran la arquitectura actual de los sistemas de información del sistema SICOV.

Ilustración 18 Mapa de zonas SICOV (AS IS)



Fuente: MinTIC, Adaptado de la guía G.SIS.04 de Arquitectura de soluciones tecnológicas 2019

A continuación, se describen cada una de las zonas del diagrama.

4.2.1.1.1 Zona de seguridad

Zona encargada de servicios de autorización, autenticación, emisión y/o validación de certificados digitales y gestión de evidencia digital, que controla y centraliza el acceso a las demás funcionalidades.

- Validación biométrica que permitan confirmar la identidad de personas con base en el documento de identidad presentado y algún aspecto de su físico como las huellas digitales, las características faciales o algún otro aspecto posible como el iris.
- Controles de acceso basado en dispositivos físicos como la MAC del equipo o un GPS.
- Los componentes de autenticación o autorización de ingreso que permiten confirmar que una persona o servicio es quien dice, ser con base en elementos o condiciones previas como un password y con base en el resultado autorizar el ingreso al sistema.
- Los componentes de permitan detectar y responder a eventos concretos.
- Alarmas es un componente que permite la identificación y divulgación de situaciones asociadas a la operación de los OAT que pudieran representar un incumplimiento normativo sujeto a vigilancia y control.

4.2.1.1.2 Zona de canales (acceso)

Esta zona contiene los canales a través de los cuales los usuarios internos o externos acceden a las prestaciones funcionales del SICOV.

Los componentes que se incluyeron en esta zona de canales de acceso son los siguientes:

- Portales web que permiten acceder desde un explorador web a funcionalidades contenidas en componentes de otras zonas.
- Canales móviles que permiten acceder a servicios o funcionalidades que requieren de movilidad para el desarrollo de la funcionalidad (por ejemplo, el inicio de clases de enseñanza automovilística prácticas).
- Intranets que permiten acceder a componentes del SICOV mediante el uso de redes locales.

4.2.1.1.3 Zona transaccional

La zona transaccional contiene componentes que soportan las actividades operativas de los OAT y sobre los que se establecen acciones de inspección o vigilancia.

Agrupa los componentes de aplicaciones de software que soportan la inspección, la vigilancia y el control a la operación diaria de los OAT, así como las aplicaciones de apoyo a sus procesos misionales.

En esta zona se ubican los siguientes componentes.

- Administración es un componente que permite incorporar y actualizar la información específica de cada OAT que le permita hacer uso del SICOV. Incluye usuarios, equipos,
- Enrolamiento Pago servicio. Este componente permite, mediante la interoperación con los aliados financieros, la consulta y consumo de PIN para el pago del servicio solicitado al OAT.
- Enrolamiento. Es un componente que permite incorporar un usuario que requiere acceder al servicio que ofrece el OAT. Normalmente incluye el servicio de validación de identidad que permita verificar que el usuario es realmente quien dice ser.
- Agendamiento. Es un componente que soporta las actividades de estructuración de horarios de disponibilidad de espacios para ofrecer los servicios del OAT a los usuarios. También permiten las reservas de espacios disponibles por parte de un usuario. Deben de facilitar el control de capacidades del OAT establecidas en la autorización para operar.
- Gestión OAT. El componente de gestión del OAT permite que se registre en el SICOV el resultado de las actividades misionales de cada tipo de OAT. La forma de registro varia del registro directo a la recepción de los resultados enviados por un sistema de gestión especializado para el OAT como es el caso de los CDA.
- Certificación. El componente de certificación permite al OAT que, con base en la información registrada o recibida relativa a la prestación del servicio (reconocimiento, enseñanza o diagnóstico automotor), emita un certificado que refleje el resultado de las acciones realizadas, y lo incorpore en el RUNT para dar cumplimento a los aspectos normativos.
- Pruebas de aptitud es un componente que permite incorporar la información resultante de realizar una prueba de aptitud con base en un equipo de diagnóstico médico.
- Evaluación de resultados pruebas médicas permite que el profesional de la salud incorpore el resultado de la evaluación del aspirante.
- Evaluación de pruebas técnicas es un componente que permite evaluar en conjunto los resultados de las pruebas realizada al vehículo y registrar los resultados.
- Control de asistencia es un componente que permite verificar que las personas ingresaron o salieron de un salón de clase.
- Seguimiento vehicular permite registrar el tránsito de un vehículo por la pista de revisión
- Videovigilancia. El componente de videovigilancia permite mediante técnicas especializadas de almacenamiento y análisis de imágenes multimedia determinar si físicamente ocurrió alga especifico como el pasa de un vehículo automotor por la pista de revisión de un CDA.

- Mesa de ayuda, es el componente externo que permite a los usuarios del SICOV acceder a soporte cuando se les presentan dificultades en su operación.
- Gestión de calidad, es el componente externo que soporta al OAT para la implementación y mantenimiento de un sistema de gestión observando los aspectos normativos vigentes que los regulan.
- Generación de reportes es el componente que permite la obtención de información para la SuperTransporte, el operador homologado, el mismo OAT y algunos actores claves como la ANSV.

4.2.1.1.4 Zona de interoperabilidad con externos

Es el compendio de capacidades tecnológicas para la interoperabilidad a nivel digital con base en el intercambio de datos entre el sistema software del SICOV y sistemas de entidades del estado o de empresas privadas, con el objeto de dinamizar y optimizar los procesos operativos.

- Gestión de PIN con aliados financieros que
- Validación biométrica con RNEC u otros operadores alternos
- Servicios de interoperabilidad con el RUNT

4.2.1.1.5 Zona de integración e intercambio de datos

Es el compendio de capacidades tecnológicas para la integración a nivel digital del intercambio de datos entre el sistema software SICOV y otros sistemas.

- El envío de información a la SuperTransporte
- Recepción de datos de resultados obtenidos en dispositivos médicos en CRC
- Recepción de resultados de pruebas técnicas a vehículos con dispositivos especializados en CDA
- Recepción de información biométrica de dispositivos en CRC y CEA
- Recepción de imágenes de cámaras en CDA

4.2.1.1.6 Zona de almacenamiento (persistencia)

Zona que contiene los componentes para la gestión y almacenamiento de la información: datos transaccionales e históricos, información no estructurada y gestión documental.

4.2.1.1.6.1 Datos estructurados

Servicios de lectura/escritura de los datos transaccionales.

4.2.1.1.6.2 Datos históricos

Servicios de clasificación movimiento lectura/escritura de datos históricos.

4.2.1.1.6.3 Información no estructurada

Servicios de lectura/escritura de archivos multimedia como videos y fotografías.

4.2.1.1.6.4 Gestión de archivos

Funcionalidades para la administración completa del ciclo de vida de los documentos físicos o digitales entrantes y salientes. Esto incluye identificación, almacenamiento y archivo.

4.2.1.1.6.5 Zona transversal

En la zona transversal se incluyen componentes que agrupan servicios utilitarios de uso común.

- Gestión de logs y auditoría que registren información operativa
- Generador de reportes con base en la información persistida
- Gestión de copias de seguridad.

Tabla 2 Caracterización de conectores Arquitectura de Referencia

ID	Zona / Subzona Origen	Zona / Subzona Destino	Tipo de Conector	Descripción
CCS1	Canales	Seguridad	Unidireccional	Todo acceso por medio de los canales debe ser autenticado y autorizado a nivel de solución por los servicios de "seguridad".
CIS2	Interoperabilidad con externos	Seguridad	Unidireccional	Todo acceso a las capacidades de la solución por parte de terceros debe ser autenticado y autorizado a nivel de solución por los servicios de "seguridad".
CCT1	Canales	Transaccional	Unidireccional	A nivel de solución, para dar respuesta a una petición de un canal, se debe consumir servicios de la capa transaccional de la solución, en la que se encuentran las aplicaciones que soportan la operación día a día del OAT, por ejemplo, los exámenes médicos de un CRC.
CTS1	Transaccional	Seguridad	Unidireccional	Los servicios transaccionales podrían apoyarse en la zona de seguridad para consumir un servicio centralizado de autenticación a través de Directorio Activo, así como para la generación o validación de certificados

ID	Zona / Subzona Origen	Zona / Subzona Destino	Tipo de Conector	Descripción
				digitales, firma de documentos, cifrado de mensajes, entre otros.
CTI1	Transaccional	Interoperabilidad con externos	Bidireccional	Según la arquitectura de referencia propuesta toda aplicación transaccional que se encuentre en la zona con el mismo nombre, para consumir o exponer servicios hacia elementos externos de la solución, deberá utilizar un servicio que debe ser implementado en la zona "Interoperabilidad con externos". Este diseño implica que ningún elemento externo tiene acceso directo a la zona transaccional ni a ninguna otra zona diferente a la de interoperabilidad. Se establece un conector bidireccional para dar flexibilidad de exponer webservice o clientes para consumir servicios externos.
CTX1	Transaccional	Intercambio de datos	Unidireccional	Se establece un conector bidireccional para permitir a los componentes transaccionales recibir datos de dispositivos externos como gps, equipos médicos, equipos biométricos.

ID	Zona / Subzona Origen	Zona / Subzona Destino	Tipo de Conector	Descripción
CAT1	Almacenamiento	Transaccional	Unidireccional	El conector entre estas dos zonas tiene su origen en el grupo de almacenamiento, esto es útil para notificar cuando se ha llevado a cabo algún proceso sobre un archivo y se necesite informarlo a alguna aplicación. Por ejemplo, cuando se han procesado archivos de gran tamaño como videos o se ha realizado a nivel de base de datos, ETL o a nivel de sistema operativo, o cuando un proceso de migración de datos ha culminado.
CTA1	Transaccional	Almacenamiento	Unidireccional	Servicios síncronos o asíncronos que son provistos a la solución para la gestión centralizada de almacenamiento sobre uno o varios repositorios: base de datos de datacenter local, almacenamiento en la nube, sistema de archivos local, sistema de archivos de red, lectura/escritura de documentos en el gestor documental.
CTV1	Transaccional	Transversal	Unidireccional	Conector para habilitar el uso de los servicios provistos por la zona "transversal" por parte de la "transaccional". Un escenario de integración puede ser el de una aplicación

ID	Zona / Subzona Origen	Zona / Subzona Destino	Tipo de Conector	Descripción
				que solicite datos de logs sobre un rango de fechas.
CIA1	Interoperabilidad con externos	Almacenamiento / Gestión de Archivos	Unidireccional	Escenario de integración para el tipo de intercambio de información con grandes volúmenes de datos, en los que un webservice o cliente webservice recibirá o enviarán archivos, que deben ser registrados o leídos desde la subzona de "Gestión de Archivos".
CHN1	Almacenamiento / históricos	Almacenamiento / Datos transaccionales	Unidireccional	Este conector está orientado a los procesos de transferencia de datos para los proyectos analíticos a partir de datos transaccionales. El detalle de la operación y horario de cada mecanismo de integración debe ser definido en la arquitectura de solución.
CAV1	Almacenamiento	Transversal	Unidireccional	Conector para habilitar el uso de los servicios provistos por la zona "transversal" por parte del grupo de "Almacenamiento". Un escenario de integración puede ser el de un componente ETL que posterior a su finalización solicite la ejecución de una copia de seguridad.

Fuente: MinTIC, Adaptado de la G.SIS.04 Guía de Arquitectura de soluciones tecnológicas 2019

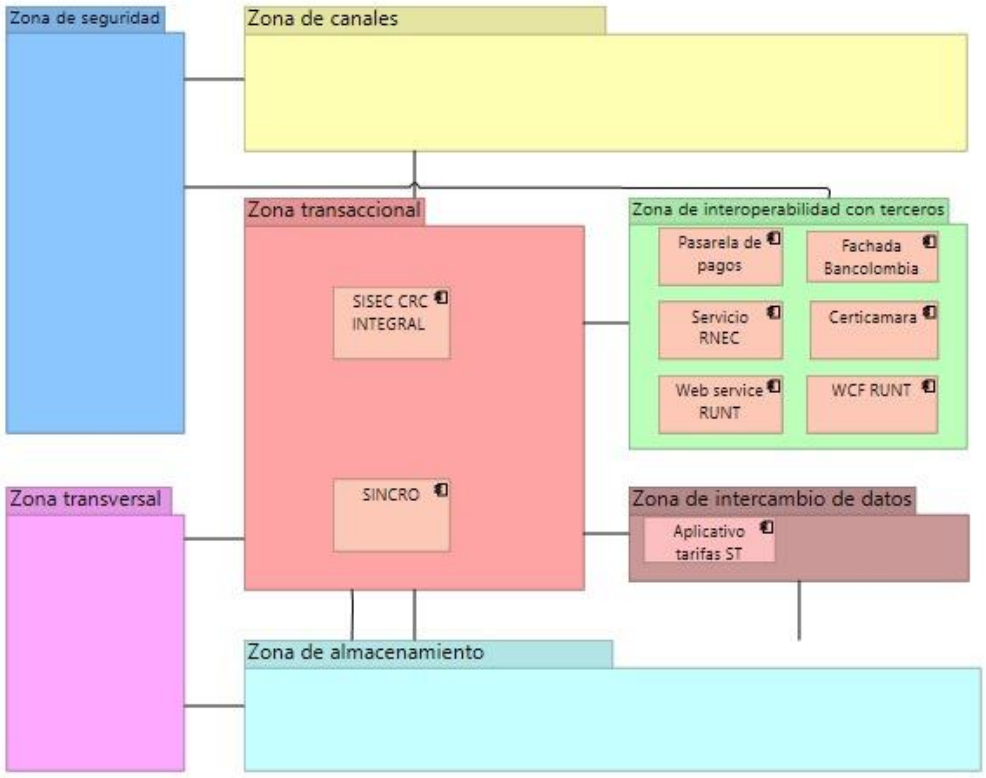
4.2.2 Arquitectura de solución actual (AS-IS)

Como se mencionó previamente, actualmente existen seis soluciones para el SICOV operando. Dos para cada tipo de OAT. En los siguientes numerales, se presentan los diagramas que representan la arquitectura de solución encontrada para cada tipo de OAT operando y que han organizado de acuerdo con las zonas presentadas previamente en la arquitectura conceptual.

4.2.2.1 Arquitectura de solución actual para los CRC

La arquitectura del SICOV para los CRC básicamente es una arquitectura multi capa. En la Ilustración 19 Arquitectura de solución CRC, se presenta una imagen del modelo construido con la herramienta ARCHI - Archimate Modelling y que se encuentra en el

Ilustración 19 Arquitectura de solución CRC



Fuente: Elaboración propia Grow Data 2021

repositorio del proyecto, correspondiente a los OAT de este tipo.

Las soluciones existentes son:

- SINCRO del homologado CONSORCIO SICOV-CRC
- SISEC CRC INTEGRAL del homologado OLIMPIA IT S.A.S.

SINCRO es una solución que está compuesta por los siguientes módulos cuyas funcionalidades específicas implementan los siguientes componentes:

- Agendamiento
  - Permite generar y registrar cita previa
  - Permite consultar y consumo PIN (Interoperación con Colpatria y Movired)
  - Permite pagos en efectivo en la red de Baloto y Punto Pago
  - Permita registrar datos del aspirante
- Enrolamiento
  - Permite realizar la validación de identidad por huellas ante la RNEC por interoperabilidad a través del operador Certicamara
  - Si falla permite método alterno con dactiloscopista
  - Permite escanear el documento del solicitante
  - Permite captura de foto y firma del aspirante
- Pruebas de aptitud
  - Permite realizar la validación de identidad por huellas ante la RNEC al aspirante y el evaluador
  - Permite realizar exámenes de aptitud (optometría, fonoaudiología o psicología) apoyado en integración cos dispositivos médicos externos
  - Integra sus propios equipos médicos particulares a su solución
- Evaluación de resultados pruebas médicas
  - Permite al médico general consolidar resultados de las pruebas de aptitud
- Certificación
  - Permite registro del examen médico
  - Permite registro FUPA en el RUNT vía interoperabilidad
  - Permite generar e imprimir el certificado de aptitud
- Dispone de servicios de georreferenciación por GPS
- Dispone de servicios de backup de resultados con persistencia de al menos un año
- Tienen una capa de presentación web

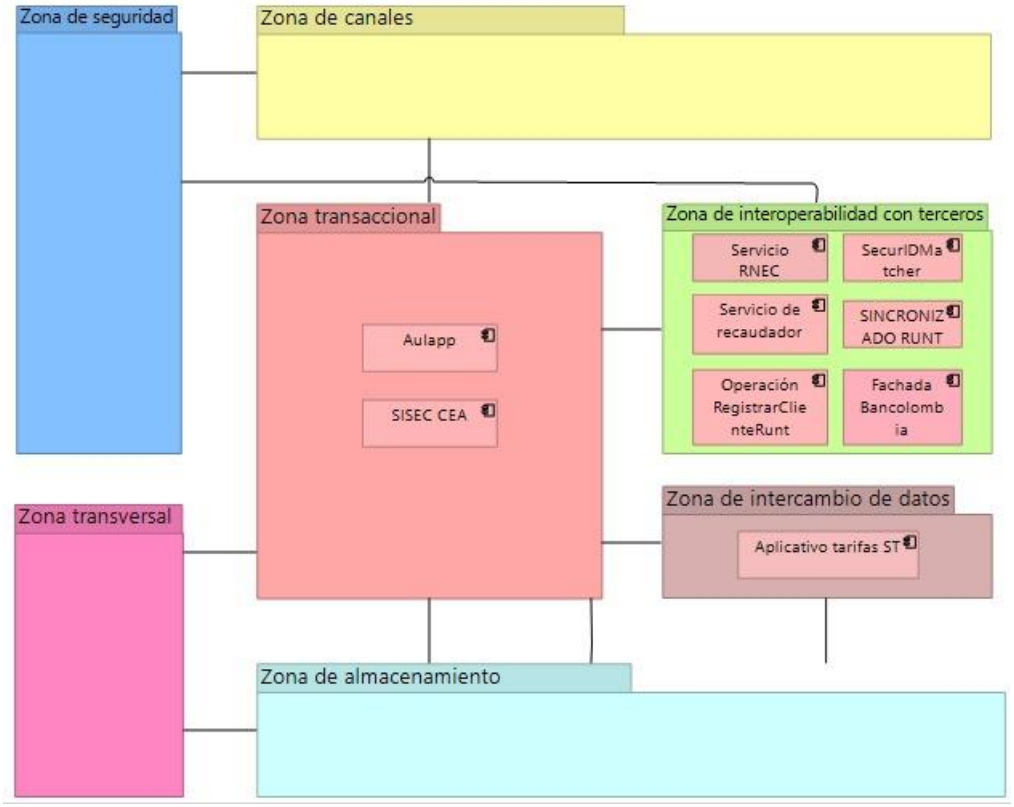
SICEC-CRC INTEGRAL es una solución que está compuesta por los siguientes módulos cuyas funcionalidades específicas implementan los siguientes componentes:

- Agendamiento
  - Permite generar y registrar cita previa
  - Permite consultar y consumo PIN (Interoperación con Colpatria y Bancolombia)
  - Permita registrar datos del aspirante
- Enrolamiento
  - Permite realizar la validación de identidad por huellas ante la RNEC por interoperabilidad a través del el mismo que es operador autorizado por RNEC
  - Permite escanear el documento del solicitante
  - Permite captura de foto y firma del aspirante
- Pruebas de aptitud
  - Permite realizar la validación de identidad por huellas ante la RNEC al aspirante y el evaluador
  - Permite realizar exámenes de aptitud (optometría, fonoaudiología o psicología) apoyado en integración cos dispositivos médicos externos
  - Integra sus propios equipos médicos particulares a su solución
- Evaluación de resultados pruebas médicas
  - Permite al médico general consolidar resultados de las pruebas de aptitud
- Certificación
  - Permite registro del examen médico
  - Permite registro FUPA en el RUNT vía interoperabilidad
  - Permite generar e imprimir el certificado de aptitud
- Dispone de servicios de georreferenciación por GPS
- Dispone de servicios de backup de resultados con persistencia de al menos un año
- Tienen una capa de presentación web

4.2.2.2 Arquitectura de solución actual para los CEA

La arquitectura del SICOV para los CEA básicamente es una arquitectura multi capa. En la Ilustración 20 Arquitectura de solución CEA, se aprecia una imagen del modelo construido en el repositorio de la herramienta ARCHI - Archimate Modelling del proyecto,

Ilustración 20 Arquitectura de solución CEA



Fuente: Elaboración propia Grow Data 2021

correspondiente a los OAT de este tipo.

Las soluciones existentes son:

- AULAPP del homologado CONSORCIO SISTEMA INTEGRADO DE GESTION Y SEGURIDAD PARA CEAS Y CIAS
- SISEC CEA INTEGRAL del homologado OLIMPIA IT S.A.S.

SICEC-CEA INTEGRAL es una solución que está compuesta por los siguientes módulos cuyas funcionalidades específicas implementan los siguientes componentes:

- Agendamiento
  - Permite generar y registrar cita previa
  - Permite consultar y consumo PIN (Interoperación con Colpatria y Bancolombia)
  - Permite pago en dos cuotas del valor de la matricula (PIN)
  - Permita registrar datos del aprendiz
- Enrolamiento
  - Permite realizar la validación de identidad por huellas ante la RNEC por interoperabilidad a través del el mismo que es operador autorizado por RNEC
  - Permite escanear el documento del aprendiz
  - Permite captura de foto y firma del aprendiz
- Control de asistencia clases teóricas
  - Permite registrar entrada y salida del salón de clase mediante validación biométrica tanto de instructor como de aprendiz. Algunas veces contra la RNEC por interoperabilidad.
  - Permite registrar todas las clases recibidas por los aprendices en la plataforma del RUNT
- Exámenes teóricos
  - Permite iniciar, presentar y terminar examen teórico
  - Permite validar por biometría a veces ante la RNEC, la identidad del alumno que presenta el examen
  - Permite evaluar los resultados del examen
- Control de asistencia clases prácticas
  - Permite registrar abordaje y desabordaje del vehículo automotor para iniciar y terminar las clases prácticas tanto de instructor como de aprendiz, mediante acceso al SICOV por app mediante canal móvil
  - Permite validar la identidad del aprendiz o del instructor mediante huella patrón de cuatro dedos (4F) o foto
  - Permite validar vehículo asignado mediante lectura módulo NFC
  - Permite reportar el recorrido a través de ubicaciones GPS
  - Permite registrar todas las clases recibidas por los aprendices en la plataforma del RUNT
- Exámenes prácticos
  - Permite abordar vehículo, presentar examen práctico y desabordar
  - Permite validar por biometría a veces ante la RNEC, la identidad del alumno que presenta el examen práctico
  - Permite registrar los resultados del examen

- Certificación
  - Permite registro en el RUNT vía interoperabilidad
  - Permite generar e imprimir el certificado de conducción
- Dispone de servicios de georreferenciación por GPS
- Dispone de servicios de backup de resultados con persistencia de al menos un año
- Tienen una capa de presentación web

AULAPP es una solución que está compuesta por los siguientes módulos cuyas funcionalidades específicas implementan los siguientes componentes:

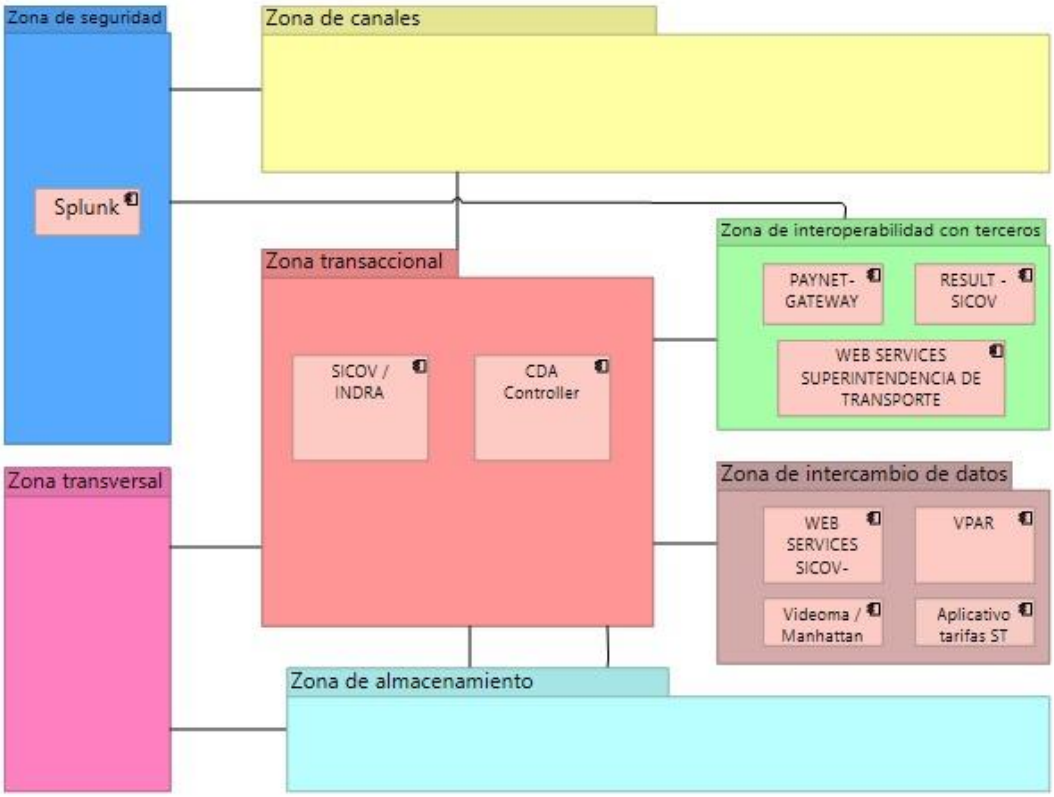
- Agendamiento
  - Permite generar y registrar cita previa
  - Permite consultar y consumo PIN (Interoperación con Colpatria)
  - Permite pago en dos cuotas del valor de la matricula (PIN)
  - Permita registrar datos del aprendiz
- Enrolamiento
  - Permite realizar la validación de identidad por huellas ante la RNEC por interoperabilidad a través del el mismo que es operador autorizado por RNEC
  - Permite escanear el documento del aprendiz
  - Permite captura de foto y firma del aprendiz
- Control de asistencia clases teóricas
  - Permite registrar entrada y salida del salón de clase mediante validación biométrica tanto de instructor como de aprendiz. Algunas veces contra la RNEC por interoperabilidad.
  - Permite registrar todas las clases recibidas por los aprendices en la plataforma del RUNT
- Exámenes teóricos
  - Permite iniciar, presentar y terminar examen teórico
  - Permite validar por biometría a veces ante la RNEC, la identidad del alumno que presenta el examen
  - Permite evaluar los resultados del examen
- Control de asistencia clases prácticas
  - Permite registrar abordaje y desabordaje del vehículo automotor para iniciar y terminar las clases prácticas tanto de instructor como de aprendiz, mediante acceso al SICOV por app mediante canal móvil
  - Permite validar la identidad del aprendiz o del instructor mediante huella patrón de cuatro dedos (4F) o foto
  - Permite validar vehículo asignado mediante lectura módulo NFC

  - Permite reportar el recorrido a través de ubicaciones GPS
  - Permite registrar todas las clases recibidas por los aprendices en la plataforma del RUNT
- Exámenes prácticos
  - Permite abordar vehículo, presentar examen práctico y desabordar
  - Permite validar por biometría a veces ante la RNEC, la identidad del alumno que presenta el examen práctico
  - Permite registrar los resultados del examen
- Certificación
  - Permite registro en el RUNT vía interoperabilidad
  - Permite generar e imprimir el certificado de conducción
- Dispone de servicios de georreferenciación por GPS
- Dispone de servicios de backup de resultados con persistencia de al menos un año
- Tienen una capa de presentación web

4.2.2.3 Arquitectura de solución para los CDA

LA solución de los SICOV para los CDA es muy diferente a la solución de los CRC y de los CEA lo cual es lógico teniendo en cuenta que el objeto a evaluar es un vehículo automotor y no un ser humano. La arquitectura de los dos SICOV CDA es una

Ilustración 21 Arquitectura de solución CDA



Fuente: Elaboración propia Grow Data 2021

arquitectura basada en eventos. En la Ilustración 21 Arquitectura de solución CDA, se aprecia una imagen del modelo construido en el repositorio de la herramienta ARCHI - Archimate Modelling del proyecto, correspondiente a los OAT de este tipo.

Las soluciones existentes son:

- SICOV CDA del homologado COMPAÑÍA INTERNACIONAL DE INTEGRACIÓN S.A. – CI2 S.A.-

- SICOV CDA del homologado INDRA SISTEMAS S.A. SUCURSAL COLOMBIA

Un aspecto clave de las dos soluciones, es que el control fundamental se centra en garantizar que los vehículos automotores recorren la pista de revisión normalmente.

SICOV-INDRA es una solución que está compuesta por los siguientes módulos cuyas funcionalidades específicas implementan los siguientes componentes:

- Seguimiento vehicular
  - Permite registrar ingreso a pista del vehículo e identificar la placa mediante VPAR
  - Permite registrar los datos del vehículo que inicia la revisión y reportarlo al RUNT. Opcional consultar datos del vehículo en el RUNT
  - Permite identificar la salida de la pista del vehículo
- Video vigilancia
  - Permite registrar en video el paso del vehículo por cada estación de revisión VPAR
  - Permite extractar y componer los videos de cada cámara que muestran el paso del vehículo por la pista.
- Evaluación de pruebas técnicas
  - El sistema de gestión propio del CDA permite mediante integración obtener los resultados de los dispositivos técnicos
  - Permite mediante integración con el sistema de gestión propio del CDA obtener los datos del formato uniforme de resultados (FUR)
- Certificación
  - Permite registro FUR en el RUNT vía interoperabilidad
  - Permite generar e imprimir el certificado de RTMYEC
- Dispone de software de monitoreo de eventos
- Permite el envío de información a la SuperTransporte correspondiente a la revisión del vehículo. En algunos casos se realiza a través de adjuntos enviados por correo electrónico.
- Dispone de servicios de georreferenciación por GPS
- Dispone de servicios de backup de resultados con persistencia de al menos un año
- Tienen una capa de presentación web

SICOV-CI2 es una solución que está compuesta por los siguientes módulos cuyas funcionalidades específicas implementan los siguientes componentes:

- Seguimiento vehicular
  - Permite registrar ingreso a pista del vehículo e identificar la placa mediante VIDEOMA
  - Permite registrar los datos del vehículo que inicia la revisión y reportarlo al RUNT. Opcional consultar datos del vehículo en el RUNT
  - Permite identificar la salida de la pista del vehículo
- Video vigilancia
  - Permite registrar en video el paso del vehículo por cada estación de revisión Manhatan
  - Permite extractar y componer los videos de cada cámara que muestran el paso del vehículo por la pista.
- Evaluación de pruebas técnicas
  - El sistema de gestión propio del CDA permite mediante integración obtener los resultados de los dispositivos técnicos
  - Permite mediante integración con el sistema de gestión propio del CDA obtener los datos del formato uniforme de resultados (FUR)
- Certificación
  - Permite registro FUR en el RUNT vía interoperabilidad
  - Permite generar e imprimir el certificado de RTMYEC
- Dispone de software de monitoreo de eventos SPLUNK
- Permite el envío de información a la SuperTransporte correspondiente a la revisión del vehículo.
- Dispone de servicios de georreferenciación por GPS
- Dispone de servicios de backup de resultados con persistencia de al menos un año
- Tienen una capa de presentación web

Las dos soluciones incluyen componente de correlaciona miento de eventos que ayuda a identificar posibles patrones de comportamiento no estándar en los CDA.

4.2.3 Catálogo de soluciones, sistemas y aplicativos (SICOV)

Las soluciones, sistema y aplicativos en este contexto de descripción de la arquitectura de solución actual se definen de la siguiente forma:

- Una solución corresponde a algún aplicativo encontrado operando en alguna implementación especifica de cualquier operador homologado del SICOV. Esto denota que fue la solución que implemento el homologado.

- En cuanto sistema, en este contexto especifico se refiere al conjunto de aplicativos implementados por los homologados para dar solución integral a las necesidades y los requerimientos específicos del SICOV.

- Finalmente, los aplicativos corresponden también a los componentes específicos encontrados en las soluciones de los homologados para cubrir aspectos concretos del SICOV.

En las siguientes secciones se presentan los catálogos de aplicativos para los OAT que se encuentran operando. Los aplicativos presentados en los catálogos, corresponden al nivel superior de acuerdo con la abstracción lograda del procesamiento y análisis de la información disponible.
Dichos catálogos son la base para la alineación con los demás dominios de arquitectura. Con base en ellos se elaboran los siguientes artefactos de arquitectura:

- Procesos – aplicaciones (Dominio de negocio)
- Aplicaciones – dominios de información (Dominio de datos)
- Diagrama de despliegue de infraestructura (Dominio de infraestructura)

4.2.3.1 Catálogo de aplicativos de los CRC

Los aplicativos que conforma la solución SICOV para los CRC agrupan las funcionalidades básicas de apoyo a la gestión administrativa del CRC, así como las funcionalidades de gestión de la operación misional.

Las dos soluciones existentes corresponden a desarrollos propios del homologado. Las soluciones siguen una arquitectura por capas. Las dos soluciones a su vez interoperan con la RNEC y el RUNT de forma similar a través de los servicios expuestos en sus sistemas por esas Entidades. La interoperación con los aliados financieros es similar en ambos casos.

El catalogó de aplicativos se puede apreciar en el anexo "Arq.Sist.Inf Catálogo de aplicativos SICOV" y contiene la aplicación central que incluye los aspectos mencionados en la arquitectura de solución. Se incluye en el catálogo elementos complementarios relacionados directamente con la interoperabilidad con otros sistemas como el RUNT o los aliados financieros Colpatria y Bancolombia.

Es preciso aclarar que la solución integral de los CRC, incluye sistemas complementarios como por ejemplo la mesa de ayuda, que no hacen parte integral del SICOV, pero que son exigidos por norma para permitir la operación del SICOV

4.2.3.2 Catálogo de aplicativos de los CEA

Los aplicativos que conforma la solución SICOV para los CEA agrupan las funcionalidades básicas de apoya a la gestión administrativa del CEA, así como las funcionalidades de gestión de la operación misional.

Las dos soluciones existentes corresponden a desarrollos propios del homologado. Las soluciones siguen una arquitectura por capas. Las dos soluciones a su vez interoperan con la RNEC y el RUNT de forma similar a través de los servicios expuestos en sus sistemas por esas Entidades. La interoperación con los aliados financieros es similar en ambos casos.

El catalogó de aplicativos se puede apreciar en el anexo "Arq.Sist.Inf Catálogo de aplicativos SICOV" y contiene la aplicación central que incluye los aspectos mencionados en la arquitectura de solución. Se incluye en el catálogo elementos complementarios relacionados directamente con la interoperabilidad con otros sistemas como el RUNT o los aliados financieros Colpatria y Bancolombia.

También es preciso aclarar que la solución integral de los CEA incluye sistemas complementarios como por ejemplo la mesa de ayuda, que no hacen parte integral del SICOV, pero que son exigidos por norma para permitir la operación del SICOV

4.2.3.3 Catálogo de aplicativos de los CDA

En el caso del catálogo de aplicativos del SICOV para CDA, este contiene sistemas especializados para la implementación del SICOV como los sistemas de gestión de videos, los componentes de reconocimiento de caracteres para la identificación de la matrícula del vehículo automotor y el sistema de correlacionamiento de eventos. Estos se complementan con las funcionalidades que dan acceso a los servicios del RUNT para el reporte del FUR y el registro del certificado de revisión RTMYEC.

4.2.4 Catálogo de servicios de intercambio de información

En el anexo "Arq.Sist.Inf Catálogo de servicios de intercambio de información" se presentan los diferentes catálogos de servicios de intercambio de información.

Se destaca que los servicios de intercambios de información se describen en términos de las entidades que intervienen en el intercambio, el sistema especifico de quien pública y la función que cumple.

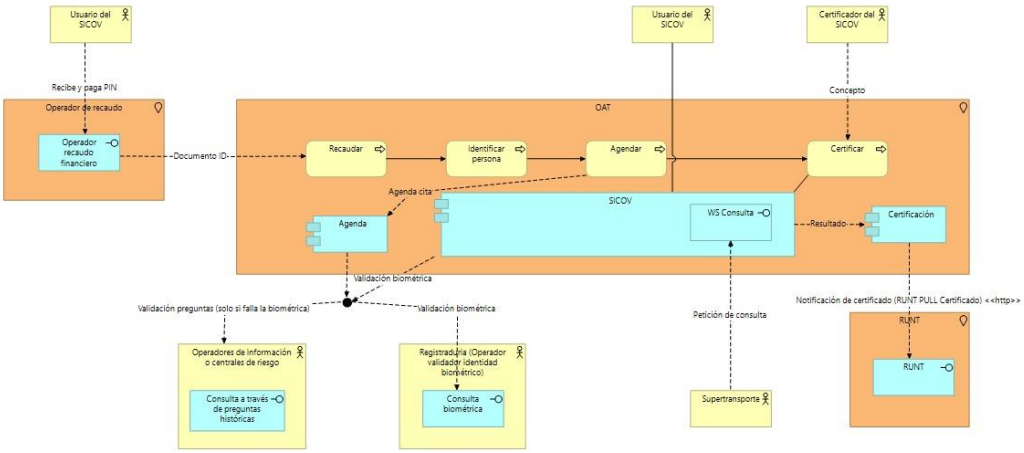
- Nombre

En las siguientes secciones se presentan los catálogos de servicios de intercambio de información para cada uno de los OAT que se encuentran operando. Dichos catálogos son la base para la elaboración del diagrama de interoperabilidad del SICOV que se presenta en el numeral 4.2.5 de este documento.

4.2.5 Diagrama actual (AS-IS) de interoperabilidad de los sistemas o aplicaciones

Con base en los catálogos de servicios de intercambio de información, presentados en la sección anterior, se modeló en la herramienta ARCHI - Archimate Modelling el diagrama de interoperabilidad que se presenta en la Ilustración 22.

Ilustración 22 Diagrama de interoperabilidad del SICOV



Fuente: Elaboración propia Grow Data 2021

En el diagrama se puede apreciar que, en la actualidad, el SICOV interopera a través de servicios web con las siguientes entidades o actores públicos y privados:

4.2.5.1 SuperTransporte.

El intercambio de información con la SuperTransporte está centrado en el envío de información desde los operadores homologados hacia la Entidad relativa a aspectos relacionados con datos de la operación de los OAT. El principal intercambio de información se da entre los CDA y la SuperTransporte e incluye la información de las revisiones realizadas a los vehículos, algunas veces por correo electrónico.

En cuanto a la interoperabilidad con actores privados externos al SICOV se encuentran los siguientes.

4.2.5.2 Aliados financieros.

EL SICOV en general interopera con los diferentes aliados financieros que han implementado soluciones que se ajustan a los requerimientos establecidos. Estos actores son Colpatria, BanColombia, quienes ofrecen diferentes medios de pago que incluyen hasta el pago en efectivo en redes como Baloto. La interoperabilidad permite que el SICOV con base en el documento de identidad del usuario (aspirante, conductor) y/o placa del vehículo a inspeccionar consulte si tiene disponible un PIN para usar como medio de pago del servicio solicitado. En caso de respuesta afirmativa, puede solicitar el uso del PIN, mediante la acción de quemado, es decir el uso del PIN para pagar por el servicio solicitado por el usuario en el OAT. Una vez realizada dicha acción el PIN no podrá ser utilizado nuevamente por ningún OAT.

4.2.5.3 Registraduría Nacional del Estado Civil (RNEC).

EL SICOV interopera con la RNEC en los puntos de control de los OAT donde se requiere de validación biométrica basada en las huellas dactilares. Estos puntos se refieren a los profesionales de la salud en los CRC, a los usuarios o solicitante del servicio bien sea en los CRC o en los CEA y a los instructores de los CEA, de acuerdo con los requerimientos establecidos en la normativa vigente. Esta validación es clave para que se puede garantizar que los actores son realmente quienes dicen ser. Como se mencionó, esto aplica para los usuarios, que son los sujetos de evaluación de aptitud, o del proceso de enseñanza de conducción, o para los demás actores del OAT que actúan como

profesionales evaluadores, instructores para impartir clases teóricas o prácticas, o responsables de generar los certificados en los CRC y los CEA. Esta interoperación no aplica para los CDA puesto que en ellos se valida la identidad del director técnico ante el SICOV.

4.2.5.4 Registro Único Nacional de Tránsito (RUNT).

EL SICOV en general interopera con la aplicación del RUNT, en el que, por norma, se deben reflejar los certificados generados por todos los OAT que operan en el país. Esta acción se realiza mediante el consumo de un web service publicado para tal fin. Dependiendo del tipo de OAT la información es diferente. El certificado emitido por el OAT es válido una vez quede registrado en el RUNT.

En algunos casos se presenta interoperación de los CDA con el RUNT para consultar las características del vehículo automotor que se va a revisar como medida adicional de control a la verificación de características contra la tarjeta de propiedad del vehículo.

4.3 Arquitectura de datos

4.3.1 Arquitectura Conceptual

La Arquitectura de Datos del sistema SICOV se describe mediante una colección integrada de documentos maestros de diseño en diferentes niveles de abstracción, incluyendo estándares (ISO/IEC/IEEE 42010:2011 y DAMA) que rigen cómo se recopilan, almacenan, organizan, usan y eliminan los datos.

También se clasifica por descripciones de todos los contenedores y rutas que toman los datos a través del sistema SICOV. Los artefactos de la Arquitectura de Datos incluyen especificaciones utilizadas para describir el estado actual, definir requerimientos de datos, guiar la integración de datos y controlar los activos de datos tal como se describe en una estrategia de datos.

Para efectos del sistema SICOV y alineados al Marco de referencia de Arquitectura de MinTIC y al DAMA se proponen los siguientes artefactos para describir la arquitectura de datos como catálogos, matrices y diagramas que se abordan en los siguientes apartados:

4.3.1.1 Catálogo de Datos

El catálogo de datos es un artefacto que se define como un inventario organizado de los activos de datos de una organización. Utiliza metadatos para ayudar a las organizaciones a administrar sus datos.

También brinda las herramientas para ayudar a los profesionales de datos a recopilar, organizar acceder, enriquecer y explotar metadatos para respaldar la detección y la gobernanza de los datos.

Para el sistema SICOV y como parte de los artefactos que conforman la arquitectura de datos se abordaron los catálogos de dominios de información y los catálogos de entidades de datos:

4.3.1.1.1 Dominios de información

Para un mejor entendimiento del catálogo de dominios de información se crea una guía para la identificación de cada atributo descrito en el catálogo.

Tabla 3. Guía catálogo dominios de información

ID	Identificador único del Dominio de información.
Nombre	Nombre del Dominio de información.
Descripción	Descripción del Dominio de información.
Fecha Identificación	Fecha de la identificación del domino de datos en el momento de la recolección de datos.
Fuente	Fuente de la identificación de los dominios de datos en el momento de la recolección de datos.

Fuente: Elaboración propia Grow Data 2021

El catálogo de dominio lista y contextualiza los dominios de información para cada uno de los diferentes Organismos de Apoyo al Tránsito – OAT.

- CRC se identifican 10 dominios de información.
- CEA se identifican 10 dominios de información.
- CIA se identifican 9 dominios de información.
- CALE se identifican 6 dominios de información.
- CDA se identifican 9 dominios de información.

Se referencia el Anexo Arq.Datos_Catálogo_Dominios_AsIs.xlsx a este documento. De igual forma el catálogo completo se encuentra en la herramienta ARCHI - Archimate Modelling.

4.3.1.1.2 Entidades de datos

Para un mejor entendimiento del catálogo de entidades de datos se crea una guía para la identificación de cada atributo descrito en el catálogo.

Tabla 4. Guía catálogo entidades de datos

ID	Identificador único de la entidad de datos.
Nombre	Nombre de la entidad de datos.
Descripción	Descripción de la entidad de datos.
Nombre Dominio	Identificación del dominio de datos al cual corresponde la entidad de datos descrita.
Fuente	Origen de la identificación de la entidad de datos recibida para la elaboración del catálogo.
Fecha Identificación	Fecha de la identificación de la entidad de datos en el momento de la recolección de datos.
Fecha de Actualización	Fecha de actualización de la entidad de datos.
Fecha de Retiro	Fecha de retiro de la entidad de datos.

Fuente: Elaboración propia Grow Data 2021

El catálogo de entidades de datos lista y contextualiza las entidades de datos de los diferentes Organismos de Apoyo al Tránsito – OAT; se describe el contenido de cada una de las hojas del catálogo.

- Ent_D_CRC, se encuentran 29 entidades de datos identificadas en el CRC.
- Ent_D_CEA, se encuentran 26 entidades de datos identificadas en el CEA.
- Ent_D_CIA, se encuentran 20 entidades de datos identificadas en el CIA.
- Ent_D_CDA, se encuentran 15 entidades de datos identificadas en el CDA.
- Ent_D_CALE, se encuentran 15 entidades de datos identificadas en el CALE.
- Ent_D_CDA_ST, se encuentran 2 entidades de datos identificadas en el CDA que son enviadas a la Superintendencia de Transporte.
- Ent_D_CEA_ST, se encuentran 5 entidades de datos identificadas en el CEA que son enviadas a la Superintendencia de Transporte.
- Ent_D_CRC_ST, se encuentran 9 entidades de datos identificadas en el CDA que son enviadas a la Superintendencia de Transporte.
- SUPERTRANSPORTE, se encuentran 29 entidades de datos identificadas del SICOV en los homologados y la Superintendencia de Transporte.

Se referencia el Anexo Arq.Datos_Catálogo_Entidades_Datos_Asls.xlsx a este documento. De igual forma el catálogo completo se encuentra en la herramienta ARCHI - Archimate Modelling.

4.3.1.2 Matrices

Las matrices son artefactos arquitectónicos que permiten apreciar la relación entre dos catálogos. Para la arquitectura de datos se realizaron dos matrices: Matriz de aplicaciones/datos, que representa la relación entre las aplicaciones y las entidades de datos a las cuales se tiene acceso; Matriz de procesos/datos, que representa la relación entre los procesos y las entidades de datos que son impactados por estos.

4.3.1.2.1 Matriz Procesos vs Entidades de datos

Para un mejor entendimiento de la matriz de Procesos / Entidades de datos se crea una guía para la identificación de cada atributo descrito en la matriz.

Tabla 5. Guía matriz procesos vs entidades de datos

Procesos	Listar los procesos de los diferentes Organismos de Apoyo al Transito - OAT.
Entidades de Datos	Lista las entidades de datos de los diferentes Organismos de Apoyo al Transito - OAT.

Fuente: Elaboración propia Grow Data 2021

Las matrices representan una relación directa entre los procesos y las entidades de datos que tienen acceso a la información de los diferentes Organismos de Apoyo al Transito – OAT.

- CRC, representa la relación entre 9 procesos y 40 entidades de datos del CRC.
- CEA, representa la relación entre 7 procesos y 54 entidades de datos del CEA.
- CDA, representa la relación entre 7 procesos y 20 entidades de datos del CDA.
- CIA, representa la relación entre 6 procesos y 20 entidades de datos del CIA.
- CALE, representa la relación entre 5 procesos y 14 entidades de datos del CALE.

A continuación, se presenta en la Ilustración 23. Matriz procesos/Entidades de datos, donde se puede observar la relación entre los procesos y las entidades. Este artefacto se entrega como Anexo Arq.Datos_Matriz_Entidades_Datos-Proceso_Asls.xlsx a este documento.

Ilustración 23. Matriz procesos/Entidades de datos

Matriz Procesos / Entidades de Datos CRC

Entidad Datos/Procesos	Configuración CRC	Recaudo	Identificación persona	Agendamiento	Evaluación psicología	Evaluación audiometría	Evaluación optometría	Evaluación medicina general	Certificación
Entidad Datos Ubicación	X								
Entidad Datos Identificación	X								
Entidad Datos Aspirante	X								
Entidad Datos Profesionales Salud	X								
Entidad Datos Certificador	X								
Entidad Datos Administrador	X								
Entidad Datos Recepcionista	X								
Entidad Datos Personales para Pago		X							
Entidad Datos Compra o Pago		X							
Entidad Datos PIN		X							
Entidad Datos Agendamiento				X					
Entidad Datos Georreferenciación				X					
Entidad Datos Historia Clínica					X	X	X	X	
Entidad Datos Huella y Verificación RNEC			X						
Entidad Datos Mecanismo Redundante			X						
Entidad Datos Validación Alterna			X						
Entidad Datos Optometría							X		
Entidad Datos Audiometría						X			
Entidad Datos Psicología					X				
Entidad Datos Medicina General								X	
Entidad Datos Valoración de Pruebas									X
Entidad Datos Registro RUNT									X
Entidad Datos Certificación									X
Entidad Datos Seguridad	X								
Entidad Datos Equipos Médicos	X								
Entidad Datos Profesionales Salud RETHUS			X						
Entidad Datos Hoja de Vida Equipos Médicos	X								
Entidad Datos Verificación Diaria y Alarmas	X								
Entidad Datos Reportes OAT	X								
Entidad Datos PosibleFraude	X								
Entidad Datos CrcDetalle	X								
Entidad Datos TarifasCRC	X								
Entidad Datos_Rangos_CRC	X								
Entidad Datos Fe_casosrechazados	X								
Entidad Datos Fe_certifmodif									X

Guía | CRC | CEA | CDA | CIA | CALE

Fuente: Elaboración propia Grow Data 2021

4.3.1.2.2 Matriz Aplicaciones vs Entidades de datos

Para un mejor entendimiento de la matriz de Aplicaciones / Entidades de datos se crea una guía para la identificación de cada atributo descrito en la matriz.

Tabla 6. Guía matriz aplicaciones vs entidades de datos

Aplicaciones	Lista las aplicaciones de los diferentes Organismos de Apoyo al Transito - OAT. Cada una de las aplicaciones debajo del nombre entre () se encuentra el nombre del homologado al cual pertenecen.
Entidades de Datos	Lista las entidades de datos de los diferentes Organismos de Apoyo al Transito - OAT.

Fuente: Elaboración propia Grow Data 2021

Las matrices representan una relación directa entre las aplicaciones y las entidades de datos que tienen acceso a la información de los diferentes Organismos de Apoyo al Transito – OAT.

- CRC, representa la relación entre 8 aplicaciones y 40 entidades de datos del CRC.

- CEA, representa la relación entre 8 aplicaciones y 51 entidades de datos del CEA.
- CDA, representa la relación entre 9 aplicaciones y 19 entidades de datos del CDA.

A continuación, se presenta en la Ilustración 24. Matriz Aplicaciones vs Entidades de datos, donde se puede observar la relación entre las aplicaciones y las entidades. Este artefacto se entrega como Anexo Arq.Datos_Matriz_Entidades_Datos-Aplicaciones_AsIs.xlsx a este documento.

Ilustración 24. Matriz Aplicaciones vs Entidades de datos

Matriz Aplicaciones / Entidades de Datos CDA

Entidad Datos Ubicación	SICOV / INDRA (H. INDRA)	VPAR (H. INDRA)	Splunk (H. INDRA)	CDA Controller (H. Ci2)	Videoma / Manhattan (H. Ci2)	WEB SERVICES SUPERINTENDENCIA DE TRANSPORTE (H. INDRA y H. Ci2)	RESULT - SICOV (H. Ci2)	PAYNET-GATEWAY (H. Ci2)	WEB SERVICES SICOV-INDRA (H. INDRA)
Entidad Datos Identificación	X								
Entidad Datos Personales para Pago								X	
Entidad Datos Compra o Pago								X	
Entidad Datos PIN								X	
Entidad Datos FUR	X			X					X
Entidad Datos Estructuración evidencia recorrido		X			X				
Entidad Datos Vehículo Placa		X			X				
Entidad Datos Verificación		X			X				
Entidad Datos Validación		X			X				
Entidad Datos Validación Resultados FUR							X		
Entidad Datos Registro RUNT							X		
Entidad Datos Equipos de Inspección	X			X					
Entidad Datos Técnico de Pista	X			X					
Entidad Datos Reportes OAT						X			
Entidad Datos IngresoCertificadosCDA						X			
Entidad Datos IngresoDefectosCDA						X			
Entidad Datos TARIFAS_CDA								X	
Entidad Datos TARIFA_CDA_ANSV								X	
Entidad Datos_RANGOS_CDA								X	

Guía | CRC | CEA | CDA

Fuente: Elaboración propia Grow Data 2021

4.3.1.3 Diagramas

Los diagramas, son una forma de representación que sirve para estructurar información y sintetizar conceptos ya sea para explicarlos a los diferentes stakeholders, o para esclarecer ideas que se estén proponiendo o contextualizando. Para efectos de la arquitectura de datos actual (As-Is) se abordaron los diagramas de flujos de información, diagrama de despliegue de infraestructura y soluciones y la arquitectura conceptual (Blue print).

A continuación, se detallan cada uno de los diagramas:

4.3.1.3.1 Flujos de información

Estos artefactos presentan los flujos de los datos entre las entidades internas, entidades externas, procesos y almacenes de datos de los diferentes Organismos de Apoyo al Transito – OAT.

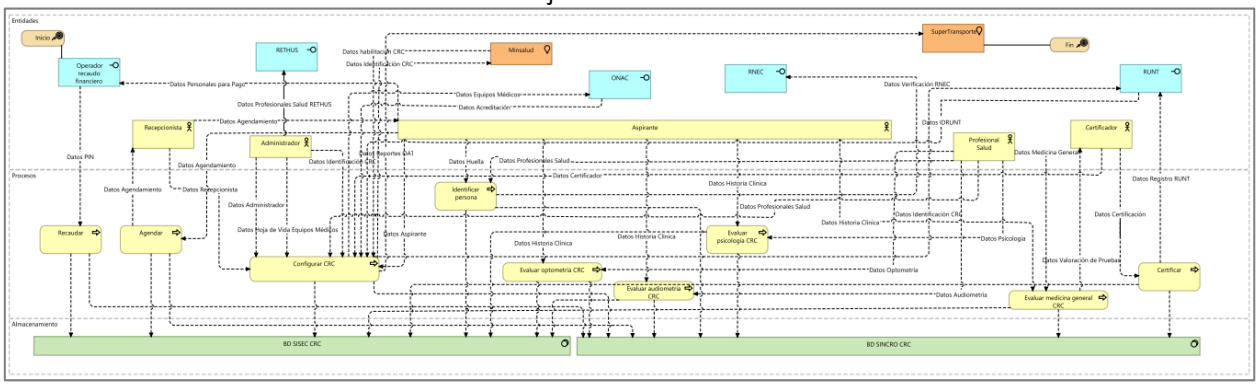
Para la lectura de cada uno de los flujos de información se indica un inicio y un fin del flujo. Adicionalmente, se pueden observar 3 componentes, los cuales son entidades, procesos y almacenamiento.

Los flujos de información ilustran las entidades de datos que interactúan con cada uno de los procesos y entidades. Para cada uno de componentes aquí descritos se requiere de cada uno de los catálogos los cuales son los procesos y las entidades de datos.

A continuación, se presenta en la Ilustración 25. Flujo de información CRC As Is. En el cual se presentan 7 entidades externas, 5 actores internos, 9 procesos y 2 objetos de almacenamiento.

Este artefacto se entrega como Anexo Arq.Datos_Flujo_Información_CRC_AsIs.pdf a este documento. De igual forma el flujo de información del CRC se encuentra en la herramienta ARCHI - Archimate Modelling.

Ilustración 25. Flujo de información CRC As Is

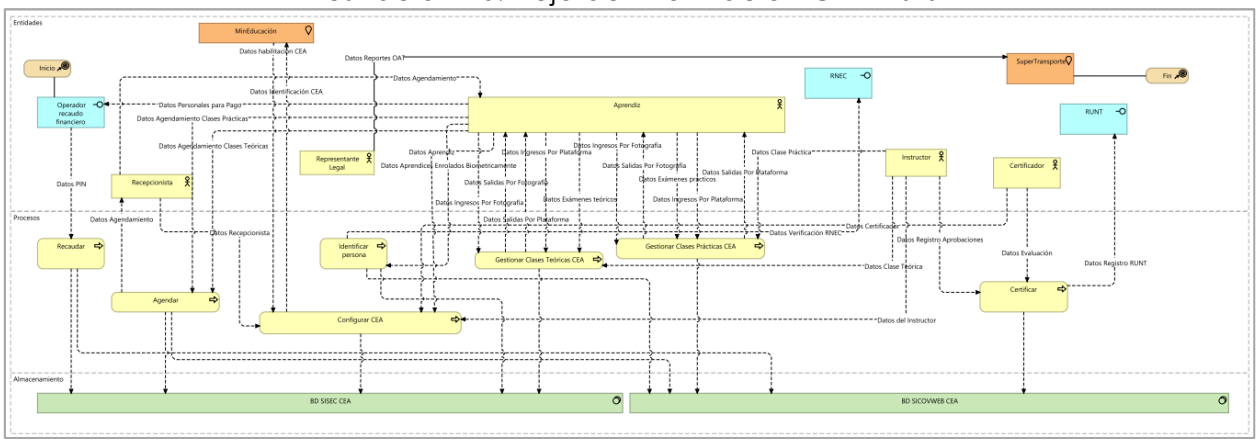


Fuente: Elaboración propia Grow Data 2021

A continuación, se presenta en la Ilustración 26. Flujo de información CEA As Is. En el cual se presentan 5 entidades externas, 5 actores internos, 7 procesos y 2 objetos de almacenamiento.

Este artefacto se entrega como Anexo Arq.Datos_Flujo_Información_CEA_AsIs.pdf a este documento. De igual forma el flujo de información del CEA se encuentra en la herramienta ARCHI - Archimate Modelling.

Ilustración 26. Flujo de información CEA As Is

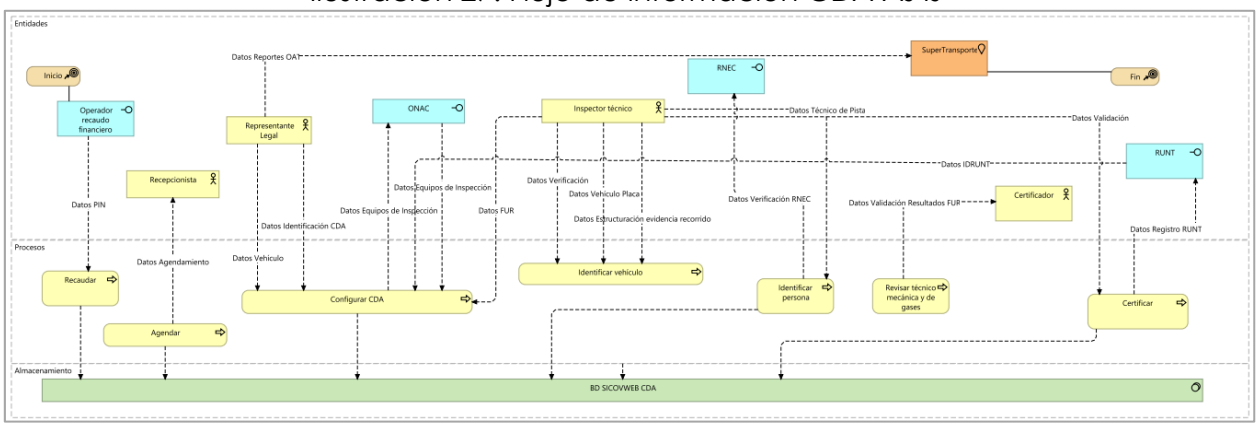


Fuente: Elaboración propia Grow Data 2021

A continuación, se presenta en la Ilustración 27. Flujo de información CDA As Is. En el cual se presentan 5 entidades externas, 4 actores internos, 7 procesos y 1 objeto de almacenamiento.

Este artefacto se entrega como Anexo Arq.Datos_Flujo_Información_CDA_AsIs.pdf a este documento. De igual forma el flujo de información del CDA se encuentra en la herramienta ARCHI - Archimate Modelling.

Ilustración 27. Flujo de información CDA As Is



Fuente: Elaboración propia Grow Data 2021

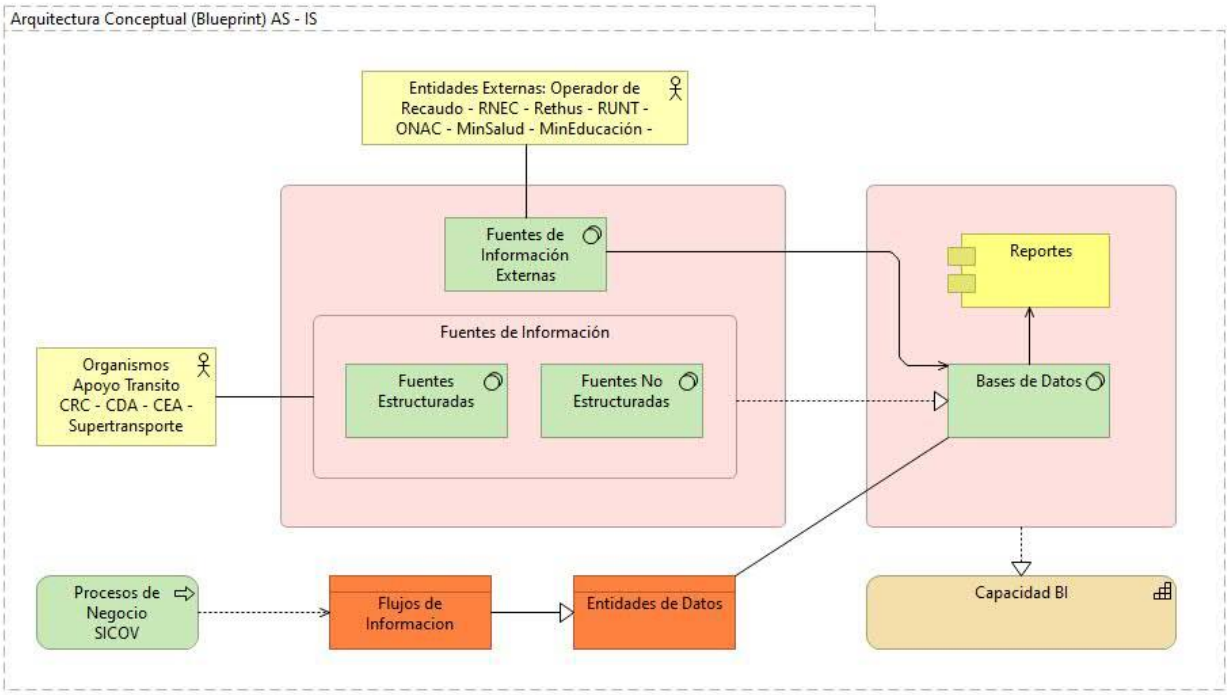
4.3.1.3.2 Arquitectura conceptual AS IS (Blueprint)

Como objetivos principales, la arquitectura de datos actual debe:

- Preparar estratégicamente a la organización para evolucionar rápidamente sus productos, servicios y datos para aprovechar las oportunidades comerciales inherentes a las tecnologías emergentes.
- Traducir las necesidades del negocio en requerimientos de datos y de sistemas para que los procesos tengan de manera consistente los datos que requieren.
- Gestionar la entrega de datos complejos e información en todo el sistema SICOV.
- Facilitar la alineación entre el negocio y TI.
- Actuar como agentes de cambio, transformación y agilidad.

A continuación, se puede apreciar en la arquitectura de datos conceptual actual del sistema SICOV:

Ilustración 28. Arquitectura Conceptual As Is



Fuente: Elaboración propia Grow Data 2021

La arquitectura de datos actual del sistema SICOV está conformada por los siguientes componentes:

- **Entidades:** Son las organizaciones que de forma directa e indirecta generan datos hacia el sistema SICOV. Estas se encuentran clasificadas en dos, las entidades externas conformadas por el operador de recaudo, RNEC, Rethus, Runt, MinSalud y MinEducación; y las entidades internas como son los organismos de apoyo a las autoridades de tránsito: CRC, CDA, CEA y la Supertransporte.

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

- **Fuentes de Información:** Conformada por las diferentes estructuras de datos que son generadas por parte de las entidades. Estas se clasifican en fuentes de datos externas, que son datos estructurados en formato csv y xml, generados por las entidades externas.

  Por otro lado, tenemos las fuentes estructuradas y fuentes no estructuradas; las primeras son generadas por los organismos de apoyo a las autoridades de tránsito en formato csv y xml, y los datos no estructurados son generados por los CDA y están conformados en su totalidad por videos de monitoreo a los vehículos automotores que acceden al centro de diagnóstico automotor.

- **Base de Datos:** Este componente abarca la persistencia y los reportes. Primeramente, se encuentran las diferentes bases de datos que soportan la capa de datos del sistema SICOV (ver el diagrama de despliegue donde se detallan en la 4.3.1.3.3) y por último se identifican diferentes reportes realizados en la SuperTransporte en la herramienta Power BI, los cuales tienen como objetivo reflejar de manera cuantitativa la gestión y control de la operación realizada por parte de los organismos de apoyo al tránsito.

- **Procesos de Negocio, Flujos y Entidades de Datos:** Estos componentes tienen como objetivo identificar las diferentes entidades de datos que conforman el sistema SICOV.

  Inicialmente se identifican y contextualizan los procesos de negocio (descritos y diseñados en el dominio de negocio); estos procesos son insumos para el diagrama de flujos de datos (ver sección de diagramas 4.3.1.3), donde se puede apreciar como estos interactúan con las diferentes entidades de datos y las bases

de datos. Finalmente, se contextualizan las entidades de datos en los catálogos de dominios y entidades de datos.

- **Capacidad BI:** Este componente, está conformado por los diferentes informes generados por los organismos de apoyo a las autoridades tránsito. Si bien, estos abordan en su totalidad analítica descriptiva, la capacidad de inteligencia de negocios es aún incipiente, dado que no se cuenta con un Data Warehouse constituido y una estrategia sólida de BI que permita generar otro tipo de tableros de control en los OAT´s.

En términos generales, se puede concluir de la arquitectura de Datos actual (AS IS), lo siguiente:

- No existe un documento de arquitectura de información que exponga los aspectos asociados con modelamiento, entidades del dato corporativas, modelos conceptuales, lógicos y físicos de manera integral. Las OAT si cuentan con información arquitectónica pero asociada a los sistemas de información de manera individual y está no se encuentra gobernada dado que no existe un repositorio central formalizado.

- Con respecto al catálogo de componentes de información se ha identificado que el sistema SICOV no cuenta actualmente con un catálogo de los componentes de acuerdo con el modelo recomendado por MinTIC, el cual incluye la recopilación de la información de atributos de la misma, de los datos, sus flujos de información, servicios y la matriz de relación entre la información, los servicios de información y los atributos de datos.

- Con respecto al manejo de datos maestros y de referencia, para todo el sistema SICOV no cuenta con una política, arquitectura, definición y herramienta para su gestión. En estos momentos se están actualizando las definiciones arquitectónicas al respecto y se contempla establecer su desarrollo en el marco de gobierno de datos, el cual, por su parte, no se encuentra actualmente implementado en el sistema SICOV.

- No se cuenta con una estrategia de gobierno de datos transversal a todo el SICOV, que permita asegurar que los datos se gestionen correctamente, de acuerdo con las políticas y las mejores prácticas. Es importante que el gobierno de datos este alineado directamente con la estrategia de la organización. Cuanto más claramente ayude a resolver problemas organizacionales, más probable será que las personas cambien sus comportamientos y adopten

prácticas de gobierno. Los motivadores del Gobierno de Datos se centran con mayor frecuencia en la reducción de riesgos o en la mejora de los procesos.

- No existe una estrategia de almacenamiento centralizada que permita tener mayor control y gobierno sobre las diferentes bases de datos de los homologados. Si bien, se cuentan con óptimos recursos en la capa de persistencia de datos, estos son gestionados de forma aislada y es difícil el intercambio de datos entre ellos.

- Si bien, se cuenta con una analítica descriptiva e incipiente, solo se cuentan con reportes aislados por demanda, los cuales son generados por la SuperTransporte con la información enviada por los OAT. Es importante implementar una estrategia de inteligencia de negocios y analítica más madura que, pueda responder a las necesidades de explotación de información de las diferentes entidades que hacen parte del sistema SICOV.

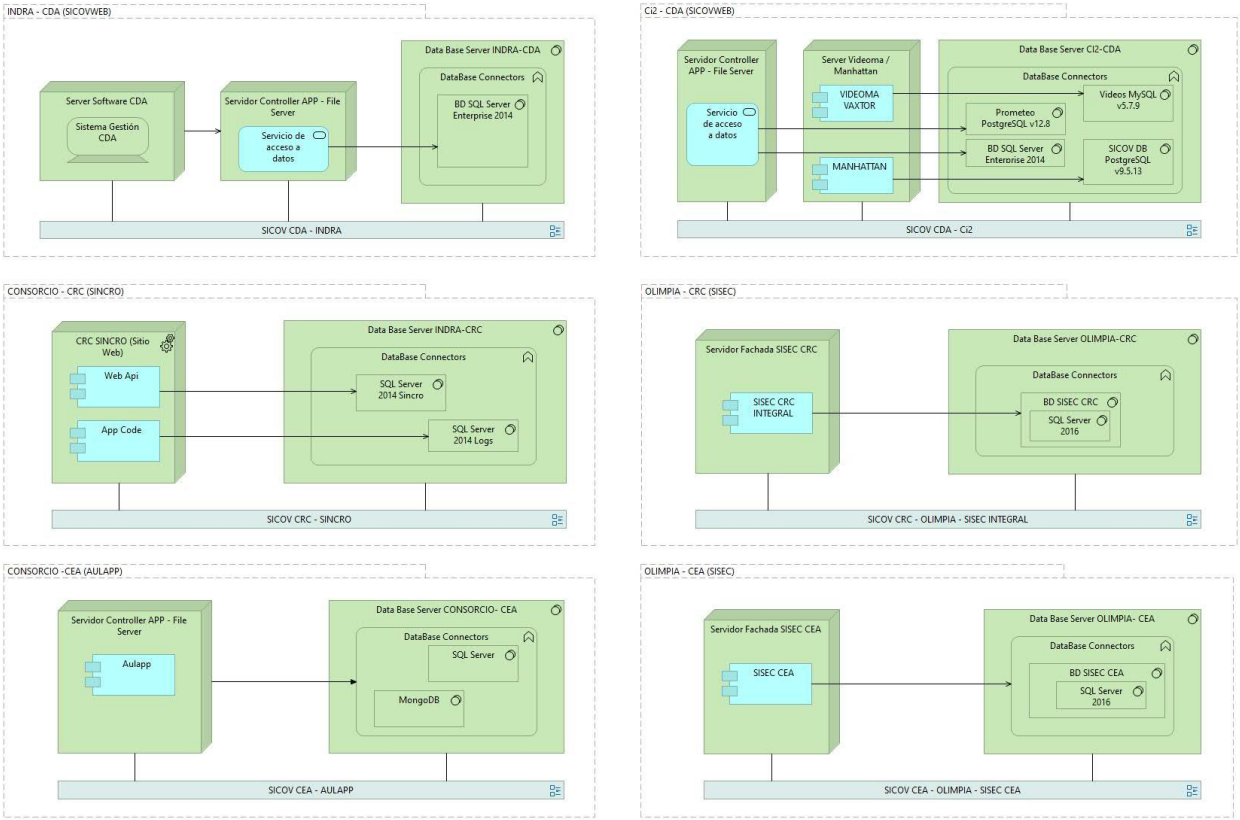
Este artefacto se entrega como Anexo Arq.Datos_Arquitectura_Conceptual_AsIs.pdf a este documento. La Arquitectura Conceptual As Is se encuentra en el repositorio de arquitectura modelado en ARCHI - Archimate Modelling.

4.3.1.3.3 Diagrama de despliegue de la infraestructura y las soluciones para la gestión de información

El diagrama de despliegue de la Ilustración 30. Diagrama de despliegue As Is modela la infraestructura tecnológica en relación con los elementos utilizados de hardware y software para soportar procesamiento de Bases de Datos y analítica de datos en cada uno de los homologados de los diferentes Organismos de Apoyo al Transito – OAT.

El diagrama ilustra de forma agrupada 2 homologados por cada OAT de la siguiente forma:

Ilustración 29. Diagrama de despliegue As Is



Fuente: Elaboración propia Grow Data 2021

- **CDA**

  - **Homologado INDRA Sistemas S.A. Sucursal Colombia:** Se visualiza un servidor controlador SICOVWEB, el cual recibe la información del sistema de gestión del CDA, para procesar la información de los FUR[3] generados por cada vehículo y de los videos realizados sobre la pista de inspección; estableciendo una comunicación con el servidor de base de datos de la aplicación SICOV del homologado la cual se encuentra en el centro de procesamiento de datos el cual posee actualmente un motor SQL Server Enterprise 2014 para llevar a cabo la misionalidad del CDA.

[3] FUR: Formato Uniforme de Resultados

- **Homologado Ci2 (Compañía Internacional de Integración S.A):** Se visualiza un servidor controlador SICOVWEB, el cual recibe la información del sistema de gestión del CDA, para procesar la información de los FUR generados por cada vehículo; estableciendo una comunicación con los servidores de las bases de datos de la aplicación SICOV del homologado la cual se encuentra en el centro de procesamiento de datos, los cuales poseen motores Prometeo PostgreSQL v12.8 y SQL Server Enterprise 2014.

  También recibe información para procesar los videos realizados sobre la pista de inspección en las aplicaciones VIDEOMA y MANHATTAN[4]; los cuales poseen motores MySQL v5.7.9 para VIDEOMA y PostgreSQL v9.5.13 para MANHATTAN.

- **CRC**

  - **Homologado Consorcio SICOV CRC (Indra Sistemas S.A., Certicamara S.A. y Digital Training S.A.):** Se visualiza un servidor web de la aplicación SINCRO CRC, el cual recibe la información generada por los equipos del CRC a través de una app code y un web api; la cual contiene los elementos de conexión a la base de datos de la aplicación SICOV del homologado la cual se encuentra en el centro de procesamiento de datos con motor SQL Server 2014; para llevar a cabo la misionalidad del CRC.

  - **Homologado Olimpia IT S.A.S:** Se visualiza un servidor que recibe la información generada por la operación en la aplicación SISEC CRC, la cual se conecta al servidor de base de datos de la aplicación SICOV del homologado la cual se encuentra en el centro de procesamiento de datos que contiene un motor de base de datos SQL Server 2016.

- **CEA**

  - **Homologado Consorcio Sistema Integrado de Gestión y Seguridad para CEAS Y CIAS:** Se visualiza un servidor que recibe la información generada por la operación en la aplicación Aulapp, la cual se conecta al servidor de base de datos de la aplicación SICOV del homologado la cual se encuentra en el centro de procesamiento de datos que contiene un motor de base de datos mongoDB y un SQL server.

[4] Mayor información revisar el catálogo de soluciones que se entrega como anexo

- **Homologado Olimpia: IT S.A.S.** Se visualiza un servidor que recibe la información generada por la operación en la aplicación SISEC CEA, la cual se conecta al servidor de base de datos de la aplicación SICOV del homologado la cual se encuentra en el centro de procesamiento de datos que contiene un motor de base de datos SQL Server 2016.

El diagrama de despliegue se encuentra en el repositorio de Arquitectura modelado en la herramienta ARCHI - Archimate Modelling y dentro de cada uno de los OAT descritos se encuentra un link directo al diagrama de despliegue completo de infraestructura tecnológica.

Este artefacto se entrega como Anexo Arq.Datos_Diagrama_despliegue_datos_AsIs.pdf a este documento.

4.4 Arquitectura de Infraestructura

Esta sección presenta el estado actual del dominio de Infraestructura del sistema SICOV

4.4.1 Catálogo de Servicios de Tecnología

Los servicios de Tecnología representan los recursos de la plataforma tecnológica (Hardware o software) que soportan actualmente el sistema SICOV en términos de servicios tecnológicos. Cualquier aplicación o servicio de negocio puede hacer uso de estos recursos.

A continuación, se presentan a nivel general los servicios TI identificados y los cuales se encuentran en el artefacto Arq.Infra_Catálogo_Servicios_TI.xlsx construido en la herramienta Microsoft Excel (que se entrega adjunto a este documento), con base en la información obtenida de los operadores homologados para cada uno de los OAT.

Tabla 7. Servicios Tecnológicos OAT

Servicio Tecnológico	OAT		
	CRC	CEA	CDA
Enrolamiento	X	X	X
Procesamiento	X	X	X
Almacenamiento	X	X	X
Conectividad	X	X	X
Seguridad Perimetral	X	X	X
Detección			X
Mesa de Servicio	X	X	X
SOC	X	X	X
Data Center	X	X	X
Energía Eléctrica Regulada	X	X	X

Fuente: Elaboración propia Grow Data 2021

4.4.2 Catálogo de Componentes de Infraestructura

Los componentes de infraestructura representan elementos tecnológicos desde una perspectiva lógica. Dichos componentes pueden alojarse en uno o varios componentes lógicos de hardware y pueden prestar, en conjunto, servicios de base para cualquier

servicio tecnológico descrito en el numeral anterior. Como ejemplos de componentes lógicos de hardware se encuentran: servidores, switch, Firewall y otros.

A continuación, se presenta a nivel general los componentes de infraestructura identificados y los cuales se encuentran en el artefacto Arq.Infra_Catálogo_Componentes.xlsx construido en la herramienta Microsoft Excel (que se entrega adjunto a este documento), con base en la información obtenida de los operadores homologados para cada uno de los OAT.

Tabla 8. Componentes Lógicos OAT

Componente Lógico	OAT		
	CRC	CEA	CDA
Datáfono	X	X	X
Huellero	X	X	X
Cámara	X	X	X
Pad de Firmas	X	X	
Escáner de Documentos	X	X	
Servidores	X	X	X
SAN / NAS	X	X	X
Switch	X	X	X
Firewall / WAF	X	X	X
Cabina Insonorizada	X		
Visiómetro	X		
Psicosométrico	X		
Tag Vehículos		X	
Luxómetro			X
Frenómetro			X
Detector de Holguras			X
Pista de Inspección			X
Analizador de Gases			X
Cámara de Detección			X

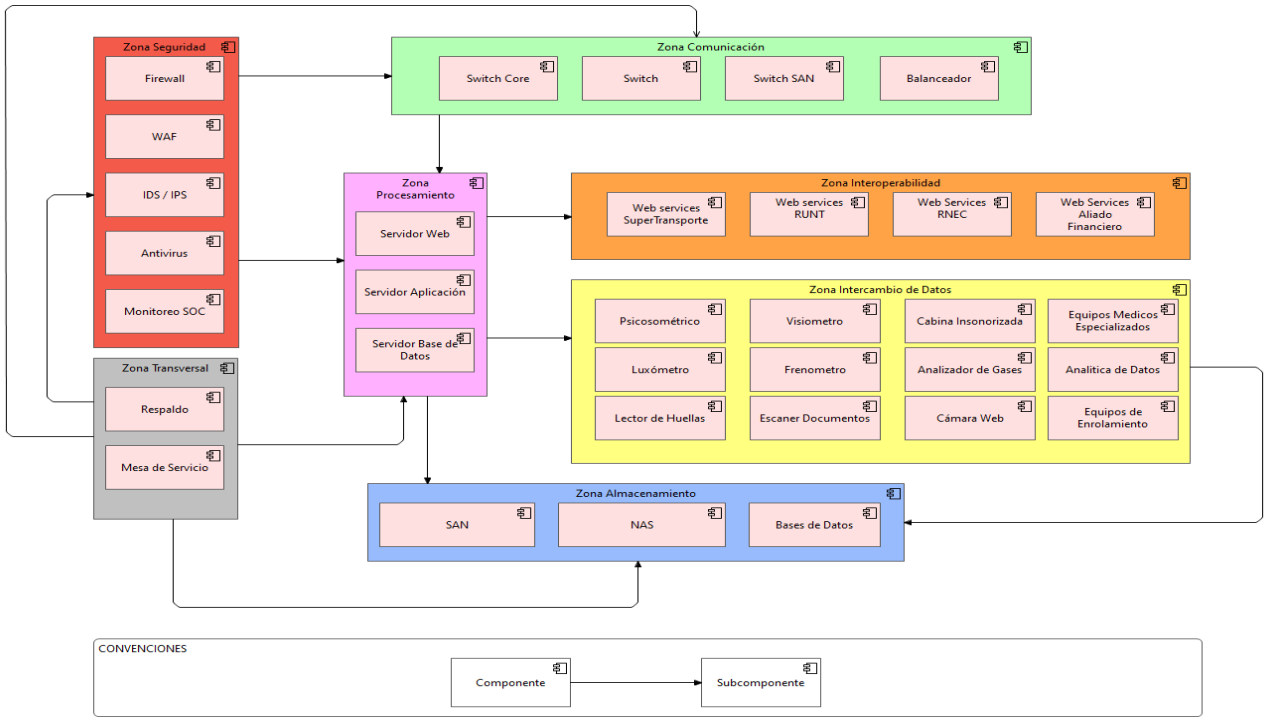
Fuente: Elaboración propia Grow Data 2021

4.4.3 Arquitectura conceptual actual (AS- IS) (Blueprint)

La arquitectura conceptual actual se encuentra enfocada de manera genérica para todos los tipos de OAT, buscando realizar el análisis del estado actual de la infraestructura tecnológica, dentro de los elementos plasmados en la arquitectura conceptual existen componentes que son generales y otros que son particulares para

algunos OAT. En el diagrama conceptual se puede visualizar las diferentes zonas de infraestructura las cuales se encuentran integrados por los diferentes componentes que apalancan al sistema SICOV desde una perspectiva global.

Ilustración 30. Arquitectura Conceptual Blue Print As Is



Fuente: Elaboración propia Grow Data 2021

En la representación esquemática se pueden identificar los siguientes elementos significativos identificados como zonas y sus componentes lógicos:

- **Zona de Seguridad**: La zona de seguridad agrupa aquellos componentes lógicos necesarios que aseguran la debida protección al sistema de información SICOV contra ataques de ciberseguridad en la capa de aplicación como en la capa de bases de datos.

    - Firewall / Waf: Estos componentes, contienen los elementos requeridos para soportar el servicio de prevención y protección a la red privada del homologado y a la zona de procesamiento donde se procesa el SICOV. Estos componentes deben cumplir con características mínimas como son: protección de redes inalámbricas wi-fi, acceso a la red y acceso a internet, protección contra intrusos, bloqueos, definición de reglas.
    - IDS / IPS: Estos componentes, contienen los elementos requeridos para soportar el servicio de detección y prevención de actividad maliciosa que pueda estar afectando la infraestructura de red que soporta el sistema SICOV. Estos componentes deben cumplir con características mínimas como son: funcionar correctamente sin intervención humana, debe ser tolerante a fallos, debe imponer mínima sobrecarga a la red del homologado.
    - Antivirus: Este componente, contiene los elementos requeridos para soportar el servicio de búsqueda, detección y eliminación de virus informáticos que puedan afectar la infraestructura tecnológica que soporta el SICOV; así como también la detección de correo basura que pueda sobrecargar la red interna. Este componente debe cumplir con características mínimas como son: protección de todos los nodos dentro de la operación del SICOV, capacidad de detección y reacción ante nuevos virus informáticos, actualización sistemática, detección mínima de falsos positivos y/o virus, integración con el correo electrónico, alertas sobre posibles infecciones en los nodos, capacidad de distintos métodos de detección y análisis, creación de discos de emergencia.
    - Monitoreo – SOC: Este componente contiene los elementos requeridos para monitorear, prevenir y/o controlar la seguridad sobre la infraestructura que apalanca el SICOV. Este componente debe cumplir con características mínimas como son: detección, análisis y corrección de problemas e incidentes de seguridad, Supervisión y análisis de las actividades en redes, servidores, terminales, bases de datos, aplicaciones y sitios web en busca de actividades o comportamientos sospechosos o anomalías, así como vulnerabilidades que puedan poner en riesgo la

seguridad del SICOV y de la información; Respuesta y defensa de ataques, Registro e investigación de todos los incidentes de seguridad que hayan ocurrido, Recuperación de la información perdida o dañada en un ataque, Realizar tareas de criptoanálisis y de ingeniería inversa sobre el malware empleado por los ciberdelincuentes.

- **Zona de Comunicación**: La zona de comunicación agrupa aquellos componentes lógicos necesarios que garantizan la debida comunicación interna entre los elementos de hardware que soportan el procesamiento y almacenamiento de la información generada en la operación del SICOV, así como la comunicación externa de los diferentes OAT con la aplicación del SICOV.

    - Switch: Este componente, contiene los elementos requeridos para soportar el servicio de comunicación e interconexión, a través de un dispositivo que sirve para comunicar los elementos tecnológicos necesarios dentro del sistema del SICOV dentro de una misma red. Este componente debe cumplir con características mínimas como son: permitir la interconexión de distintos segmentos físicos de la red local (LAN), determinar el destino de los datos y enviarlos de manera eficiente, interconectar las redes por medio de cables UTP, recibir la señal cualquiera de los puertos para compartirla al resto de los puertos, contar con varios puertos (desde 4 puertos, 8 puertos, 16 P, 32 P y hasta 52 Puertos).
    - Switch Core: Este componente contiene los elementos requeridos para brindar alta disponibilidad a la comunicación del SICOV apoyándose en principios redundantes. Este componente debe cumplir con características mínimas como son: brindar características de alta disponibilidad, contar con componentes redundantes como fuentes de poder con balanceo de carga, doble o triple bus de datos compartido, módulos redundantes de fibra óptica, procesadores redundantes del switch y alta densidad de puertos Fast o Gigabit Ethernet.
    - Switch SAN: Este componente contiene los elementos requeridos para conectar componentes de almacenamiento y gestionar el tráfico de información de almacenamiento.
    - Balanceador: Este componente contiene los elementos requeridos para direccionar las solicitudes de los diferentes OAT que requieran acceso al SICOV de manera simultánea.

- **Zona Procesamiento**: La zona de procesamiento agrupa aquellos componentes lógicos que son necesarios para poder procesar el sistema de información del SICOV y la información generada dentro de su funcionalidad.

- Servidor Web: Este componente contiene los elementos requeridos para el procesamiento de la aplicación SICOV permitiendo las conexiones con los diferentes organismos de apoyo a las autoridades de tránsito. Este componente debe cumplir con características mínimas como son: capacidad de almacenamiento, transferencia de datos, seguridad, hardware del servidor, soporte web.
- Servidor de Aplicaciones: Este componente contiene los elementos requeridos para proporcionar servicios de aplicación referentes al SICOV y que son necesarios para su operación, gestión y monitoreo.
- Servidor Base de Datos: Este componente contiene los elementos requeridos para gestionar las consultas a los usuarios que solicitan información generada por la operación del SICOV dentro de las bases de datos relacionadas. Este componente debe cumplir con características mínimas como son: indexación, replicación de datos, balanceo inteligente de carga, almacenamiento de archivos, agregación de datos, configuración de privilegios de usuarios y encriptación por SSL/TLS.

- **Zona de Almacenamiento**: La zona de almacenamiento agrupa aquellos componentes lógicos necesarios para poder almacenar y respaldar la información generada dentro de la operación del sistema SICOV.

  - SAN: Este componente contiene los elementos requeridos para brindar acceso a alta velocidad al almacenamiento de la información generada en el sistema SICOV.
  - NAS: Este componente contiene los elementos requeridos ´para compartir la capacidad de almacenamiento de los diferentes servidores que apalancan el procesamiento del SICOV.

- **Zona de Interoperabilidad**: La zona de interoperabilidad agrupa aquellos componentes lógicos necesarios para el intercambio de información entre el SICOV y los diferentes interesados externos.

  - Web Services: Este componente contiene los elementos requeridos para intercambiar información con las diferentes entidades externas (Supertransporte, Runt, Rnec, Aliado Financiero) por medio de estándares y protocolos.

- **Zona Intercambio de Datos**: La zona de intercambio de datos agrupa aquellos componentes lógicos desde la operación de los habilitados y los cuales son necesarios para garantizar la recopilación y la captura de los datos requeridos

por los diferentes organismos de apoyo al tránsito (CRC, CEA, CDA) de cara al ciudadano.

- Psicosométrico: Este componente contiene los elementos requeridos para soportar el proceso de realizar el examen psicológico, a través de un dispositivo utilizado para pruebas de tamizaje en aptitudes de coordinación motriz aplicable en la evaluación y certificación al ciudadano que busca ser reconocido como conductor de vehículos automotores en los centros de reconocimiento a conductores (CRC).
- Cabina Insonorizada: Este componente contiene los elementos requeridos para soportar el proceso de realizar el examen auditivo, a través de un dispositivo que tiene la capacidad de garantizar un entorno adecuado de aislamiento acústico para la realización de las pruebas audio métricas a los ciudadanos que buscan ser certificados en los centros de reconocimiento a conductores (CRC).
- Visiometro: Este componente, contiene los elementos requeridos para soportar el proceso de realizar el examen óptico, a través de un dispositivo utilizado para la realización de los exámenes oftalmológicos y de visión a los ciudadanos que requieren los servicios de los centros de reconocimiento a conductores en los centros de reconocimiento a conductores (CRC)
- Luxómetro: Este componente, contiene los elementos requeridos para soportar el proceso que permite medir simple y rápidamente la iluminación real y no subjetiva de los faroles de los vehículos automotores, realizado en los centros de diagnóstico automotor (CDA)
- Frenómetro: Este componente, contiene los elementos requeridos para soportar el proceso de realizar una evaluación fiable del estado del sistema de frenado de un vehículo automotor, realizado en los centros de diagnóstico automotor (CDA)
- Detector de Holguras: Este componente, contiene los elementos requeridos para soportar el proceso de efectuar el control visual de las holguras en un eje del vehículo (manguetas, pivotes, suspensiones, articulaciones, rodamientos, puente, etc.), realizado en los centros de diagnóstico automotor (CDA)
- Analizador de Gases: Este componente contiene los elementos requeridos para soportar el proceso de verificación de la calidad de emisiones de vehículos de motor a diésel y a gasolina, realizado en los centros de diagnóstico automotor (CDA)
- Cámara Detección: Este componente contiene los elementos requeridos para soportar el proceso de detección del número de placa del vehículo automotor al ingreso y salida del CDA, así mismo la de grabar el paso del

vehículo automotor por las diferentes estaciones de la pista del CDA, realizado en los centros de diagnóstico automotor (CDA)

- Lector de Huellas: Este componente contiene los elementos requeridos para soportar el proceso de identificación y enrolamiento, a través de un dispositivo que tiene la capacidad de leer, guardar e identificar las huellas dactilares de los ciudadanos aspirantes / pacientes y de los directores técnicos. Este componente aplica para los CRC, CEA y CDA.
- Escáner de Documentos: Este componente contiene los elementos requeridos para soportar el proceso de identificación y enrolamiento, a través de un lector modular de cedulas de ciudadanía que escanea y provee una imagen del documento de identidad del ciudadano que solicita los servicios del OAT. Este componente aplica para los CRC y CEA.
- Cámara Web: Este componente contiene los elementos requeridos para soportar el proceso de identificación y enrolamiento, a través de una cámara digital la cual puede capturar las imágenes del rostro de los ciudadanos al momento de realizar el registro en el SICOV. Este componente aplica para los CRC y CEA.
- Pad de Firmas: Este componente contiene los elementos requeridos para soportar el proceso de identificación y enrolamiento, a través de un dispositivo capaz de registrar y llevar un registro digital de la firma del ciudadano que se registra en el SICOV para su uso y/o almacenamiento. Este componente aplica para los CRC y CEA.

- Zona Transversal: La zona transversal agrupa aquellos componentes lógicos que son necesarios para brindar el apoyo a la operación del SICOV ya sea de manera preventiva y/o reactiva.

  - Respaldo: Este componente contiene los elementos requeridos para generar la copia de los datos originales generados por el SICOV con el fin de poder disponer de estos en caso de que sean requeridos.
  - Mesa de Servicio: Este componente contiene los elementos requeridos para brindar el soporte necesario a los diferentes organismos de apoyo al tránsito cuando presentan alguna incidencia que afecte la operación del SICOV.

4.4.4 Arquitectura de Solución

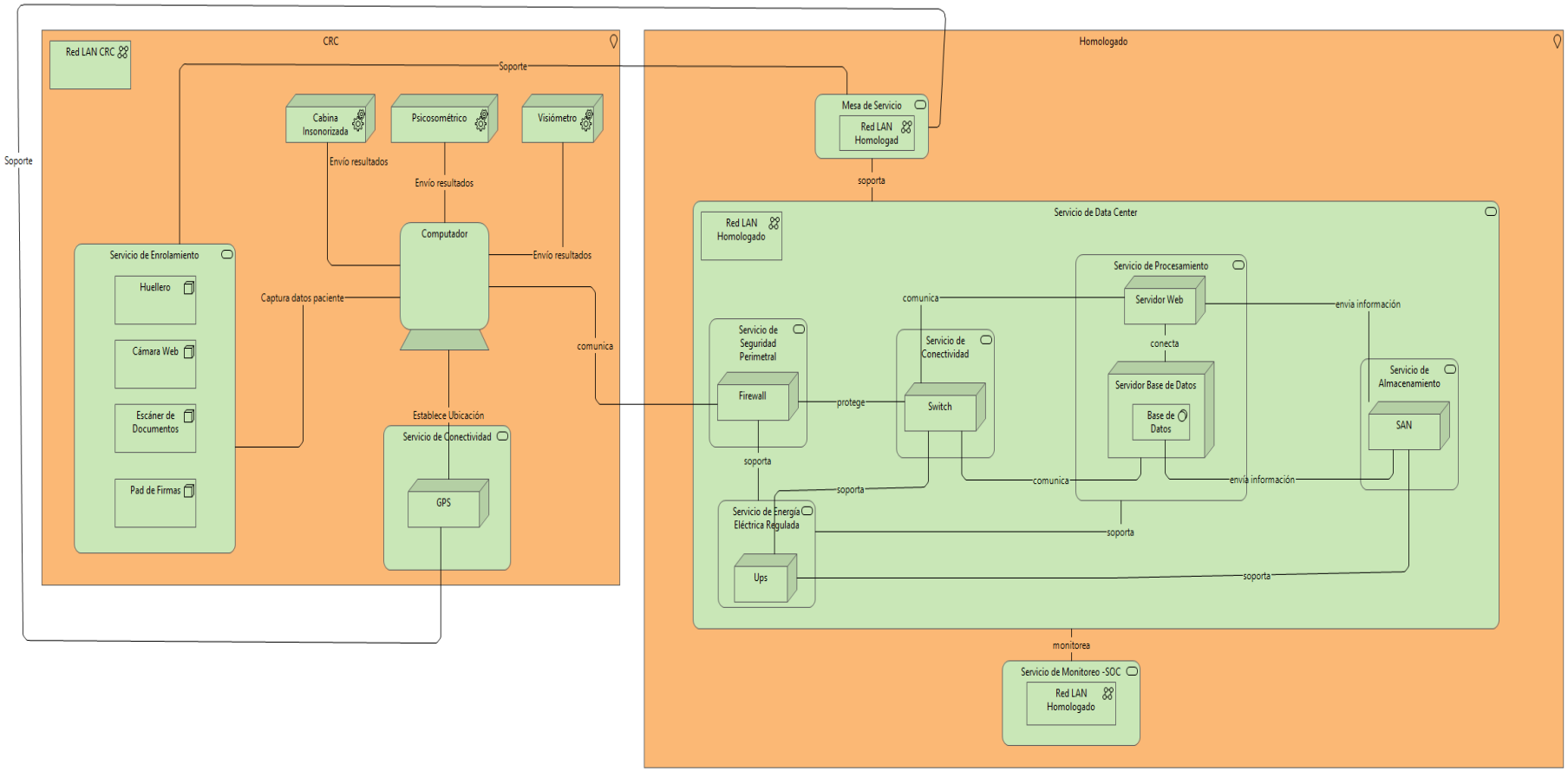
En este capítulo se muestra el diagrama de la arquitectura de solución para los diferentes organismos de apoyo al tránsito (CRC, CEA y CDA) de acuerdo con la información recibida y analizada de los diferentes homologados que prestan el SICOV. Actualmente los CALE y los CIA no se encuentran en operación bajo el esquema del

SICOV, por lo tanto no se desarrolla la arquitectura de solución actual para estos tipos de OAT. Esta arquitectura de solución se encuentra diseñada bajo el concepto cliente / servidor, el cual es un modelo donde las tareas se distribuyen entre los diferentes servicios para satisfacer las peticiones realizadas por los organismos de apoyo al tránsito, garantizando la operación normal de los OAT de cara al ciudadano.

4.4.4.1 Arquitectura de solución para los CRC

En el siguiente diagrama de solución se puede visualizar los diferentes servicios tecnológicos que son requeridos para la operación de los centros de reconocimiento de conductores, y cada componente que apalanca la operación de este.

Ilustración 31. Arquitectura Solución actual CRC



Fuente: Elaboración propia Grow Data 2021

Se puede observar cómo se interrelacionan estos servicios de acuerdo con su naturaleza mostrando los componentes que hacen parte de dichos servicios.

Partiendo de la ubicación física del CRC, se encuentra el servicio de enrolamiento el cual por medio de sus componentes capturan los datos del aspirante y los envía hacia un computador del CRC; adicional se encuentran los equipos médicos los cuales se comunican con el sistema de gestión del SICOV transmitiendo la información de los resultados de las pruebas realizadas a los ciudadanos, todo lo anterior por medio de la red local del CRC.

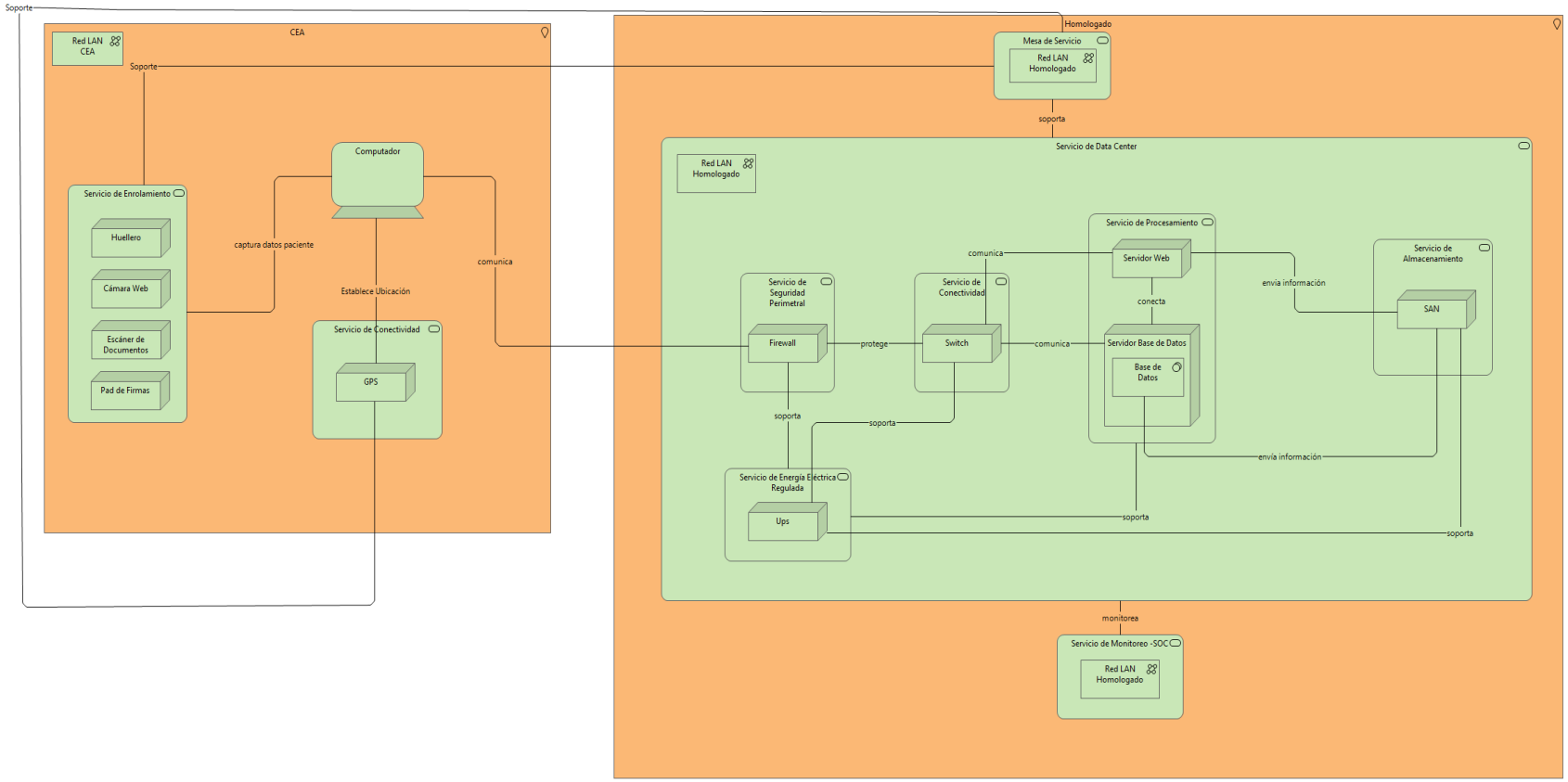
Ya en la ubicación del centro de procesamiento de datos del homologado, se identifican los servicios base que permiten la protección de la red local del homologado mediante el servicio de seguridad perimetral y su componente firewall.

Mediante el servicio de conectividad se accede al servicio de procesamiento de datos donde se encuentran los elementos de infraestructura como servidores (web y base de datos) los cuales envían la información procesada al servicio de almacenamiento. Todo lo anterior se encuentra apalancado por el servicio de data center, el cual se encuentra soportado y monitoreado por el servicio de mesa de servicio, el servicio de monitoreo – SOC y el servicio de energía eléctrica regulada.

4.4.4.2 Arquitectura de solución para los CEA

En este diagrama de solución se puede visualizar los diferentes servicios tecnológicos que son requeridos para operar el SICOV para los centros de enseñanza automovilística.

Ilustración 32. Arquitectura Solución actual CEA



Fuente: Elaboración propia Grow Data 2021

Se puede observar desde las diferentes ubicaciones como se interrelacionan estos servicios de acuerdo con su naturaleza mostrando los componentes que hacen parte de dichos servicios.

Partiendo de la ubicación física del CEA, se encuentra el servicio de enrolamiento el cual por medio de sus componentes capturan los datos del aspirante y los envía hacia un computador del CEA; adicional se encuentra dentro del servicio de conectividad el componente GPS, el cual por medio de este se establece la ubicación geográfica del CEA, todo lo anterior por medio de la red local del CEA.

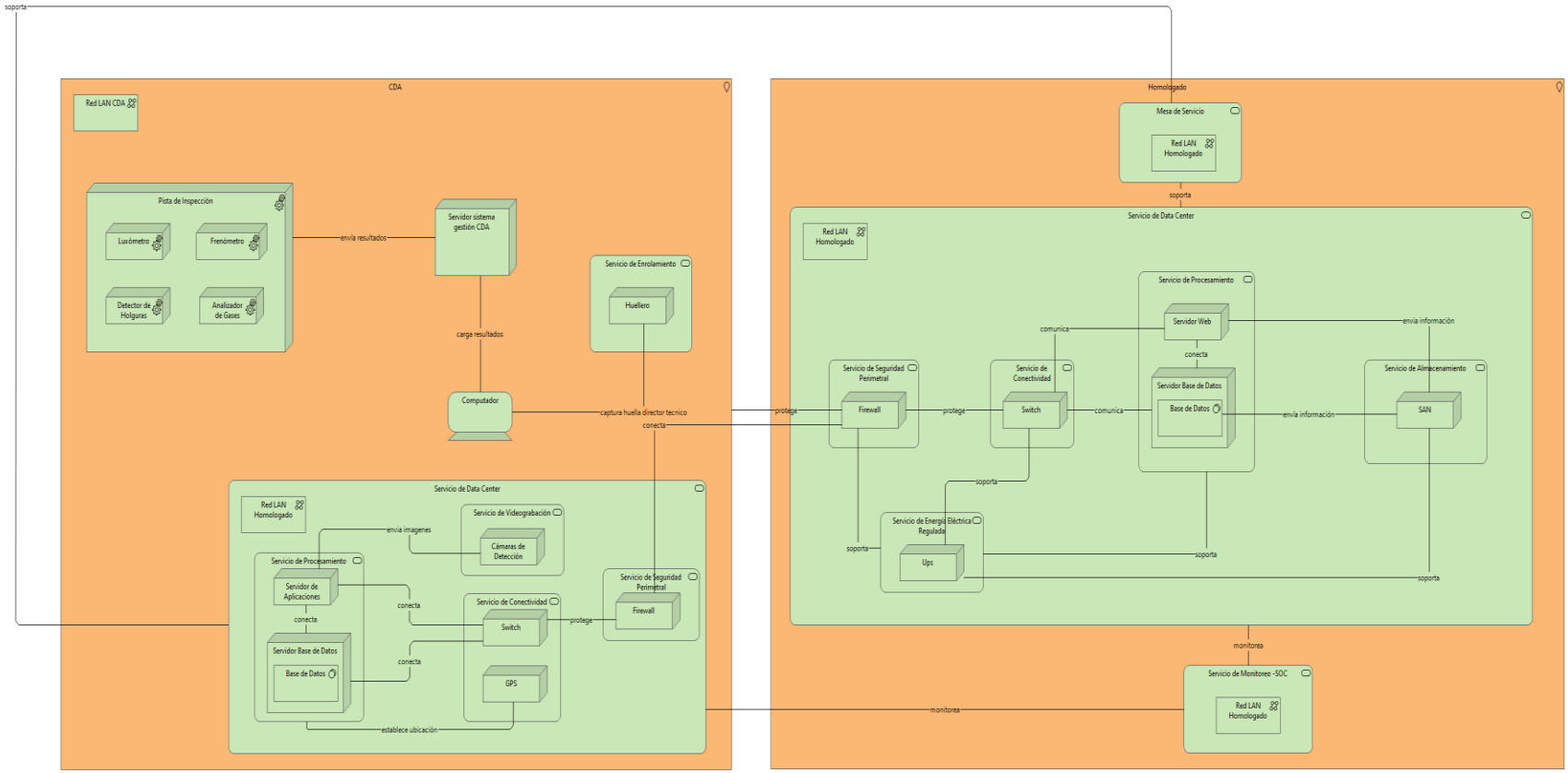
Ya en la ubicación del homologado se identifican los servicios base que permiten la protección de la red del homologado mediante el servicio de seguridad perimetral y su componente firewall.

Mediante el servicio de conectividad se accede al servicio de procesamiento donde se encuentran los componentes de servidores (web y base de datos) los cuales envían la información procesada al servicio de almacenamiento. Todo lo anterior, se encuentra apalancado por el servicio de data center, el cual se encuentra soportado y monitoreado por el servicio de mesa de servicio, el servicio de monitoreo – SOC y el servicio de energía eléctrica regulada.

4.4.4.3 Arquitectura de solución para los CDA

En este diagrama de solución se puede visualizar los diferentes servicios tecnológicos, que son requeridos para satisfacer las necesidades que conllevan en el despliegue del SICOV para los centros de diagnóstico automotor y cada componente que apalanca la operación de este.

Ilustración 33. Arquitectura Solución actual CDA



Fuente: Elaboración propia Grow Data 2021

Se puede observar desde las diferentes ubicaciones como se interrelacionan estos servicios de acuerdo con su naturaleza mostrando los componentes que hacen parte de dichos servicios.

Partiendo de la ubicación física del CDA, se encuentran los equipos de medición los cuales realizan el envío de los resultados de las mediciones realizadas a los vehículos automotores, estos resultados los envían a un servidor propio perteneciente al CDA, el cual contiene el sistema de gestión del centro de diagnóstico automotor, donde este servidor envía los resultados al SICOV para que el director técnico avale los resultados capturados; se encuentra el servicio de enrolamiento el cual por medio de su componente Huellero captura los datos del director técnico para avalar los resultados obtenidos en cada una de las pruebas realizadas a los vehículos; adicional se encuentra el servicio de data center el cual concentra los servicios de procesamiento con el servidor de aplicaciones de captura de placas y video grabación, los cuales se comunican mediante el servicio de conectividad y el servicio de seguridad perimetral con el servidor web del SICOV que se encuentra en el centro de procesamiento de datos del homologado, todo lo anterior por medio de la red LAN del homologado.

Ya en la ubicación del homologado se identifican los servicios base que permiten la protección de la red del homologado mediante el servicio de seguridad perimetral y su componente firewall.

Mediante el servicio de conectividad se accede al servicio de procesamiento donde se encuentran los componentes de servidores (web y base de datos) los cuales envían la información procesada al servicio de almacenamiento. Todo lo anterior se encuentra apalancado por el servicio de data center, el cual se encuentra soportado y monitoreado por el servicio de mesa de servicio, el servicio de monitoreo – SOC y el servicio de energía eléctrica regulada.

4.4.5 Diagramas de Despliegue

En este capítulo se muestran los diagramas de despliegue para los diferentes organismos de apoyo a las autoridades de tránsito (CRC, CEA y CDA) de acuerdo con la información recibida y analizada de los diferentes homologados que gestionan el SICOV, los cuales detallan la relación entre los diferentes componentes de procesamiento que actualmente se encuentran desplegados para apalancar la operación del SICOV.

Actualmente los CALE y los CIA no se encuentran en operación bajo el esquema del SICOV, por lo tanto, no se desarrollan los diagramas de despliegue actuales para estos tipos de OAT.

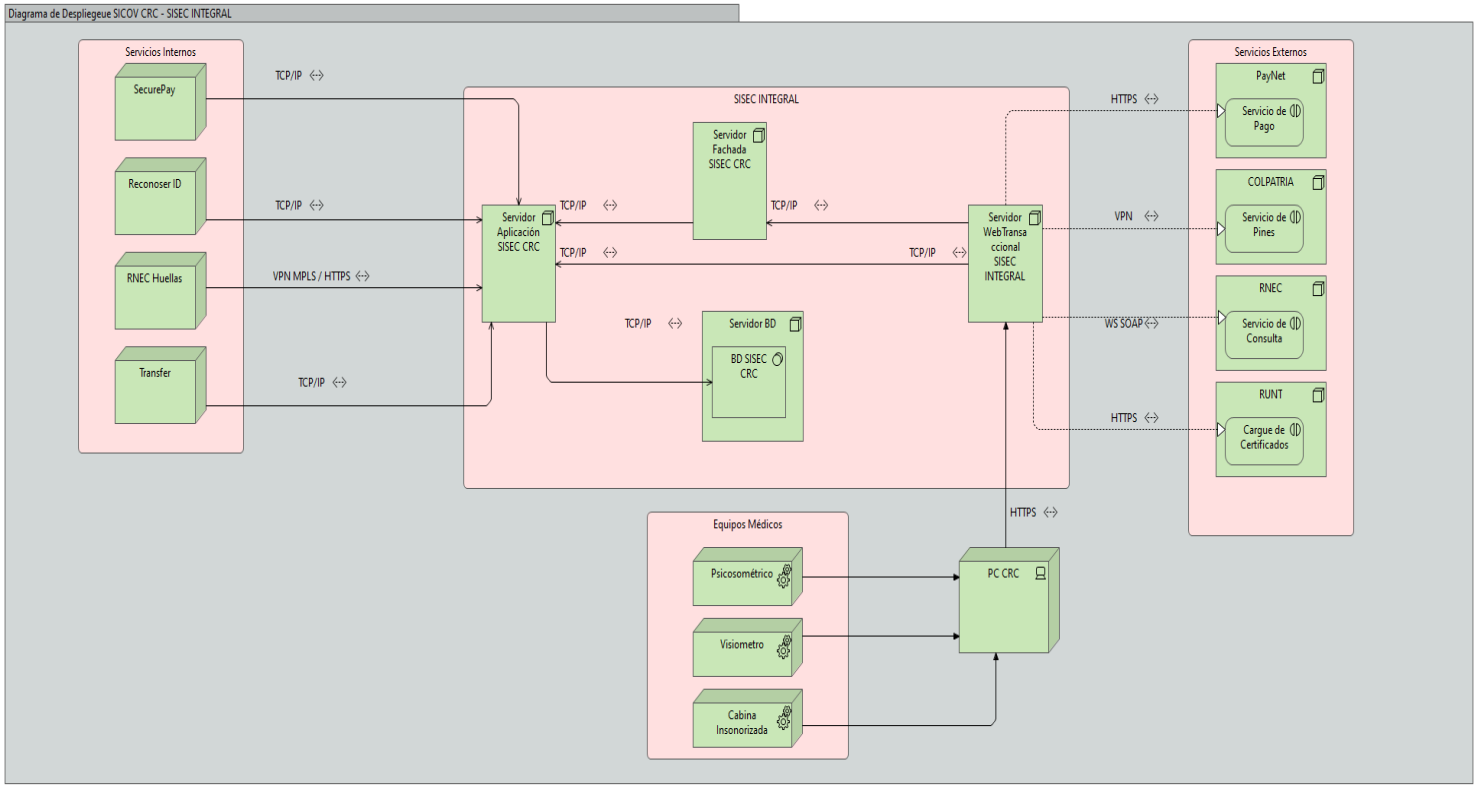
Estos diagramas de despliegue se desarrollan por cada uno de los homologados que actualmente se encuentran prestando el servicio del SICOV, los cuales son:

- CRC (Homologado Olimpia IT S.A.S y Consorcio SICOV CRC)
- CEA (Homologado Olimpia IT S.A.S y Consorcio SICOV CEA)
- CDA (Homologado Indra y Homologado Ci2)

4.4.5.1 Diagrama de despliegue CRC – Olimpia IT S.A.S.

En el siguiente diagrama se pueden visualizar los diferentes servidores que se encuentran desplegados en la infraestructura de este homologado, y su relación con los servicios externos e internos necesarios para cumplir con la misionalidad del CRC.

Ilustración 34. Diagrama de despliegue homologado CRC - Olimpia



Fuente: Elaboración propia Grow Data 2021

Para esta solución se cuenta con un servidor de fachada que realiza el puente entre el servidor web transaccional y el servidor de aplicación el cual gestiona y procesa la información de los servicios internos que son necesarios para soportar la operación. El servidor web transaccional gestiona y procesa la información con los servicios externos (servicio de pago, servicio de pines, servicio de consulta de las huellas, servicio de cargue de certificados generados), así mismo este servidor recibe la información generada por los equipos médicos desde los centros de reconocimiento a conductores.

El servidor de aplicaciones del SICOV del homologado Olimpia se conecta con el servidor de base de datos para almacenar la información generada por la operación. Igualmente se observan los diferentes protocolos de comunicación necesarios para la conexión entre estos componentes como lo son:

- TCP/IP: Conjunto de protocolos que permiten la comunicación efectiva entre los componentes del SICOV que se encuentran en una misma red.

- HTTPS: Protocolo que permite la transferencia de información utilizando el internet desde redes externas.

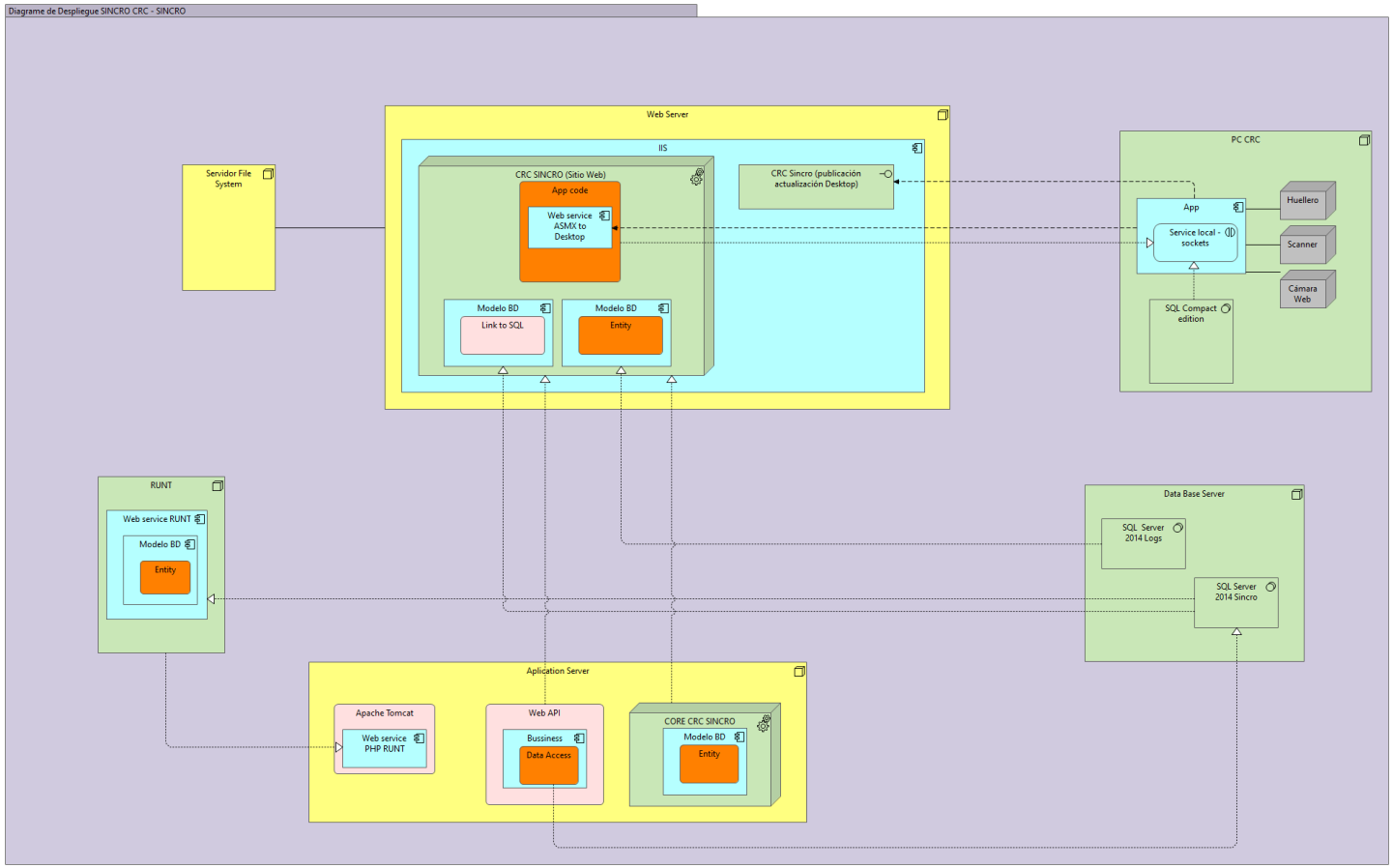
- VPN: Protocolo que permite la comunicación de los componentes del SICOV mediante una red privada, confiable y segura.

- Web Services (SOAP): Protocolo que permite la comunicación de los componentes del SICOV con las diferentes unidades externas (RNEC) por medio de intercambio de datos XML.

4.4.5.2 Diagrama de despliegue CRC – Consorcio SICOV CRC

En este diagrama se pueden visualizar los diferentes servidores que se encuentran desplegados en la infraestructura de este homologado para soportar la operación del SICOV para CRC

Ilustración 35. Diagrama de despliegue CRC – Consorcio SICOV CRC



Fuente: Elaboración propia Grow Data 2021

Para esta solución se cuenta con un servidor web el cual recibe la información generada por los equipos del CRC a través de una app code, y el cual contiene los elementos de conexión con el servidor de aplicación por medio de un web API y el servidor de base de datos a través de link to SQL.

Se visualiza la comunicación con el RUNT desde el servidor de base de datos mediante un web service a través de un entity.

El servidor de aplicación se comunica también con el RUNT mediante un web service SOAP basado en PHP desde un servidor de aplicaciones apache tomcat, y por medio de un web API con el servidor de base de datos.

Igualmente se observan los diferentes protocolos de comunicación necesarios para la conexión entre estos componentes como lo son:

- TCP/IP: Conjunto de protocolos que permiten la comunicación efectiva entre los componentes del SICOV que se encuentran en una misma red.

- HTTPS: Protocolo que permite la transferencia de información utilizando el internet desde redes externas.

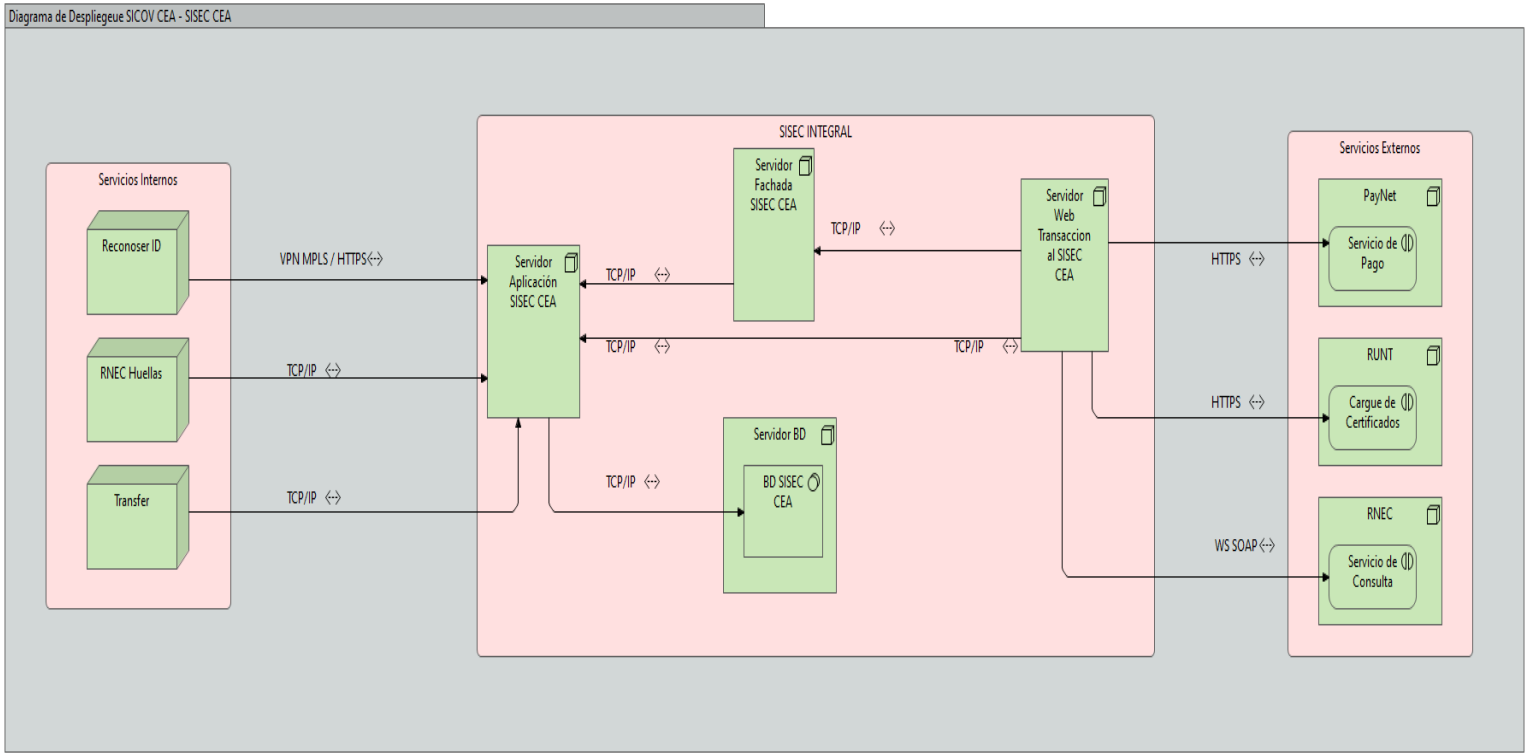
- VPN: Protocolo que permite la comunicación de los componentes del SICOV mediante una red privada, confiable y segura.

- Web Services (SOAP - PHP): Protocolo diseñado en lenguaje PHP que permite la comunicación de los componentes del servidor de aplicación con las diferentes unidades externas (RUNT) por medio de intercambio de datos.

4.4.5.3 Diagrama de despliegue CEA – Olimpia IT S.A.S.

En el siguiente diagrama se pueden visualizar los diferentes nodos (servidores) que se encuentran desplegados en la infraestructura de este homologado, y su relación con los servicios externos e internos necesarios para operar el SICOV CEA.

Ilustración 36. Diagrama de despliegue CEA - Olimpia



Fuente: Elaboración propia Grow Data 2021

Para esta solución se cuenta con un servidor de fachada que realiza el puente entre el servidor web transaccional y el servidor de aplicación el cual gestiona y procesa la información de los servicios internos que son necesarios para soportar la operación. El servidor web transaccional gestiona y procesa la información con los servicios externos (servicio de pago, servicio de consulta de las minucias, servicio de cargue de certificados generados). El servidor de aplicaciones se conecta con el servidor de base de datos para almacenar la información generada por la operación.

Igualmente se observan los diferentes protocolos de comunicación necesarios para la conexión entre estos componentes como lo son:

- TCP/IP: Conjunto de protocolos que permiten la comunicación efectiva entre los componentes del SICOV que se encuentran en una misma red.

- HTTPS: Protocolo que permite la transferencia de información utilizando el internet desde redes externas.

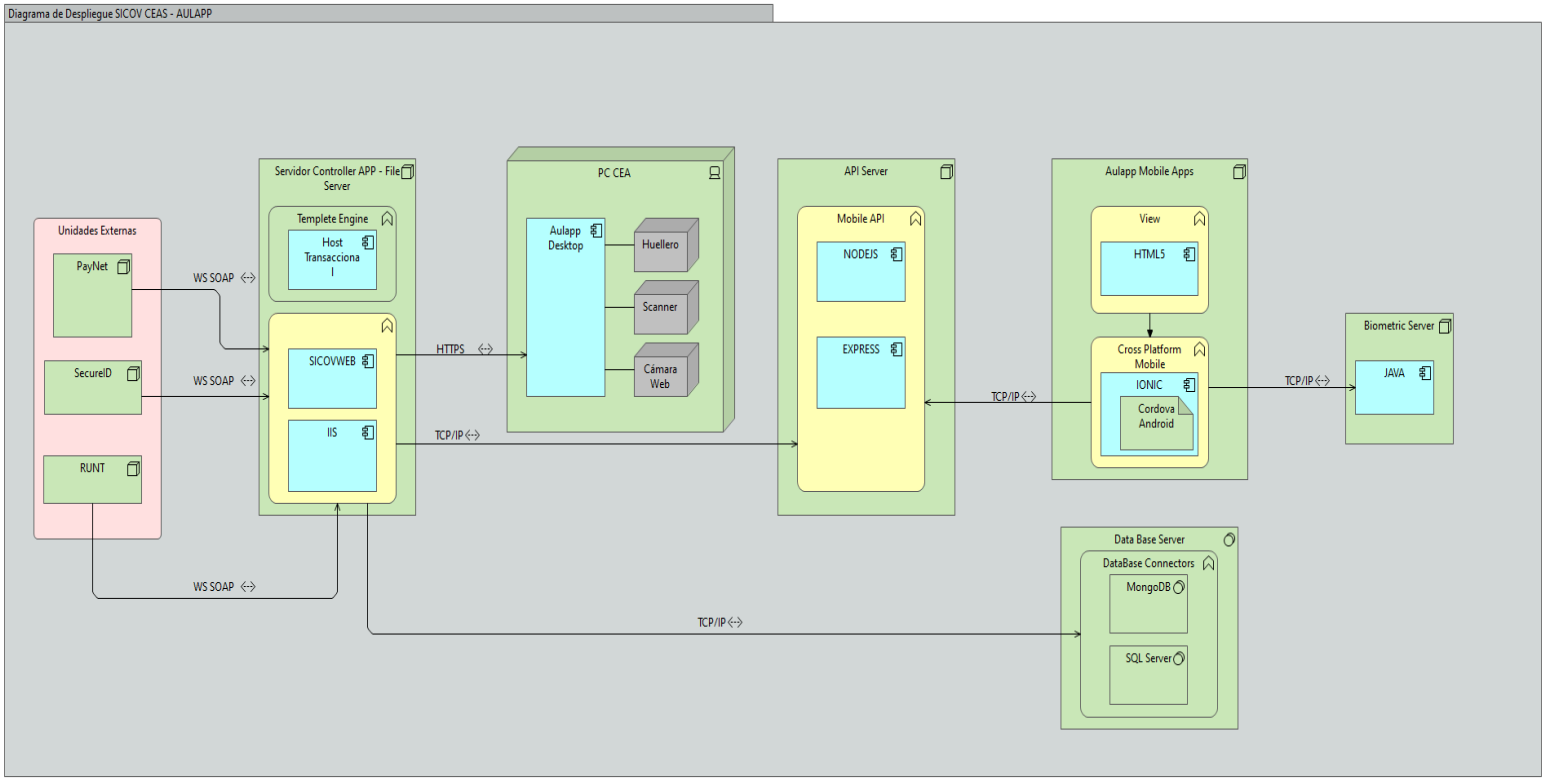
- VPN: Protocolo que permite la comunicación de los componentes del SICOV mediante una red privada, confiable y segura.

- Web Services (SOAP): Protocolo que permite la comunicación de los componentes del SICOV con las diferentes unidades externas (RNEC) por medio de intercambio de datos XML.

4.4.5.4 Diagrama de despliegue CEA – Consorcio SICOV CEA

En este diagrama se pueden visualizar los diferentes servidores que se encuentran desplegados en la infraestructura de este homologado,

Ilustración 37. Diagrama de despliegue CEA - SICOV CEA



Fuente: Elaboración propia Grow Data 2021

Para esta solución se cuenta con un servidor api que sincroniza al servidor web de la aplicación aulapp con el servidor de aplicación móvil aulapp mobile.

El servidor aulapp del homologado SICOV CEA recibe la información generada por la operación del centro de enseñanza automovilística mediante la aplicación aulapp desktop la cual se encuentra instalada localmente en los computadores del centro de enseñanza automovilística, así mismo intercambia información mediante web services con las diferentes unidades externas y también se conecta al servidor de base de datos del homologado SICOV CEA, el cual contiene un motor de base de datos mongoDB y un SQL server.

El servidor aulapp mobile se conecta con un servidor perteneciente al homologado SICOV CEA, el cual contiene las huellas de los ciudadanos que se obtienen de las clases prácticas.

Igualmente, la infraestructura actual utiliza diferentes protocolos de comunicación necesarios para la conexión entre sus componentes como lo son:

- TCP/IP: Conjunto de protocolos que permiten la comunicación efectiva entre los componentes del SICOV que se encuentran en una misma red.

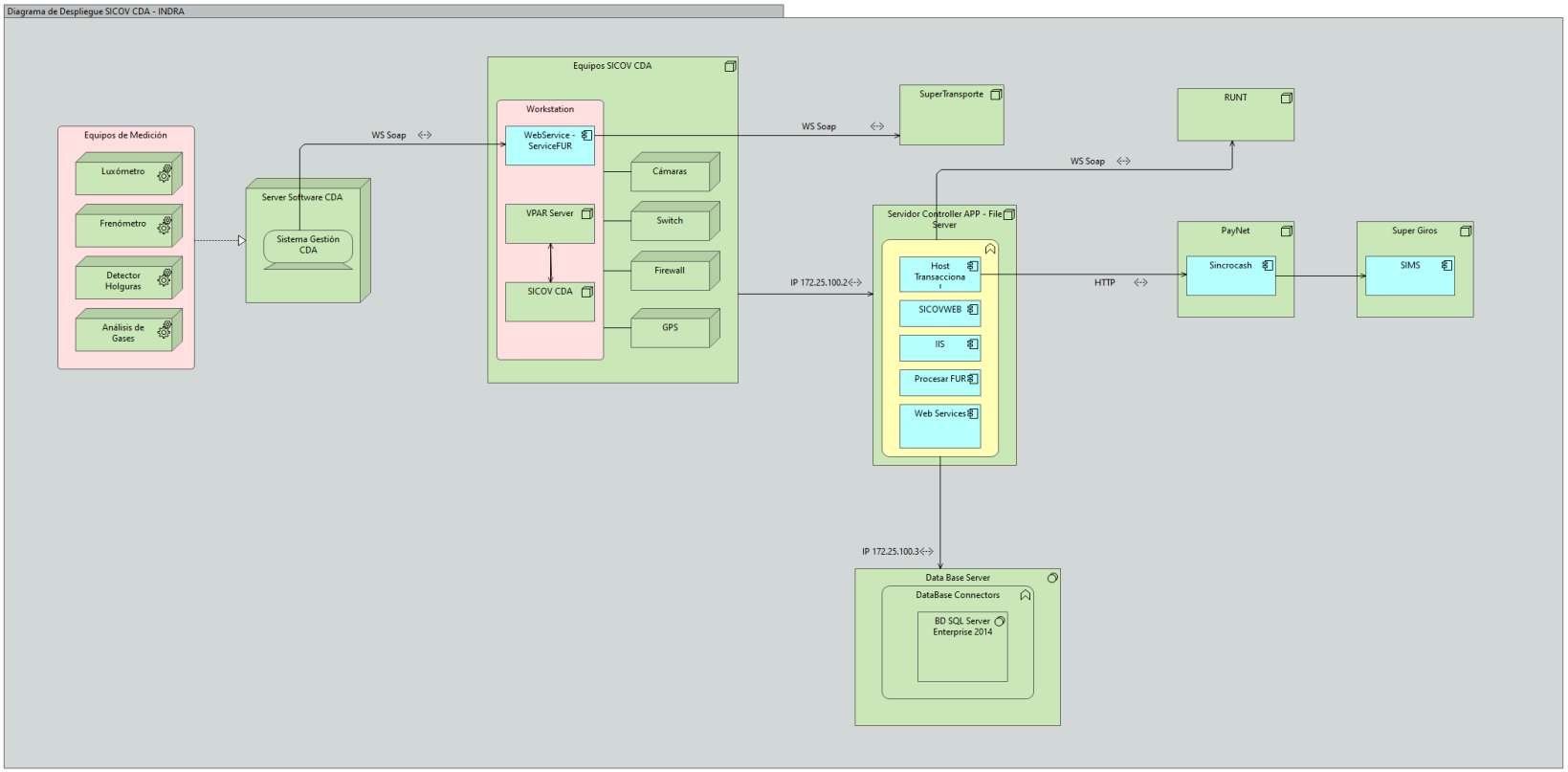
- HTTPS: Protocolo que permite la transferencia de información utilizando el internet desde redes externas.

- Web Services (SOAP): Protocolo que permite la comunicación de los componentes del SICOV con las diferentes unidades externas (RNEC) por medio de intercambio de datos XML.

4.4.5.5 Diagrama de despliegue CDA – Indra

En el siguiente diagrama se pueden visualizar los diferentes nodos (servidores) que se encuentran desplegados en la infraestructura de este homologado y de los equipos requeridos para la operación de los centros de diagnóstico automotor.

Ilustración 38. Diagrama de despliegue CDA - Indra



Fuente: Elaboración propia Grow Data 2021

Para esta solución se cuenta con un servidor controlador el cual recibe la información de los equipos que se encuentran instalados en los CDA y los cuales procesan la información de los FUR generados y de los videos realizados sobre la pista de inspección. A su vez el controlador realiza la comunicación con los aliados financieros (paynet y supergiros), así como la comunicación con el servidor de base de datos de la aplicación SICOV y el intercambio de información con el RUNT vía web services.

Los equipos de medición que generan los resultados sobre los vehículos en la pista de inspección envían estos resultados a un servidor propio del CDA el cual contiene el sistema de gestión, este a su vez envía estos resultados al Workstation el cual envía los FUR generados a la Supertransporte vía web services.

Igualmente se observan los diferentes protocolos de comunicación necesarios para la conexión entre estos componentes como lo son:

- TCP/IP: Conjunto de protocolos que permiten la comunicación efectiva entre los componentes del SICOV que se encuentran en una misma red.

- HTTPS: Protocolo que permite la transferencia de información utilizando el internet desde redes externas.

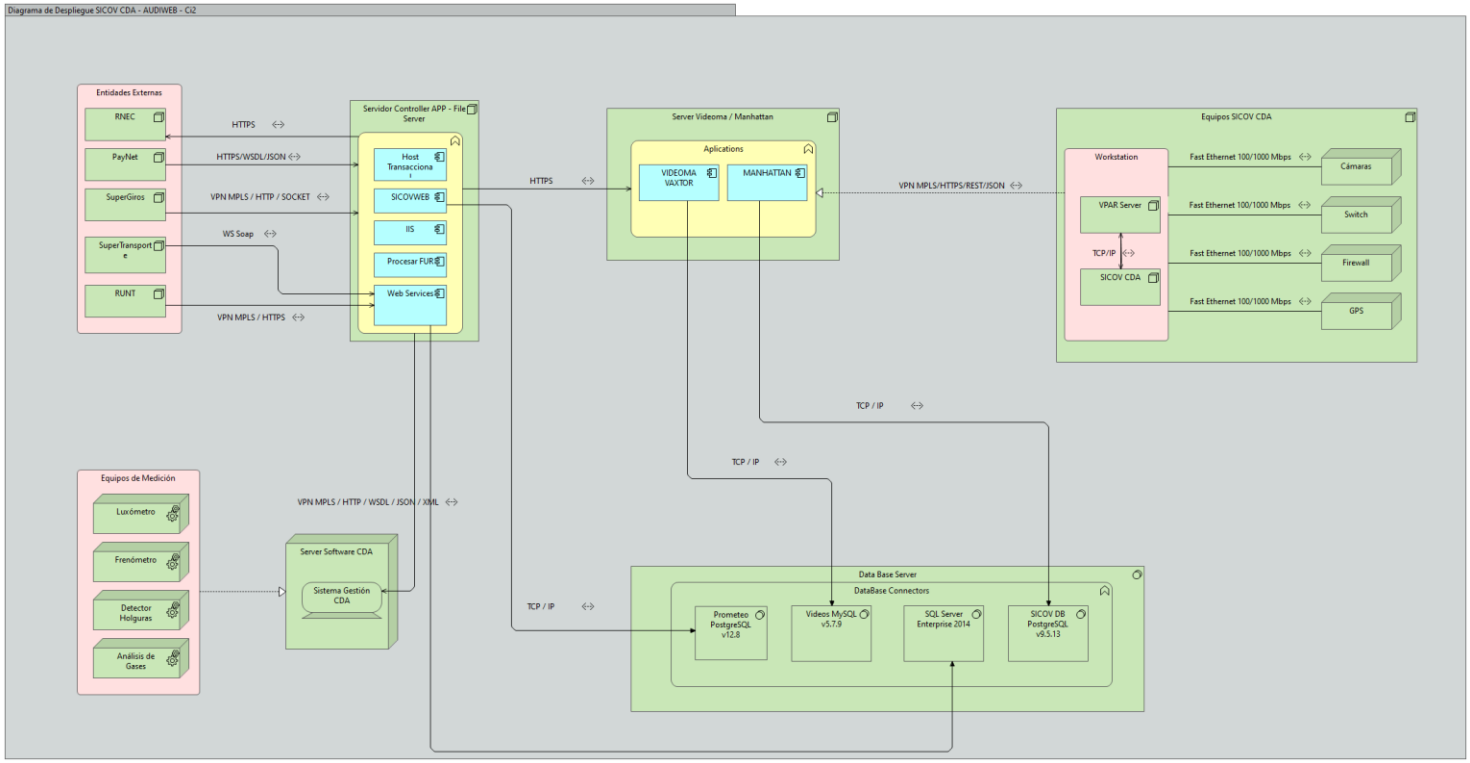
- Web Services (SOAP): Protocolo que permite la comunicación de los componentes del SICOV con las diferentes unidades externas (RNEC) por medio de intercambio de datos XML.

- VPN: Protocolo que permite la comunicación de los componentes del SICOV mediante una red privada, confiable y segura.

4.4.5.6 Diagrama de despliegue CDA – Ci2

En el siguiente diagrama se pueden visualizar los diferentes servidores (nodos) que se encuentran desplegados en la infraestructura de este homologado y de los equipos requeridos para la operación de los centros de diagnóstico automotor.

Ilustración 39. Diagrama de despliegue CDA - Ci2



Fuente: Elaboración propia Grow Data 2021

Para esta solución se puede visualizar que existe un servidor de aplicaciones ubicado en las instalaciones del CDA, el cual recibe los resultados de los equipos de medición y este a su vez los envía al servidor controlador de SICOV ubicado en el centro de datos del homologado a través de una conexión VPN.

El servidor controlador o servidor web interactúa con las entidades externas (Rnec, Paynet, Supergiros, Supertransporte y Runt) para el intercambio de información. Así mismo interactúa con el servidor de aplicaciones del aplicativo videoma y manhattan los cuales gestionan los videos de monitoreo generados en el CDA. Igualmente, el controlador se conecta al servidor de base de datos de Prometeo y al SQL server Enterprise 2014.

El servidor de aplicaciones se conecta con las bases de datos relacional Videos y SICOV DB. Al mismo tiempo que recibe la información del Workstation o servidor de aplicaciones que se encuentra ubicado en las instalaciones físicas del CDA, el cual contiene los aplicativos de vpar y SICOV CDA.

Igualmente se observan los diferentes protocolos de comunicación necesarios para la conexión entre estos componentes como lo son:

- TCP/IP: Conjunto de protocolos que permiten la comunicación efectiva entre los componentes del SICOV que se encuentran en una misma red.

- HTTPS: Protocolo que permite la transferencia de información utilizando el internet desde redes externas.

- Web Services (SOAP): Protocolo que permite la comunicación de los componentes del SICOV con las diferentes unidades externas (RNEC) por medio de intercambio de datos XML.

- VPN: Protocolo que permite la comunicación de los componentes del SICOV mediante una red privada, confiable y segura.

4.5 Arquitectura de seguridad actual

4.5.1 Contexto

En la actualidad, la información está definida como uno de los activos más valiosos y primordiales para cualquier tipo de organización, la cual, sólo tiene sentido cuando está disponible y es utilizada de forma íntegra, oportuna, responsable y segura. Esto implica, que es necesario que la entidad mantenga la apropiada gestión de los activos de información con el objetivo de asegurar y controlar su acceso, tratamiento y uso.

Ante esta evolución permanente a nivel tecnológico, la Superintendencia de Transporte ha trabajado proactivamente en la concepción, planeación e implementación de una estrategia integral de acuerdo con los lineamientos y metas del Gobierno Nacional, orientada al desarrollo de la política de Gobierno Digital, así como evidenciar el cumplimiento de los requisitos de seguridad para los Organismos de Apoyo al Tránsito. Por ello, se realizó la revisión del cumplimiento con los requisitos establecidos en las resoluciones 6246 de 2016, 13830 de 2014 y 60832 de 2016, 22180 y 14554 de 2017, las cuales establecen los anexos técnicos para la implementación del Sistema de Control y Vigilancia - SICOV, específicamente en temas de seguridad y privacidad de la información alineados con el Marco de Arquitectura Empresarial – MAE de MinTIC y las buenas prácticas internacionales como lo es la norma ISO 27001:2013 y los controles de seguridad de la información descritos en la norma ISO 27002:2013.

4.5.2 Marco normativo

A continuación, se detalla la normatividad aplicable al sistema SICOV en materia de seguridad y privacidad de la información.

TIPO DE DOCUMENTO	REQUISITO LEGAL	ENTIDAD EMISORA	DESCRIPCIÓN
Ley	1273 de 2009	El Congreso de la República	Por medio de la cual se modifica el Código Penal, se crea un nuevo bien jurídico tutelado - denominado "de la protección de la información y de los datos"- y se preservan integralmente los sistemas que utilicen las tecnologías de la información y las comunicaciones, entre otras disposiciones.

TIPO DE DOCUMENTO	REQUISITO LEGAL	ENTIDAD EMISORA	DESCRIPCIÓN
Ley	1581 de 2012	El Congreso de la República	Por la cual se dictan disposiciones generales para la protección de datos personales.
Ley	1712 de 2014	Congreso de la Republica	Por medio de la cual se crea la Ley de Transparencia y del Derecho de Acceso a la Información Pública Nacional y se dictan otras disposiciones.
Decreto	1377 de 2013	El Congreso de la República	Datos personales, Por el cual se reglamenta parcialmente la Ley 1581 de 2012.
Resolución	6246 de 2016	Superintendencia de Puertos y Transporte	Resolución: "Por la cual se expide el anexo técnico para la implementación del Sistema de Control y Vigilancia de que trata la Resolución 13829 de 2014".
Resolución	13830 de 2014	Superintendencia de Puertos y Transporte	Por la cual se expide al anexo técnico para la implementación de los Sistemas de Control y Vigilancia ordenado a través de la Resolución número 9304 del 24 de diciembre de 2012.
Resolución	60832 de 2016	Superintendencia de Puertos y Transporte	Por el cual se expide al anexo técnico para la implementación del Sistema de Control y Vigilancia de que trata la Resolución 05790 de 2016.

TIPO DE DOCUMENTO	REQUISITO LEGAL	ENTIDAD EMISORA	DESCRIPCIÓN
Resolución	22180 de 2017	Superintendencia de Puertos y Transporte	Por el cual se adiciona el numeral 2.6.2.2.14 al numeral de la Resolución 013830 del 23 de septiembre de 2014.
Resolución	14554 de 2017	Superintendencia de Puertos y Transporte	Por el cual se incorpora un numeral al anexo técnico adoptado mediante Resolución 013830 de 23 de septiembre de 2014.
Documento maestro	Documento maestro de 2019	Ministerio de Tecnologías de la Información y las Comunicaciones	MAE.G.GEN.01 – Documento Maestro del Modelo de Arquitectura Empresarial
Norma	NTC-ISO/IEC 27001:2013	Organización Internacional para la Estandarización (ISO)	Norma técnica colombiana - tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información (SGSI).
Norma	NTC-ISO/IEC 27002:2013	Organización Internacional para la Estandarización (ISO)	Norma técnica colombiana - tecnología de la información. Técnicas de seguridad. Código de prácticas para controles de seguridad de la información).

Tabla 9. Normatividad aplicable en Seguridad y privacidad de la información

4.5.3 Enfoque

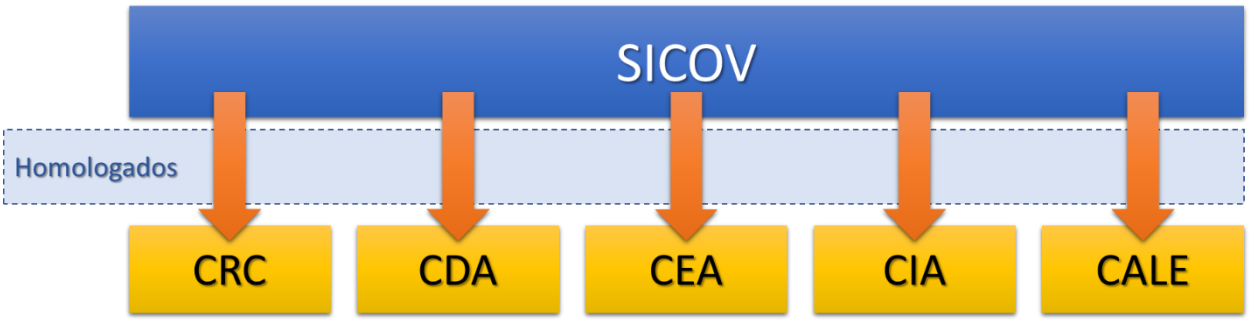
El presente dominio cubre la revisión e identificación del estado actual de arquitectura en seguridad, con base en los requisitos de las siguientes resoluciones:

- **Resolución 6246 de 2016**: *"Por la cual se expide el anexo técnico para la implementación del Sistema de Control y Vigilancia de que trata la Resolución 13829 de 2014"*.
- **Resolución 13830 de 2014**: *"Por la cual se expide al anexo técnico para la*

implementación de los Sistemas de Control y Vigilancia ordenado a través de la Resolución número 9304 del 24 de diciembre de 2012".

- **Resolución 60832 de 2016**: *"Por el cual se expide al anexo técnico para la implementación del Sistema de Control y Vigilancia de que trata la Resolución 05790 de 2016".*
- **Resolución 5786 de 2016: "***Por la cual se modifica el numeral 2.4.4, del anexo técnico adoptado mediante Resolución número 013830 del 23 de septiembre de 2014 y se adopta otra disposición".*
- **Resolución 22180 de 2017: "***Por el cual se adiciona el numeral 2.6.2.2.14 al numeral de la Resolución 013830 del 23 de septiembre de 2014"*
- **Resolución 14554 de 2017:** *"Por el cual se incorpora un numeral al anexo técnico adoptado mediante Resolución 013830 de 23 de septiembre de 2014"*
- **MAE.G.GEN.01** – Documento Maestro del Modelo de Arquitectura Empresarial (Seguridad)
- **Norma ISO 27001:2013**: Norma técnica colombiana - tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información (SGSI).
- **Norma ISO 27002:2013**: Norma Técnica Colombiana - Tecnología de la Información. Código de prácticas para controles de seguridad de la información.

Ilustración 40 - Alcance del diagnóstico



Fuente: Grow Data SAS, basado en las entrevistas con stakeholders

- Centros de Reconocimiento de Conductores – CRC
- Centros de Enseñanza Automovilística – CEA
- Centros Integrales de Atención - CIA
- Centros de Diagnóstico Automotor
- Centro de Apoyo Logístico de Evaluación - CALE

4.5.4 Estado actual (AS-IS)

4.5.4.1 Estado Actual de la Arquitectura de Seguridad

La identificación del estado actual de la entidad en lo relacionado con las buenas prácticas internacionales de las normas ISO/IEC 27001:2013 y la ISO/IEC 27002:2013, se realiza bajo una revisión de controles documentados, implementados, socializados y mejorados; mediante la aplicación de reuniones con el personal de seguridad de la información y la verificación documental existente suministrada por las partes interesadas y homologados (OAT´s).

Para identificar el nivel de madurez del estado actual a nivel de seguridad se utiliza la escala que se presenta en la Tabla 1010, la cual contiene los diferentes rangos y el nivel para clasificar los controles en seguridad de la información identificados en el sistema SICOV.

Nro.	NIVEL DE MADUREZ	LIMITE INFERIOR	LIMITE SUPERIOR
0	Inexistente	0	0
1	Inicial	1	20
2	Limitado	21	40
3	Definido	41	60
4	Gestionado	61	80
5	Optimizado	81	100

Tabla 10. Niveles de madurez

- **Definición de los Niveles de Madurez**
  - **Nivel 0 - Inexistente**: Carencia completa de cualquier proceso reconocible. La entidad no ha reconocido que existe un problema a resolver.
  - **Nivel 1 - Inicial**: Evidencia el reconocimiento de la entidad ante la existencia de problemas de gestión de seguridad y privacidad de la información que requieren ser resueltos. Sin embargo, no existen procesos establecidos; en su lugar, existen enfoques ad-hoc que tienden a ser aplicados de forma individual o caso por caso. El enfoque general hacia la administración es desorganizado.

- **Nivel 2 – Limitado**: Se han desarrollado los procesos hasta el punto en que se siguen procedimientos similares en diferentes áreas que realizan la misma tarea. No hay entrenamiento o comunicación formal de los procedimientos estándar, y se deja la responsabilidad al individuo. Existe un alto grado de confianza en el conocimiento de los individuos y, por lo tanto, los errores son muy probables.

- **Nivel 3 - Definido**: Los procedimientos se han estandarizado y documentado y se han difundido a través de entrenamiento. Sin embargo, se deja que el individuo decida utilizar estos procesos. Por lo tanto, es poco probable que se detecten desviaciones. Los procedimientos formalizan las prácticas existentes.

- **Nivel 4 - Gestionado**: Es posible monitorear y medir el cumplimiento de los procedimientos y tomar medidas cuando los procesos no estén trabajando de forma efectiva. Los procesos están bajo constante mejora y proporcionan buenas prácticas. Se llega a utilizar la automatización y herramientas.

- **Nivel 5 - Optimizado**: Los procesos se han refinado hasta un nivel de mejor práctica, se basan en los resultados de la mejora continua y en un modelo de madurez con la entidad. Las tecnologías de la información se usan de forma integrada para automatizar el flujo de trabajo, brindando herramientas para mejorar la calidad y la efectividad, haciendo que la entidad se adapte de manera rápida.

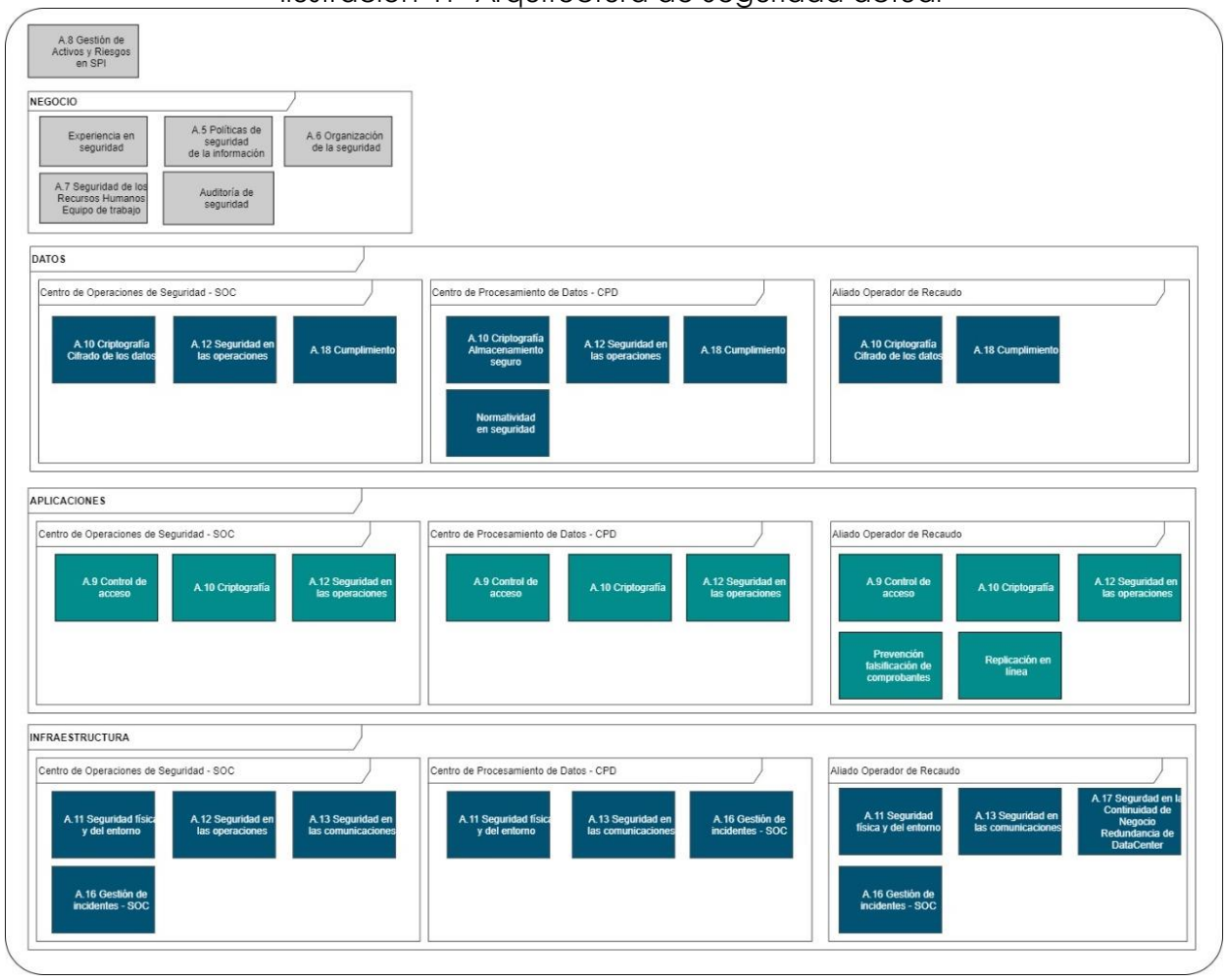
La identificación del estado actual y estado objetivo requiere que se realice una revisión específica de los requisitos de seguridad de la información, descritos en la normatividad vigente que deben dar cumplimiento los organismos de apoyo a las autoridades de tránsito (OAT) para la implementación del Sistema de Control y Vigilancia – SICOV. De acuerdo con lo anterior, se presenta de manera general los requisitos de seguridad de la información de acuerdo con las resoluciones vigentes:

- **Resolución 6246 de 2016**
- **Resolución 13830 de 2014**
- **Resolución 60832 de 2016**:
- **MAE.G.GEN.01** – Documento Maestro del Modelo de Arquitectura Empresarial (Seguridad)
- **Norma ISO 27001:2013**
- **Norma ISO 27002:2013**

Los requisitos de seguridad de la información establecidos en la normatividad pueden ser agrupados de acuerdo con las aplicaciones, datos, infraestructura y el negocio. De esta manera, es posible identificar los requisitos a cumplir por parte de los organismos de apoyo a las autoridades de tránsito en seguridad de la información en términos de SICOV y su operación en lo que respecta a experiencia, controles ambientales, controles de acceso (físico y lógicos), seguridad perimetral, redundancia en infraestructura tecnológica, servicios de SOC (Security Operation Center), seguridad en EndPoint, seguridad en los datos (cifrado) y en general, lo establecido en el MAE de MinTIC (a nivel de seguridad) y las buenas prácticas de seguridad de la información.

A continuación, se presenta el diagrama de requisitos alto nivel agrupados de acuerdo con los dominios de arquitectura empresarial.

Ilustración 41- Arquitectura de Seguridad actual



Fuente: Elaboración propia Grow Data - 2021

Como eje transversal a los dominios de arquitectura y en búsqueda de brindar mecanismos de seguridad y privacidad de la información se tiene la gestión de activos de información y riesgos en seguridad y privacidad de la información, siendo la columna vertebral de un modelo de seguridad. Esto implica que en todos los procesos se deberá identificar los activos y por tanto los riesgos que puedes afectar la confidencialidad, integridad y disponibilidad de SICOV.

A continuación, se presentan los resultados identificados durante la revisión de la información compartida, así como las reuniones con las partes interesadas a nivel de

arquitectura de seguridad de la información de acuerdo con la normatividad mencionada.

4.5.4.2 Avance general en seguridad y privacidad de la información

Durante la revisión del nivel de avance en seguridad y privacidad de la información de SICOV, se ha avanzado en el establecimiento e implementación de salvaguardas alineadas con los estándares nacionales e internacionales. Por ello, es prudente presentar los aspectos positivos identificados durante la realización de la arquitectura AS-IS de seguridad de SICOV.

A continuación, se mencionan los aspectos identificados:

- Se cuenta con la definición y aprobación formal de la política y políticas en seguridad de la información en un nivel avanzado de madurez en los homologados y en la SuperTransporte, pero no enfocados puntualmente al sistema SICOV.

- Se cuenta con infraestructura tecnológica robusta para la protección de los activos de información a nivel tecnológico que hacen parte del sistema SICOV.

- Se identifica la implementación de modelos de alta disponibilidad en los equipos de seguridad perimetral, comunicaciones y en general de la infraestructura crítica que soporta el sistema SICOV, lo que asegura la continuidad de las operaciones y conectividad del sistema en cada uno de los homologados.

- Se identificó que la gestión de usuarios, a nivel de registro y cancelación de cuentas de usuario está en un nivel de madurez gestionado. Por lo tanto, este procedimiento, esta implementado y evaluado por los homologados para un control eficaz de la gestión de usuarios que interactúan con SICOV.

- En cuanto a la seguridad física y del entorno, se tienen controles definidos e implementados en los organismos de apoyo al tránsito (CDA – CEA – CRC) y homologados entrevistados. Se cuenta con seguridad en perímetro, control de acceso, oficinas y recintos, áreas seguras, de carga y despacho.

- Se tienen definidos controles para la seguridad en redes y el control de acceso a esta. Esto mediante la definición e implementación de políticas para autenticación y existencia de políticas de seguridad perimetral.

- En referencia al servicio de correo electrónico, se identifica en un nivel óptimo al establecer un proceso de tercerización, donde se cuenta con niveles de seguridad avanzados por parte del proveedor.

- La gestión de incidentes de seguridad cuenta con el soporte técnico de implementación de herramientas tipo SIEM y procedimientos definidos e implementados para su reporte, atención y respuesta en caso de que se presenten.

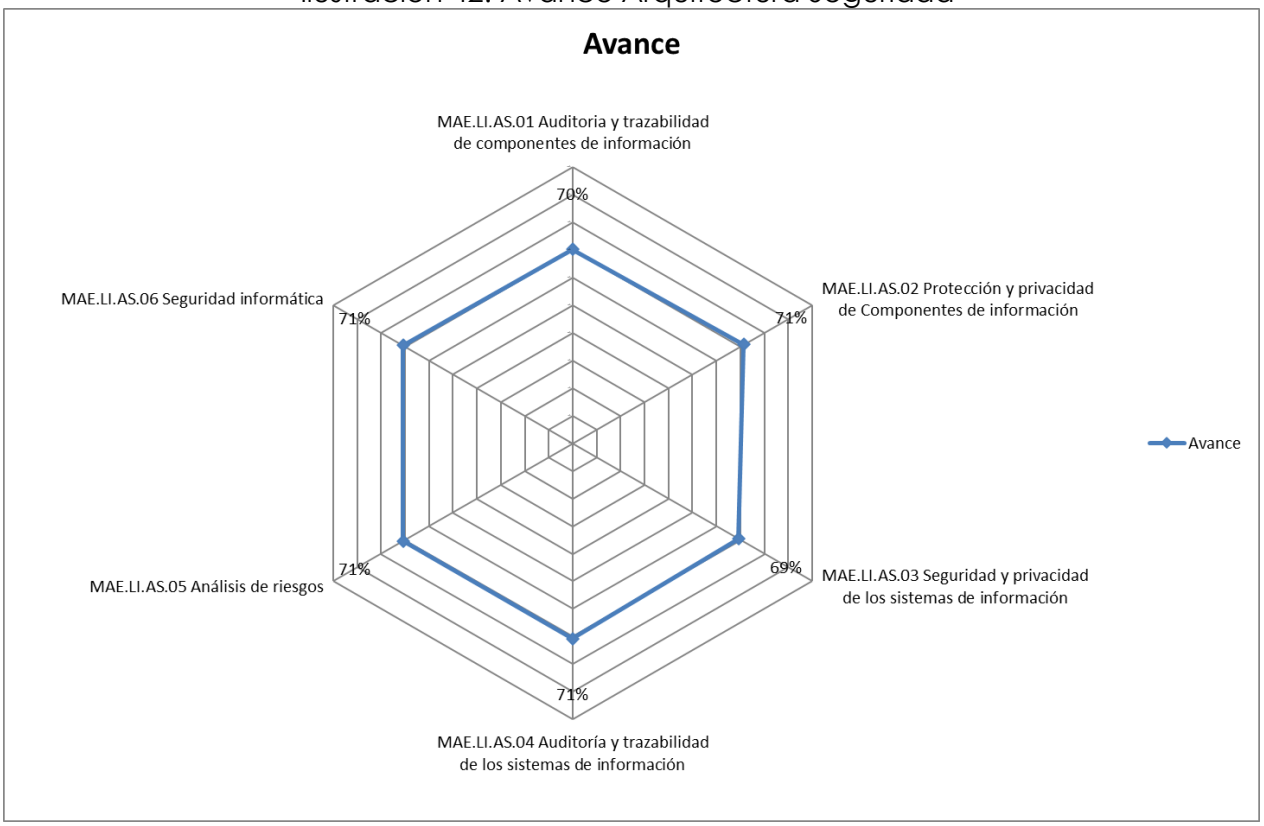
4.5.4.3 ARQUITECTURA DE SEGURIDAD AS - IS (DOMINIOS MAE)

Como resultado de la revisión del avance en seguridad y privacidad de la información en el sistema SICOV, se realizó una validación de cumplimiento con lo establecido en el Modelo de Arquitectura Empresarial (MAE) establecido por MinTIC.

Por lo anterior, se identificó que se han definido e implementado controles enfocados a cumplimiento de las diferentes líneas estratégicas de seguridad dentro de SICOV. Por ello, el resultado obtenido durante la revisión general alcanzó un puntaje de 71%.

En la Ilustración 42, se detalla el nivel de avance según las líneas estratégicas.

Ilustración 42. Avance Arquitectura Seguridad



Fuente: Elaboración propia Grow Data - 2021

A nivel transversal, existen controles del MSPI y la norma ISO 27001:2013, que hacen parte de las diferentes líneas estratégicas del MAE. Por lo tanto, a continuación, se presenta el nivel de madurez de los lineamientos de control que corresponden a todas las líneas estratégicas:

- Políticas de seguridad de la información en Los homologados, las cuales están definidas, documentas, y en proceso de implementación y revisión. Esto implica que se tiene un nivel de madurez **GESTIONADO.**

- La seguridad de las operaciones contiene controles en un nivel de avance **GESTIONADO**, en particular la gestión de cambios y la sincronización de relojes Los demás controles (Separación de las instalaciones de desarrollo, pruebas y operación, registro de eventos, protección de la información de registro y el registros del administrador y del operador), se encuentran en un nivel de

madurez inferior, lo que implica su especial atención para lograr mejorar el avance en los lineamientos de seguridad, según el MAE.

- En lo relacionado con la transferencia de información, para el dominio de seguridad en las comunicaciones el nivel de avance evidenciado corresponde a **GESTIONADO.** Estos controles corresponden a: políticas y procedimientos de transferencia de información, acuerdos sobre transferencia de información, seguridad en los mensajes electrónicos.

A continuación, se presenta el avance en los lineamientos de control que son particulares de cada línea estratégica:

4.5.4.3.1 MAE.LI.AS.01. Auditoría y trazabilidad de la información

Descripción del lineamiento:

La Dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe definir los criterios necesarios para asegurar la trazabilidad y auditoría sobre las acciones de creación, actualización, modificación o borrado de los Componentes de información. Estos mecanismos deben ser considerados en el proceso de gestión de dichos componentes. Los sistemas de información deben implementar los criterios de trazabilidad y auditoría definidos para los Componentes de información que maneja.

Estado actual (AS IS):

En lo relacionado con la auditoría y trazabilidad de la información, se identifica un avance del **70%**, lo que implica un nivel de madurez **GESTIONADO.** Realizando una revisión detallada, el nivel de avance de los dominios de control que se relacionan entre el MSPI a esta línea estratégica corresponden a:

- Gestión de activos, en el objetivo de control: Manejo de medios de soporte, identificando un nivel de madurez **DEFINIDO**.
- Seguridad física y del entorno, con un nivel de madurez **GESTIONADO**, esto, en lo relacionado con retiro de activos, seguridad de los equipos fuera de las instalaciones, disposición segura o reutilización de equipos.
- Gestión de incidentes de seguridad, en la recolección de evidencia, con un nivel de madurez **DEFINIDO**.
- Finalmente, en lo relacionado con cumplimiento, al identificar un nivel de madurez **GESTIONADO**.

4.5.4.3.2 MAE.LI.AS.02. Protección y privacidad de componentes de información

Descripción del lineamiento:

La Dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe incorporar, en los atributos de los Componentes de información, la información asociada con los responsables y políticas de la protección y privacidad de la información, conforme con la normativa de protección de datos de tipo personal y de acceso a la información pública.

Estado actual (AS IS):

Adicional a los anteriores dominios y controles mencionados de manera transversal, la protección y privacidad de componentes de información, cuenta con un avance del **71%**, lo que implica un nivel de madurez **GESTIONADO.**

De acuerdo con la revisión se identificó:

- Gestión de activos, específicamente en los controles de: Inventario de activos, propiedad de los activos, uso aceptable de los activos, devolución de activos, los cuales tiene un nivel de madurez **GESTIONADO**.
- La definición e implementación de políticas criptográficas y gestión de llaves, se identifica en un nivel **DEFINIDO**.
- Seguridad física y del entorno, con un nivel de madurez **GESTIONADO**, esto, en lo relacionado con retiro de activos, seguridad de los equipos fuera de las instalaciones, disposición segura o reutilización de equipos.
- Gestión de incidentes de seguridad, en la recolección de evidencia, con un nivel de madurez **GESTIONADO**.
- Finalmente, a nivel de cumplimiento legal o normativo, se identifica un nivel de madurez **GESTIONADO**, donde se cuenta con controles de la legislación aplicable, protección de datos personales y revisión independiente de cumplimiento de controles.

4.5.4.3.3 MAE.LI.AS.03. Seguridad y privacidad de los sistemas de información

Descripción del lineamiento:

La Dirección de Tecnologías y Sistemas de la Información debe analizar e incorporar aquellos componentes de seguridad y privacidad de la información que sean necesarios durante todas las fases del ciclo de vida de los sistemas de información.

Estado actual (AS IS):

En lo relacionado con la línea de seguridad y privacidad de los sistemas de información, se identificó un avance del **69%**, lo que corresponde a un nivel de madurez **GESTIONADO**.

De acuerdo con la revisión se identificó:

- Gestión de activos, específicamente en los controles de: Inventario de activos, propiedad de los activos, uso aceptable de los activos, devolución de activos, los cuales tiene un nivel de madurez GESTIONADO.
- La definición e implementación de políticas criptográficas y gestión de llaves, se identifica en un nivel DEFINIDO.
- La seguridad en las operaciones, en lo relacionado con la documentación de los procesos, gestión de cambios, gestión de la capacidad y la exigencia de separación de ambientes de desarrollo, pruebas y operación, software malicioso y copias de respaldo, se identifica un nivel de madurez GESTIONADO.
- La gestión de vulnerabilidades técnicas está en un nivel de madurez GESTIONADO, debido a que se cuenta con controles técnicos para aplicar parches de seguridad a nivel de sistemas operativos y restricciones implementadas para la instalación de software en los equipos de cómputo final.
- Se tiene controles de separación de redes por medio de VLANs implementadas. Esto lleva a un nivel de madurez GESTIONADO.
- Finalmente, los controles de seguridad de la información en las relaciones con los proveedores, la entidad se encuentra en un nivel DEFINIDO, esto ante la ausencia de implementación de la política de seguridad para relación con proveedores, el tratamiento de la seguridad dentro de los acuerdos con proveedores y controles que permitan garantizar la cadena de suministro de tecnología de información y comunicación.

4.5.4.3.4 MAE.LI.AS.04. Auditoría y trazabilidad de los sistemas de información

Descripción del lineamiento

La Dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe desarrollar mecanismos que aseguren el registro histórico de las acciones realizadas por los usuarios sobre los Sistemas de Información, manteniendo la trazabilidad y apoyando los procesos de auditoría.

Estado actual (AS IS):

De acuerdo con la línea de auditoría y trazabilidad en el sistema de información, se identificó un avance del **71%**, lo que corresponde a un nivel de madurez **GESTIONADO.** Se realizó la revisión con un enfoque en controles de seguridad como la gestión de accesos, gestión de logs o registros en el sistema de información, gestión de incidentes de seguridad, entre otros.

De acuerdo con la revisión se identificó:

- La seguridad en las operaciones, en lo relacionado con la documentación de los procesos, gestión de cambios, gestión de la capacidad y la exigencia de separación de ambientes de desarrollo, pruebas y operación, software malicioso y copias de respaldo, se identifica un nivel de madurez GESTIONADO.
- La gestión de vulnerabilidades técnicas está en un nivel de madurez GESTIONADO, debido a que se cuenta con controles técnicos para aplicar parches de seguridad a nivel de sistemas operativos y restricciones implementadas para la instalación de software en los equipos de cómputo final.
- Se tienen controles únicamente para la separación de redes por medio de VLANs implementadas. Esto lleva a un nivel de madurez GESTIONADO.

4.5.4.3.5 MAE.LI.AS.05. Análisis de riesgos

Descripción del lineamiento

La Dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe realizar el análisis y gestión de los riegos asociados a su infraestructura tecnológica, aplicaciones y componentes de información, haciendo énfasis en aquellos que puedan comprometer la seguridad de la información o que puedan afectar la prestación de los servicios de la entidad durante la ejecución de los ejercicios de arquitectura empresarial.

Estado actual (AS IS):

A nivel de la línea de análisis de riesgos, se identificó la implementación de metodologías de gestión de riesgos en seguridad de la información, seguimiento y control mediante aplicación de acciones o controles para llevarlos a niveles aceptables. EN general se identifica un avance del **71%**, lo que corresponde a un nivel de madurez **GESTIONADO.**

4.5.4.3.6 MAE.LI.AS.06. Seguridad informática

Descripción del lineamiento:

La Dirección de Tecnologías y Sistemas de la Información o quien haga sus veces debe diseñar los controles de seguridad informática para gestionar los riesgos que atenten contra la disponibilidad, integridad y confidencialidad de la información identificados durante la ejecución de los ejercicios de arquitectura empresarial.

Estado actual (AS IS):

A nivel de la línea de seguridad informática, se identificó un avance del **71%**, lo que corresponde a un nivel de madurez **GESTIONADO.** Este lineamiento cubre gran parte de los controles de seguridad informática, entre ellos, la seguridad a nivel de redes, seguridad en las operaciones, criptografía y gestión de llaves, gestión de control de acceso lógico, gestión de medios removibles, gestión de incidentes de seguridad entre otras. De acuerdo con a la revisión, se tiene un avance importante en la implementación de controles técnicos y administrativos en seguridad informática, aunque para llegar al nivel superior, se requiere completar las revisiones de cumplimiento, es decir la evaluación de los controles y aplicar mejoras u oportunidades de mejora a dichos controles.

Controles de seguridad en redes y comunicaciones:

SICOV cuenta con controles de seguridad definidos, implementados y gestionados desde la infraestructura de los homologados. Durante la revisión se evidenció que se tiene:

- Segmentación de redes, permitiendo tener separados el tráfico a nivel de red.
- Seguridad perimetral por medio de firewall y WAF a nivel de aplicaciones.
- Implementación de controles para la detección y prevención de intrusos, así como su gestión a nivel de monitoreo y seguimiento.
- Cifrado de la información en tránsito por medio de comunicaciones seguras.
- Control en la gestión de usuarios a nivel de red, reduciendo riesgos de acceso no autorizados o escalada de privilegios.

La seguridad a nivel de redes implementada tiene un nivel de madurez avanzado desde los homologados, donde se da cumplimiento no sólo a los controles de seguridad propuestos por la norma ISO 27001:2013, sino que se cuenta con controles (Anti DDoS, IDS/IPS) que permiten proteger las redes con mayor eficacia.

5 Justificación del enfoque arquitectónico

5.1 Modelo de Intención

5.1.1 Preocupaciones para la arquitectura empresarial de SICOV

Dentro de las actividades de establecimiento del proyecto y como parte del desarrollo de la Arquitectura Empresarial para SICOV, es necesario identificar las preocupaciones, intereses, expectativas y necesidades de los interesados, (de acuerdo con el marco de TOGAF) dado que esta información se deberá convertir en insumo para los lineamientos y aspectos por resolver con la Arquitectura Empresarial Objetivo (TO-BE).

Estas preocupaciones enfocan la construcción de una vista de diseño de la arquitectura como se muestra en la Ilustración 43.

Ilustración 43. Método de construcción de vistas a partir de las preocupaciones

Fuente: Elaboración propia Grow Data 2021

Las preocupaciones se han agrupado teniendo en cuenta los siguientes criterios:

- Resaltar las preocupaciones de la Superintendencia, teniendo en cuenta que es el principal interesado.

- Preocupaciones expresadas por otros interesados diferentes a la ST y que son comunes a los diferentes OAT (generales).
- Preocupaciones referidas a la relación con actores del sistema (Registraduría y ONAC).
- Preocupaciones específicas por tipo de OAT (CRC, CEA y CDA)

5.1.1.1.1 Superintendencia de Transporte

A continuación, se presentan las preocupaciones o intereses de la Supertransporte

- 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, por ejemplo, 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.
- Se requiere establecer mecanismos que permitan garantizar que el futuro concesionario del SICOV según el modelo de habilitación que defina la ST, no se quede con un software estático , sino que exista la obligatoriedad de incorporar en el tiempo mejoras y evolución en el sistema.
- Establecimiento de estándares y lineamientos para que independiente del proveedor del sistema, existan las mismas funcionalidades, reportes y validaciones en el SICOV.
- Fortalecimiento de los tiempos de atención de incidentes de actores externos como RUNT, operadores de recaudo y SICOV.
- Establecer o fortalecer los ANS entre el o los futuro(s) concesionarios y los OAT (entrega de tags, llamadas, requerimientos, entre otros), así como, entre el (los) futuro(s) concesionario(s)y la Superintendencia de Transporte
- No existe un marco de interoperabilidad 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 a las autoridades de tránsito (secretarias de tránsito), que establezca criterios para el intercambio seguro y efectivo de datos
- El reporte de datos, indicadores y estadísticas hacia la Supertransporte sobre la operación del SICOV debe realizarse a través de servicio web y debe mejorarse la oportunidad de entrega de información, ya que actualmente se recibe la información vía correo electrónico
- Establecer una hoja de ruta que permita la evolución de los sistemas de información que soportan el SICOV a los nuevos requerimientos normativos y tecnológicos que mejoren el funcionamiento y prestación de servicios de los OAT.

Estructurar un esquema de mejora continua que permita rápidamente incorporar nuevas tecnologías y mejores prácticas.

- El sistema SICOV debe 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.
- Integrar con el SICOV el software de gestión de los CDA. Adicionalmente, el software de gestión debería estandarizarse y que existan lineamientos mínimos para su desarrollo y funcionamiento.
- Que el SICOV proporcione a la Supertransporte información procesada: estadísticas básicas y alertas tempranas. Tener reportes en tiempo real de la operación de los SICOV
- El sistema SICOV es deseable que genere conjuntos de datos abiertos, y que sean publicarlos en el Portal de Datos Abiertos y definir estrategias para incentivar su uso
- Evolucionar la arquitectura de SICOV que permitan facilidad de evolucionar y escalar en el tiempo sin traumatismos.
- Afectaciones en la prestación del servicio por indisponibilidad de la plataforma tecnológica que soporta las soluciones del SICOV
- Afectaciones en la prestación del servicio por indisponibilidad de las plataformas de terceros con las que interopera la plataforma tecnológica como RUNT, Operadores de Recaudo, entre otros.
- El esquema provisto por la ST para el reporte de tarifas debe evolucionar a servicios web u otro y el cálculo de las tarifas no puede ser responsabilidad de la ST, la ST solo debe validar que las tarifas se están calculando acorde con la normatividad.

5.1.1.2 Generales

A continuación, se presentan las preocupaciones generales:

- Contar con una herramienta que permita evaluar los ANS de soporte y servicio del SICOV en sus diferentes niveles de interacción (STT – Homologados – OAT).
- Considerar la implementación de cursos teóricos virtuales haciendo uso de tecnología de punta.
- Mejorar la provisión de reportes y estadísticas por parte de los administradores o gestores del sistema (homologados, concesionarios u otros)a los OAT a fin de hacer un seguimiento proactivo y establecer procesos de mejora continua.

- Garantizar soluciones para Android e IOS si se hace uso de soluciones móviles.

- Definir el grado de cooperación e intercambio de información entre homologados o concesionarios en caso de que se mantenga un esquema con varios operadores.
- Mejora del proceso de conciliación y reporte de pagos a la ANSV.
- Garantizar la disponibilidad operativa del sistema SICOV.
- Disponer por parte de la Supertransporte y los homologados un mecanismo de alertas que garantice la consolidación de la información del SICOV, reportes sobre la totalidad de OAT del país (habilitados, suspendidos, con no conformidades pendientes, etc.) y disminuya la ilegalidad del proceso. Por ejemplo, que garantice que si un aspirante se presentó a un CRC y no fue aprobado no se presente en otro para obtener la aprobación; o que se realice la inscripción en el CEA sin haber realizado el proceso de aptitud en el CRC.
- Velar por la alineación tecnológica del SICOV para los CIA y CALE cuando se disponga su entrada en funcionamiento.
- En los CALE y con el apoyo de la ANSV (Agencia Nacional de Seguridad Vial) velar por la continua aplicabilidad y pertinencia de las preguntas para el examen teórico y lineamientos técnicos para el examen práctico de tal forma que se unifique el nivel de dificultad
- Definir y mantener actualizados los criterios de cálculo de capacidad por clase para el caso de los CEA, en especial si son virtuales, para ajustar los criterios en el CEA y CIA (proponer revisar el tema de la aplicación de la norma técnica NTC 4595 para educación no formal, y verificar la opción de la virtualidad en los procesos de formación).
- Hacer la validación de la identidad en inicio y fin de cada prueba dentro del proceso de CRC, pero no los intermedios.
- Biometría con la Registraduría y verificación de placa en la pista del CDA.
- No existe una estandarización de los catálogos de servicios entre el SICOV y los recaudadores para facilitar la integración y conciliación de los pagos.
- Mejorar los mecanismos de identificación biométrica con el fin de disminuir el ingreso al SICOV por excepción biométrica.

5.1.1.3 Registraduría

A continuación, se presentan las preocupaciones relacionadas con la RNEC:

- Establecer nuevas formas de validación de la identidad: reconocimiento facial, cédula digital, que pueden ser implementadas en los diferentes SICOV (en todas las etapas consumir el servicio de la Registraduría para validar identidad de la persona – evaluar costos y riesgos jurídicos).

5.1.1.4 Relación con ONAC

A continuación, se presentan las preocupaciones relacionadas con el ONAC:

- No hay una forma de validar, de manera automática, los certificados de conformidad de cada uno de los OAT (CRC, CDA, CEA, CIA) para que se encuentren habilitados en el SICOV. Los CDA y CRC deben contar con certificado de Acreditación emitido por el ONAC. Los CEA – CIA, deben contar con certificado de conformidad del servicio expedido por un Organismo Evaluador de la Conformidad-OEC acreditado por – el ONAC, bajo la norma ISO/IEC 17065 o la que la modifique, adicione o sustituya.
- Validación en línea y tiempo real del estado del certificado de acreditación para el caso de CRC y CDA (Activo, Suspendido, Retirado, Vencido). Se debe buscar evolucionar a un esquema de interoperabilidad.
- No son claros y homogéneos los criterios de validación de los auditores del ONAC.

5.1.1.5 CRC

A continuación, se presentan las preocupaciones relacionadas con los CRC:

- Definir esquemas eficientes de interoperabilidad con las Secretarías de Salud, en cuanto a la habilitación de los CRC para prestar los servicios de salud y con el MinSalud para tener actualizado el registro de profesionales de salud (interoperabilidad con sistema RETHUS y REP)
- Contar con diferentes medios de pago para las personas que no se encuentran bancarizadas, nuevas plataformas transaccionales como Nequi o Daviplata.
- Implementar procedimientos efectivos para integración de todos los equipos al sistema de gestión, controlando a la vez la recepción de la información mínima necesaria para realizar dicha labor.
- Mitigar las limitaciones en la impresión de los reportes de psicología. A través de la estandarización de acuerdo con los lineamientos técnicos de la resolución 217 de 2014 y sus modificatorias (funcionamiento y operación de los CRC). Por ser un documento con restricción de privacidad sólo debe tener la condición de "apto o no apto" – llegar a un acuerdo entre CRC para la forma como debe ser presentado el certificado y el fundamento jurídico por el cual se presenta de esa manera.
- Reducir la interacción de los profesionales con la evaluación. En la medida de lo posible tomar los resultados del dispositivo. Tener en cuenta los equipos de ofimática por donde se ingresa a los equipos de evaluación. No se controlan y no se sabe qué hay en los equipos y no se puede manejar la seguridad de los

SICOV. Son equipos que envían información, por ejemplo, se desarrolla la evaluación de psicología y es envía el resultado luego al SICOV.

- En la operación de los CRC no necesariamente hay una sola persona encargada del cargue de la información al RUNT (hqRUNT), aunque el usuario y clave que ejerce el rol de certificador es uno sólo, este manejo de usuario y clave por parte de diferentes personas puede alterar el proceso (manejo de usuarios dentro del sistema).
- Controlar el registro y causa de la repetición de los exámenes.
- Algunos CRC con varias sedes tienen centralizados los certificadores, es necesario garantizar la validación de la IP pública de cada sede y confirmar que se certifique en el lugar a través de mecanismos de GPS u otros.
- Falta de conocimiento del SICOV de las no conformidades identificadas por el ONAC que se gestionan en el CRC.

5.1.1.6 CEA

A continuación, se presentan las preocupaciones relacionadas con los CEA:

- Mantener la integridad del proceso al permitir el acceso a los cursos del CEA únicamente cuando se cuente con un certificado de aptitud del CRC correspondiente a la categoría de la licencia de conducir a solicitar
- Facilitar el servicio de integración al RUNT para el registro de las horas teórico-prácticas cursadas, en la actualidad es un proceso que se realiza de manera asincrónica y manual, lo que aumenta la introducción de errores en la digitación
- Se verifica identidad en inicio y fin de cada una de las clases y exámenes, pero no los intermedios, esto no permite validar que la persona que ingresa a la clase es la misma que asiste.
- Fortalecer el control al no permitir que, si el registro biométrico se realizó por huellas dactilares, el registro en las clases y los exámenes sea por excepción biométrica.
- Revisar alternativas para la implementación de tags o dispositivos no removibles para el seguimiento de rutas en las clases prácticas
- Revisar la posibilidad de inclusión de exámenes prácticos a través del apoyo de plataformas de simulación virtual.
- Reglamentar la realización de formación virtual, para el componente teórico: capacidad de las clases, reconocimiento facial para validar la asistencia.
- Validar el número de horas máximo de un instructor en el sistema SICOV de acuerdo con la norma, no solo entre OAT del mismo homologado sino de todo el sistema. Revisar la norma y si es pertinente aumentar el número de horas máximo.
- Validar que los instructores de los CEA estén registrados en RUNT y que estén asociados a un CEA especifico.

- Revisar el alcance de los consorcios u homologados frente a los centros de enseñanza frente a incumplimientos.
- Definir reglas claras para el proceso de traslado o migración de un OAT a otro homologado del sistema SICOV en caso de que se mantenga el esquema de habilitación de varios operadores.

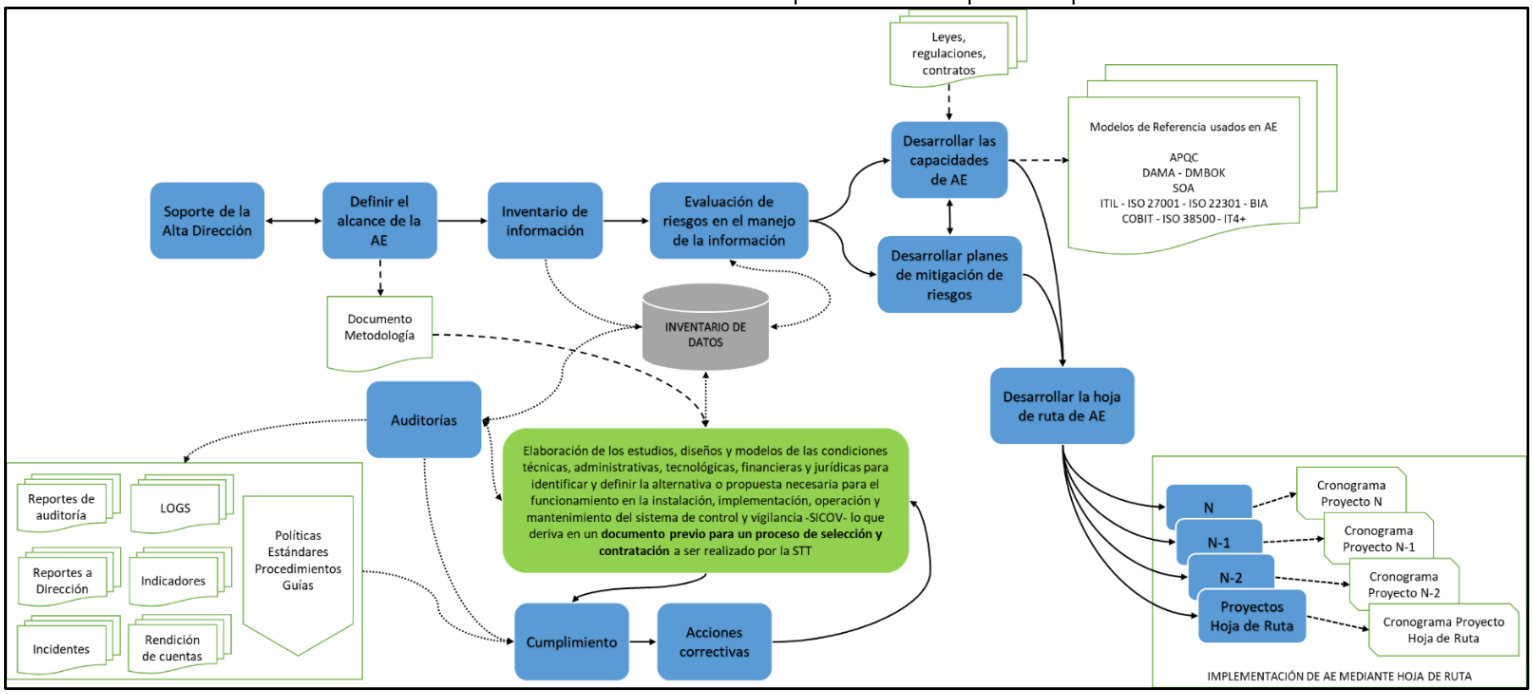
5.1.1.7 CDA

A continuación, se presentan las preocupaciones relacionadas con los CDA:

- Generar un mecanismo de integración con el RUNT que permita verificar que el vehículo a ser evaluado no tenga un registro o solicitud pendiente en otro CDA.
- Generar integración con el RUNT para validar los datos del vehículo antes de expedir el certificado de revisión técnico-mecánica y de gases.
- Aumentar la cobertura de la validación de identidad biométrica a todos los técnicos que hacen parte del proceso de revisión, no sólo del director técnico.
- Garantizar que el vehículo que entra a la pista sea el mismo que la recorre, identificando intentos de fraude a través de cambios de vehículos.

Una vez determinadas estas preocupaciones se construye la siguiente vista que permite dar alcance en el desarrollo de la arquitectura a estos elementos anteriormente mencionados.

Ilustración 44. Vista construida a partir de las preocupaciones



Fuente: Elaboración propia Grow Data 2021

5.2 Controles

5.2.1 Uso del sistema vial por vehículos automotores en Colombia

El sistema vial para vehículos automotores en Colombia es usado por los conductores y por los vehículos automotores que usan dichos conductores para transitar por todos los tipos de vías, las cuales son compartidas con peatones y por los demás usuarios que utilizan otro tipo de vehículos no automotores. El Estado debe garantizar la seguridad de todos los actores viales: pasajeros, peatones, transeúntes y conductores de vehículos automotores y no automotores.

Para garantizar la seguridad, los conductores, deben asegurar, de forma responsable que su participación en el sistema vial se realiza minimizando los factores de riesgo que puedan afectar la seguridad de los demás. Los conductores disponen de acceso a los servicios ofrecidos por los OAT, cuyo propósito fundamental es facilitarle la verificación del cumplimiento de los requisitos básicos que deben cumplir para conducir vehículos automotores en el sistema vial, a fin de reducir los índices de accidentalidad.

Inicialmente, los aspirantes a conductores o los conductores que desean obtener por primera vez su licencia de conducción, renovarla o recategorizarla , cuentan con el servicio ofrecido por los centros de reconocimiento de conductores (CRC), en los que el aspirante a conductor puede obtener el certificado que demuestra que cuenta con la aptitud física, mental y de coordinación motriz para conducir vehículos automotores en Colombia.

Adicionalmente, los aspirantes cuentan con el servicio ofrecido por los Centros de Enseñanza Automovilística (CEA) en los que pueden recibir la instrucción necesaria para obtener el certificado de capacitación en conducción de vehículos automotores. En el futuro, los aspirantes contarán también con el servicio de realización y ejecución de las pruebas teóricas y prácticas que estarán a cargo de los Centros de Apoyo Logístico de Evaluación (CALE), en los que, de forma especializada, se le permitirá al usuario demostrar su conocimiento teórico práctico para conducir de forma segura para sí mismo y para los demás.

De otra parte, los conductores cuentan con el servicio ofrecido por los Centros Integrales de Atención (CIA) en los que, cuando por cualquier motivo hayan cometido una infracción a las normas de tránsito, pueden recibir la instrucción teórica necesaria (reeducación) para tratar de evitar que a futuro vuelvan a cometer dichas infracciones.

Finalmente, los conductores o los propietarios de los vehículos automotores cuentan con el servicio ofrecido por los Centros de Diagnóstico automotor(CDA) en los que pueden

realizar la revisión técnico mecánica y de emisiones de contaminantes de dichos vehículos, en cumplimiento de las normas de seguridad viales y ambientales.

Es muy importante para el sistema en general, que los conductores asuman una posición absolutamente responsable, para determinar que pueden participar de forma segura en el uso de las vías. Un conductor responsable nunca pretenderá obtener un certificado de ninguna índole para conducir, si no cuenta con los requisitos que garanticen su seguridad y la de los demás.

En este sentido es indispensable para los aspirantes y los conductores, tener la absoluta certeza de que los servicios ofrecidos por los OAT, se ajustan estrictamente a los requerimientos establecidos en las normas reguladoras vigentes que les aplica y de esta forma puedan determinar con la mayor precisión posible, que podrán hacer uso del sistema vial de manera segura y que no representarán un posible peligro para sí mismos o los demás.

En este orden de ideas, debe existir un **mecanismo que permita prevenir la conducta inapropiada** de cualquier aspirante a conductor, conductor o propietario de vehículo automotor, que requiera de un certificado para obtener, renovar o recategorizar la licencia de conducción, sin ser merecedor a ello, o pretender no cumplir con las posibles restricciones que deberá observar para no ser un peligro para los demás o para que un vehículo que no cumple con las condiciones técnico mecánicas para transitar, reciba el certificado.

Algunos posibles **comportamientos irregulares de propietarios de vehículos, conductores o aspirantes a conductores** son los siguientes:

- Ofrecer incentivos al personal del OAT para que oculte o modifique los resultados obtenidos en la prestación del servicio al conductor o al vehículo automotor, permitiéndole obtener el certificado de forma irregular sin que refleje la realidad.
- Pretender ser sustituido o reemplazado por otra persona durante la prestación del servicio, para ocultar su condición que le impida obtener el certificado solicitado al OAT.
- Presentar un vehículo automotor diferente al que se debe revisar, (mediante acciones irregulares) para determinar su condición técnico mecánica y de emisión de contaminantes.

También debe existir un **mecanismo que permita garantizar al aspirante a conductor, al conductor o al propietario del vehículo automotor, que los servicios prestados por los OAT reflejan con precisión y exactitud su condición real** que es la base para determinar si puede conducir o no y en caso afirmativo, si deberá observar algún tipo de restricción.

Igualmente, se debe garantizar que los resultados de las revisiones de los vehículos automotores reflejan de forma precisa y exacta su condición real y que cualquier condición del vehículo que pueda significar un peligro potencial durante su uso, será identificado e informado al responsable para su ajuste y corrección antes de volver a ser utilizado en las vías.

Algunas posibles situaciones en la que los certificados expedidos por un OAT pudieran no reflejar la realidad del objeto a certificar son las siguientes:

- Los equipos técnicos de medición y apoyo para la evaluación de la persona o del vehículo automotor, arrojan resultados que no corresponden a la realidad bien sea por que
    - No están correctamente calibrados
    - Han sido alterados para que cambien el resultado obtenido
    - La transmisión de datos desde el equipo técnico de medición al sistema de información que registra los resultados es vulnerable y permite alteraciones de los resultados durante la transmisión
    - El equipo de medición no permite transmitir datos a un equipo de cómputo y estos deben ser transcritos de forma manual, susceptible de errores de digitación (voluntarios o involuntarios).
    - El sistema de información de apoyo para el registro y la evaluación de los resultados de las pruebas realizadas permite cambiar dichos resultados.
    - El sistema de información de apoyo para el registro y la evaluación de los resultados de las pruebas realizadas permite ignorar los resultados y registrar una evaluación diferente a la resultante de los resultados obtenidos.
- Los aspirantes inscritos a clases teóricas o prácticas se registran como asistentes al iniciar y terminar la clase, pero en realidad no ingresan al salón de clase o al vehículo en el que deben recibir la instrucción práctica.

Existen otras situaciones en la que los certificados expedidos por un OAT, si bien es cierto pueden reflejar la realidad del objeto evaluado, no cumplen con la totalidad de las normas exigidas:

- El OAT no cuenta con un registro vigente en el RUNT, es decir, no cumple con todos los requisitos exigidos para entrar a operar o para continuar operando
    - Un CRC no está debidamente inscrito en REPS
    - Un CEA no tiene reconocimiento o dicho reconocimiento se encuentra temporalmente suspendido de la autoridad de educación (secretaria)
    - Un CIA no está autorizado por el Instituto Nacional Penitenciario y Carcelario -INPEC para ofrecer el servicio de casa-cárcel o no cuenta con

convenio o contrato suscrito con la persona natural o jurídica que esté aprobada por el INPEC para prestar el servicio de casa-cárcel.
    - Un CDA no tiene autorización de la autoridad ambiental (secretaria – CAR)
    - Un CRC o CDA no cuenta con la acreditación del ONAC para expedir certificados o la misma se encuentra suspendida.
- El personal humano de OAT no cumple los requisitos exigidos
    - El personal de la salud no tiene registro ante RETHUS vigente al momento de realizar un examen con propósitos de certificación
    - Los instructores de CEA o CIA no cumplen el perfil exigido o han sido sancionados con infracciones de tránsito en el último año
    - Los instructores del CEA sobrepasan las horas máximas de instrucción semanal permitidas por norma
    - El personal técnico y directivo del CDA no cumplen el perfil exigido
- El personal del OAT que realiza las pruebas o emite los certificados, no coincide con los inscritos y autorizados, como resultados de suplantaciones
- Los vehículos usados para realizar clases prácticas de conducción o evaluaciones no son los autorizados al OAT.
- EL OAT no cumple con las restricciones de capacidad impuestas por el organismo certificador o de acreditación
- El OAT es suspendido parcial o totalmente para operar, pero esta situación no es registrada en el sistema
- Los vehículos usados para la enseñanza o evaluación en CEA o CALE no cumplen con las normas vigentes (RTM&EC, Seguro obligatorio, impuestos)

5.2.2 El control

5.2.2.1 Definición

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.

5.2.2.2 Objetivo del sistema vial

El principal objetivo que se debe alcanzar en un sistema vial para vehículos automotores, es garantizar que todos los participantes, tanto personas como vehículos automotores, cuentan con las condiciones necesarias para que el sistema sea seguro para todos los conductores y para todos los actores y bienes relacionados directamente con el sistema

vial vehicular como son, los peatones, los usuarios de las vías que utilizan vehículos no automotores como bicicletas, monopatines, patines, patinetas y similares.

5.2.2.3 Control en el sistema vial

En el sistema vial, el control es el ejercicio a través del cual las instituciones del sistema: MinTransporte, MinSalud, Superintendencia de Transporte, ONAC, ANSV, Secretarías de Educación, Secretarías de Salud, los OEC, controlan las actividades de los diferentes actores del sistema para detectar desviaciones en la ejecución de este y efectúan acciones correctivas. Por su parte, los conductores ejercen el autocontrol con el fin de mantener la seguridad en las vías.

Todos los actores del sistema, a través de sus actuaciones, propician el logro principal del objetivo de contar con un sistema lo más seguro posible para todos los participantes.

5.2.2.4 El autocontrol para los aspirantes, conductores y propietarios de vehículos automotores

El autocontrol para los aspirantes, conductores y propietarios de vehículos automotores es el ejercicio mediante el cual ellos garantizan el control de sus acciones, (tendientes a obtener certificados que demuestren que pueden participar en el sistema de tránsito sin convertirse en un riesgo potencial para los demás actores), detectan desviaciones y efectúan correctivos necesarios para propicie el logro del principal objetivo 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:

- Estadísticas de afectaciones físicas a personas (muertes, heridos) por accidentes de tránsito ocasionados por personas o vehículos a los que se les otorgó certificado en las condiciones mencionadas
- Sanciones económicas o penales recibidas por quienes fueron descubiertos realizando las acciones irregulares para obtener el certificado con acciones penales como por ejemplo la suplantación de identidad.

5.2.3 El papel del SICOV en el sistema de tránsito en Colombia.

Con el propósito de alcanzar un sistema vial lo más seguro posible para todos los actores, el SICOV debe estar orientado a garantizar que los OAT responden a las necesidades de los usuarios de obtener certificados conforme a la normatividad vigente. Esto implica que deban validar todos los requerimientos de cada uno de los actores del sistema vial, para que se puedan implementar las acciones de mejora, identificar las desviaciones y efectuar los correctivos necesarios.

En ese orden de ideas, el SICOV deberá monitorear y registrar todos los puntos de control en los procesos que afectan directamente las actividades de los OAT y con base en los registros, generar la información necesaria que permita efectuar los correctivos.

5.2.4 Instrumentos para el apoyo al control

- El inventario y descripción de los controles que debe poseer el sistema SICOV se encuentra en el Anexo:
    - Controles_Dominios
- Para la verificación del cumplimiento de los controles se definen listas de chequeo para de forma objetiva se realice la inspección / análisis / auditoría en donde se evidencie el cumplimiento de dichos controles:
    - Controles_Listado de Chequeo Requerimientos y Verificación -SICOV-CDA
    - Controles_Listado de Chequeo Requerimientos y Verificación SICOV-CEAS-CIAS
    - Controles_Listado de Chequeo Requerimientos y Verificación SICOV-CRCs

5.3 Principios

La definición de principios que hace TOGAF® dice:

"Los principios son reglas y pautas generales, destinadas a ser duraderas y rara vez enmendadas, que informan y respaldan la forma en que una organización se propone cumplir el desarrollo de la arquitectura empresarial. A su vez, los principios pueden ser solo un elemento en un conjunto estructurado de ideas que definen y guían colectivamente a la organización, desde la visión de arquitectura hacia los resultados de la arquitectura y sus artefactos".

A su vez, el Modelo de Arquitectura Empresarial (MAE) de MinTIC expone:

"Corresponden a reglas de alto nivel que direccionan los lineamientos definidos en el Modelo de Arquitectura Empresarial y se deben tener en cuenta para la toma de decisiones durante la ejecución de los ejercicios de Arquitectura Empresarial (AE) a nivel institucional, sectorial y territorial".

De acuerdo a la definición de TOGAF los principios de arquitectura:

- Están relacionados únicamente con el trabajo de arquitectura y los paquetes de trabajo que de este se desprenden.
- Gobiernan el proceso de arquitectura determinando el desarrollo de la arquitectura, su diseño y artefactos.
- Los principios de arquitectura son desarrollados por los arquitectos empresariales para guiar la toma de decisiones con respecto al diseño de la arquitectura y sus artefactos.

Adicionalmente, a pesar de estar identificados en el contexto del SICOV una serie de entidades privadas como prestadoras del servicio, se mantiene la naturaleza pública del SICOV por ser un servicio que se presta a nombre del Estado como lo establece el artículo 113 de la Constitución Política de Colombia.

Que el decreto 620 de mayo de 2020, establece que: ARTICULO 2.2.17.1.2. Ámbito de aplicación. Serán sujetos obligados a la aplicación del presente título, todos los organismos y entidades que conforman las ramas del Poder Público en sus distintos órdenes, sectores y niveles, los órganos autónomos e independientes del Estado, **y los particulares, cuando cumplan funciones administrativas o públicas.**

Teniendo en cuenta estos antecedentes, se utiliza en el lenguaje de definición de los principios el contexto público a pesar de que el servicio es prestado por privados. Esto se reafirma, por ejemplo, en la impresión de una tarjeta de conducción que dice "República de Colombia" a pesar de que los trámites son realizados en entidades de orden privado.

Bajo este mismo contexto, cuando nos referimos a entidad o funcionario se refiere a las entidades y funcionarios de las mismas, sean públicas y/o privadas involucradas en el funcionamiento del SICOV.

5.3.1 Negocio

PRINCIPIO DE NEGOCIO 1
Orientación a resultados
RACIONAL
Toma como eje de toda la gestión pública, las necesidades de los ciudadanos asociadas al propósito fundamental de la entidad, así como los resultados necesarios para su satisfacción.
IMPLICACIONES
Incumplimiento en la prestación de servicios al ciudadano con respecto a los trámites realizados en el SICOV.

PRINCIPIO DE NEGOCIO 2
Articulación interinstitucional
RACIONAL
Adelantar acciones de coordinación, cooperación y articulación con otras organizaciones del sector público o privado, del orden territorial, nacional o internacional, con el fin de formular e implementar estrategias para resolver las necesidades de los ciudadanos asociadas al propósito fundamental de la entidad.
IMPLICACIONES
Problemas de interoperabilidad entre las diferentes entidades involucradas en los trámites realizados por el SICOV que impactan al ciudadano.

PRINCIPIO DE NEGOCIO 3
Excelencia y calidad
RACIONAL
Lograr que a lo largo del tiempo, los atributos de los servicios o productos públicos, brindados a los grupos de interés , sean los mejores para satisfacer sus necesidades.
IMPLICACIONES
No contar con mecanismos de mejora asociados a la prestación de servicios al ciudadano que permitan mantener su calidad y tiempos de respuesta en el tiempo.

PRINCIPIO DE NEGOCIO 4
Aprendizaje continuo e innovación
RACIONAL
Mejora permanente, incorporando la innovación, aprovechando la creatividad de sus grupos internos y, en lo posible, de los grupos de interés de la entidad.
IMPLICACIONES
Dentro de la arquitectura se establecen mecanismos de actualización e innovación del SICOV. Actualización del sistema, reajustes de funciones, evolución de los servicios prestados. Omitir estas directrices conlleva al estancamiento del sistema, el deterioro de la prestación de servicios y una mala atención al ciudadano.

PRINCIPIO DE NEGOCIO 5
Integridad, transparencia y confianza
RACIONAL
Criterios de actuación de los servidores de la entidad y el deber hacia los ciudadanos.
IMPLICACIONES
Los servidores de la entidad deben cumplir en todo momento con las actuaciones establecidas en el marco regulatorio que determina el funcionamiento del SICOV y en concordancia con la atención al ciudadano.

PRINCIPIO DE NEGOCIO 6
Toma de decisiones basada en evidencia
RACIONAL
Capturar, analizar y usar información para la toma de decisiones que afectan la consecución de los resultados de la entidad.
IMPLICACIONES
Toda decisión debe minimizar los elementos de incertidumbre asociados a las múltiples variables de análisis. Para esto se deben determinar controles que permiten asegurar el ciclo de vida de la información y la generación de reportes asociados a la toma de decisiones. El incumplimiento de estos controles conlleva a toma de decisiones basadas en información insuficiente y un grado de incertidumbre no controlado.

PRINCIPIO DE NEGOCIO 7
La gestión de TI es responsabilidad de toda la entidad
RACIONAL
Todas las personas participan de una u otra forma en toma de decisiones que afectan el entorno de la gestión de TI y por consiguiente en la consecución de los objetivos estratégicos de la entidad.
IMPLICACIONES
Para operar en equipo, cada parte interesada o cliente deberá aceptar la responsabilidad de desarrollar el entorno de su información y cumplir con las políticas de gobierno de TI. Se requerirá el compromiso de recursos para implementar este principio.

PRINCIPIO DE NEGOCIO 8
Cumplimiento de la ley
RACIONAL
La política de la entidad y de sus funcionarios y contratistas, es cumplir con las leyes, políticas y regulaciones. Esto no impide realizar las gestiones necesarias que puedan conducir a cambios en las leyes y regulaciones.
IMPLICACIONES

PRINCIPIO DE NEGOCIO 8
Cumplimiento de la ley
La entidad debe ser consciente de cumplir con las leyes, regulaciones y políticas con respecto a la misión que debe cumplir y a su modelo de negocio. Educación y acceso a las reglas. La eficiencia, necesidad y sentido común no son los únicos factores de impulso. Los cambios en la ley y los cambios en las regulaciones pueden generar cambios en nuestros procesos o aplicaciones.

Tabla 11. Principios de negocio

5.3.2 Datos

PRINCIPIO DE INFORMACIÓN 1
La información es un activo y es responsabilidad de todos los funcionarios.
RACIONAL
Todas las entidades relacionadas con el sistema SICOV, deberán participar en la definición, administración y custodia y seguridad de la información a fin de garantizar el cumplimiento de la ley para lo cual fue creado el sistema SICOV. La administración de la información permitirá asegurar que tanto los procesos como los sistemas que los soporten garanticen la seguridad, integridad, confiabilidad, accesibilidad y disponibilidad de la información posibilitando con ello la mejora en el servicio y la toma de decisiones inteligente basada en la información. La correcta administración de la información facilita el control de riesgo y el cumplimiento de los compromisos regulatorios de acuerdo a sus competencias constitucionales y legales. La correcta administración de los datos de parte de los "responsables de proceso" facilitará los controles y procesamiento de la información que TI realiza por medio de la operación de toda la infraestructura tecnológica y permitirá la administración de las políticas de seguridad y acceso a la información.
IMPLICACIONES
Se deben definir con claridad las fronteras y responsables de los datos para cada proceso e identificar las relaciones existentes entre los mismos.

Existe la posibilidad que se generen cambios en los procesos, así como en la normativa y políticas relacionadas con la misma que deben ser revisados, analizados y modificados por los diferentes responsables. Existe la posibilidad que se generen requerimientos de negocio que impacten los sistemas de información, mismos que deberán ser modificados por la Gestión de TI. Es posible que se generen cambios en las políticas de acceso, seguridad y monitoreo de la información las cuales deberán ser asumidas por la Gestión de TI y por la seguridad de la Información.

PRINCIPIO DE INFORMACIÓN 2
La información debe ser compartida
RACIONAL
La información debe ser compartida y deberá posibilitar la colaboración entre los sistemas, servicios y procesos contribuyendo con ello al logro de los objetivos estratégicos. La información compartida entre los organismos permite brindar productos y servicios a los ciudadanos mediante mecanismos de oferta cruzada que posibilita tener una visión única del ciudadano. La información compartida es un factor para el logro del incremento de la eficiencia administrativa y la mejora en los procesos. La información compartida permite la toma eficiente de análisis y decisiones estratégicas para el negocio La información compartida permite generar de forma más eficiente la información para control interno, mitigación del riesgo y para brindar la información a los entes de control de forma oportuna.
IMPLICACIONES
Para que la información pueda ser compartida se requiere de mecanismos y tecnologías que posibiliten su integración.

PRINCIPIO DE INFORMACIÓN 3
La definición de los datos debe tener un vocabulario común en la entidad.
RACIONAL

Se debe definir un diccionario de datos que permita generar la meta data (estructuración, atributos y características acerca de los datos) que permita la administración de la información de la entidad de forma consistente e integrada. La existencia de un diccionario o glosario de información establecido en base a estándares permite la generación de estructuras de Administración de datos maestros (Master Data Management) que permite implementar la vista única ciudadanos, la oferta cruzada y la generación de información para cumplimiento, control interno y mitigación del riesgo. Para poder conformar un diccionario de datos estandarizado se requiere el compromiso de toda la entidad, así como la identificación de los responsables de la información.
IMPLICACIONES
La generación del diccionario de datos implica el compromiso de los funcionarios de la entidad, así como de la Gestión de TI y el Gobierno de Arquitectura Empresarial para mantenerlo actualizado. Se requiere conformar un repositorio que permita almacenar de forma centralizada el diccionario de datos. Se requiere brindar la orientación y capacitación a la entidad acerca de las metodologías, estrategias y herramientas para conformar el diccionario de datos.

PRINCIPIO DE INFORMACIÓN 4
La información debe apoyar la toma de decisiones a fin de maximizar la eficiencia y la eficacia en la entidad.
RACIONAL
Se debe emplear la información como un insumo para el desarrollo de reportes, consultas y generación de índices que permitan la toma de decisiones administrativas y financieras. La integración de la información y la generación de metadata son la base para generar índices e información que proporcionen los elementos para definir productos, servicios y estrategias de negocio enfocadas a aumentar la eficiencia y la eficacia.
IMPLICACIONES

La entidad debe definir los tipos de consultas, reportes e índices que se requieren generar para la toma de decisiones estratégicas. El área de TI debe apoyar el desarrollo o compra de aplicaciones que permitan generar los índices, consultas y reportes de conformidad con los requerimientos de los organismos de la Entidad.

PRINCIPIO DE INFORMACIÓN 5
La información debe ser accesible y confiable
RACIONAL
La información integrada de los ciudadanos y los productos y servicios de los mismos debe ser posible consultarla desde cualquiera de los canales y puntos de atención, y debe poseer la integridad y calidad que garanticen su confiabilidad. La consolidación de la información, su accesibilidad y la eliminación de la redundancia son condiciones requeridas para que la información pueda ser la base para mejorar la calidad del servicio a los ciudadanos e incrementar la confianza institucional. La toma de decisiones depende de la confiabilidad y oportunidad de la información. La disminución del riesgo en sus diferentes dimensiones depende en buena medida de la calidad y confiabilidad de la información. Una de las bases para el cumplimiento de los requerimientos de los entes de control es la información exacta, integrada y fácil de generar.
IMPLICACIONES
Para garantizar la accesibilidad de los datos en todos los canales y puntos de atención se requiere contar con un registro maestro de datos. Los procesos de calidad de datos son indispensables para que la información sea confiable, por ello se requiere que la entidad en su totalidad participe en este proceso definiendo la metadata e implementando los desarrollos con las herramientas tecnológicas de administración de información idóneas. Se requiere definir nuevos procesos y desarrollos o compras de aplicaciones que permitan que la información centralizada pueda ser consultada desde cualquiera de los puntos de atención al ciudadano.

PRINCIPIO DE INFORMACIÓN 6
Las políticas de seguridad, privacidad y gobernabilidad de la información deben ser consistentes en toda la entidad.
RACIONAL
La seguridad y administración de la información debe manejarse por medio de lineamientos, políticas, procesos, normativa y controles que garanticen que los datos estén seguros en la entidad y debe aplicar igual para todos los tipos de información. La seguridad y privacidad de la información son elementos clave para garantizar los requerimientos de cumplimiento generados por los entes de control. La gobernabilidad permite que se generen lineamientos que permitan garantizar el monitoreo, auditoría y calidad de la información y permita definir y controlar las responsabilidades de los diferentes actores organizacionales en el mantenimiento de los datos. La información segura y correctamente administrada potencia el cumplimiento de todos los principios de las diversas vistas.
IMPLICACIONES
El área encargada de la Gestión de TI en conjunto con las diferentes áreas de la entidad, todos alineados con el Gobierno de Arquitectura Empresarial, deberán generar los lineamientos, políticas y procedimientos que permitan garantizar la seguridad y privacidad de los datos. Deberán desarrollar los controles y el monitoreo requerido en las diversas aplicaciones de manera que se garantice la seguridad y privacidad de la información.

Tabla 12. Principios de Información

5.3.3 Sistemas Información

PRINCIPIO DE SISTEMAS DE INFORMACIÓN 1
Las aplicaciones deben ser independientes de las plataformas y éstas de cualquier marca o proveedor
RACIONAL
Se debe promover el uso de aplicaciones que puedan operar en diferentes plataformas que sigan estándares abiertos que eliminen o al menos minimicen la dependencia de un único proveedor.

PRINCIPIO DE SISTEMAS DE INFORMACIÓN 1
Las aplicaciones deben ser independientes de las plataformas y éstas de cualquier marca o proveedor
La eliminación de aplicaciones legadas que solo pueden operar en una única plataforma ayuda a disminuir el riesgo tecnológico de depender de un único o de un conjunto reducido de proveedores. El contar con aplicaciones que no dependen de una única plataforma facilita los procesos de integración de aplicaciones y datos lo cual favorece la prestación de productos y servicios a los ciudadanos. Los gastos de operación y mantenimiento pueden ser reducidos con el uso de aplicaciones y plataformas que no dependen de un solo proveedor.
IMPLICACIONES
La entidad deberá realizar los procesos de migración de aplicaciones legadas hacia otras que puedan funcionar independientemente de las plataformas de base de datos, sistemas operativos y de cualquier otro elemento de software. Se requiere la definición de estándares de arquitectura que faciliten el proceso de selección e implementación de sistemas que no dependan de una única plataforma y de plataformas que no dependan de un único proveedor. Se necesitan definir políticas, controles y procesos que garanticen la gobernabilidad de las nuevas plataformas mediante la aplicación de estándares como COBIT® e ITIL®.

PRINCIPIO DE SISTEMAS DE INFORMACIÓN 2
Se debe promover la reutilización
RACIONAL
Se debe implementar una arquitectura enfocada en la reutilización de componentes y servicios que sirvan como "piezas de lego" para conformar aplicaciones y acceso a los datos. Una arquitectura basada en componentes y servicios que puedan ser reutilizados facilita la administración y mantenimiento de las soluciones y permite responder de forma más rápida a los requerimientos.

El uso de un inventario de servicios y componentes permite implementar de forma más eficiente los procesos de negocio en las soluciones tecnológicas favoreciendo la alineación de los desarrollos tecnológicos con los servicios y productos de la entidad.
IMPLICACIONES
Se requiere realizar un análisis del inventario de aplicaciones de la organización a fin de generar un plan de migración que permita ir de forma incremental adoptando arquitecturas que promuevan la reutilización como las arquitecturas orientadas a servicios y componentes (SOA). Es necesario definir estándares tecnológicos que soporten los procesos de reutilización. Se requiere asignar recurso humano adecuado para implementar el proceso de migración hacia arquitecturas orientadas a servicios. Es necesario definir procesos y estructuras de gobernabilidad de los servicios y componentes que soporten la reutilización. Es probable que se requiera adquirir herramientas que posibiliten la migración hacia arquitecturas orientadas a servicios.

PRINCIPIO DE SISTEMAS DE INFORMACIÓN 3
Todos los sistemas de información deben poseer controles de auditoría y monitoreo en las aplicaciones
RACIONAL
Todos los sistemas que procesen información deben poseer capacidades de auditoría y monitoreo en las transacciones que procesen información crítica. El mantenimiento de bitácoras que registren los cambios realizados en la información crítica procesada por las aplicaciones es necesario para la gestión de riesgo y para el control interno. Las facilidades de monitoreo y control de los datos permiten contar con información e indicadores necesarios para definir acuerdos de nivel de servicio tanto técnicos como de negocio que permitan definir políticas de mejora de servicio al ciudadano. Los controles, monitoreo y bitácora de cambios permiten mantener los estándares de seguridad de las aplicaciones y los datos.
IMPLICACIONES

Deben generarse estándares, políticas y procedimientos que definan las características de las pistas de auditoría y monitoreo que deberán implementarse en las aplicaciones críticas tanto en las existentes como en las nuevas adquisiciones. Se debe realizar un análisis de las aplicaciones e infraestructura existente a fin de generar un plan de trabajo que permita implementar los controles de auditoría y monitoreo que se necesiten. Es necesario asignar los recursos de TI y de negocio que se requieran para implementar los controles de auditoría y monitoreo en las aplicaciones.

PRINCIPIO DE SISTEMAS DE INFORMACIÓN 4
La arquitectura de las aplicaciones debe soportar el acceso seguro a los datos y transacciones.
RACIONAL
Todos los sistemas deberán poseer mecanismos de seguridad que aseguren la protección contra ingresos no autorizados. La seguridad en el acceso a las aplicaciones en línea, tanto a los datos como a las transacciones debe evitar el acceso no autorizado, así como el manejo de privilegios de acceso de conformidad con las funciones del usuario que ingresa. El acceso a la información masiva que se genera para fines internos o para informar a los entes de control debe poseer controles de seguridad y de inscripción que permitan mantener la confidencialidad. Los controles de acceso deben estar alineados con los principios de seguridad y acceso a los datos, así como con la generación de facilidades de auditoría y control. La seguridad en el acceso a las aplicaciones permite el logro de los objetivos estratégicos relacionados con el control interno y la mitigación del riesgo.
IMPLICACIONES

PRINCIPIO DE SISTEMAS DE INFORMACIÓN 4
La arquitectura de las aplicaciones debe soportar el acceso seguro a los datos y transacciones.
La entidad debe revisar los controles de seguridad y accesos de todas las aplicaciones existentes a fin de implementar mecanismos estándar de seguridad en todos los sistemas. Deben generarse estándares de seguridad de acceso para las diversas capas de la arquitectura, desde el acceso a los canales y puntos de atención al ciudadano, pasando por las aplicaciones, servicios y componentes de negocio y finalmente hasta los accesos de las fuentes de datos. Estos estándares deberán aplicar tanto a los sistemas ya existentes como a los nuevos que la entidad adquiera o desarrolle. Deben diseñarse controles y estándares para manejar la seguridad en el acceso de aplicaciones de aliados de negocio como las entidades descentralizadas o grupos de interés.

PRINCIPIO DE SISTEMAS DE INFORMACIÓN 5
Se debe promover la innovación
RACIONAL
Se debe implementar una estrategia y arquitectura tecnológica enfocada en la innovación abierta institucional, para la mejora de servicios apoyados en el uso intensivo de las TIC. Una estrategia de innovación apoyada en el uso intensivo de las TIC permite responder de forma más rápida y eficiente a los requerimientos institucionales, de los ciudadanos y entidades relacionadas. Las TIC se convierten en el centro de desarrollo de estrategias orientadas a la mejora continua de los servicios institucionales y la mejora de la satisfacción del ciudadano. Las plataformas de trabajo colaborativo para la interacción con el ciudadano permiten la innovación abierta en el desarrollo de política pública para la resolución de problemas prioritarios.
IMPLICACIONES

Se debe establecer un sistema de gestión de la innovación abierta alineada con las prácticas de Arquitectura Empresarial, que facilite la generación de valor para la institución y el ciudadano. Se deben integrar plataformas de trabajo colaborativo para la innovación abierta.

Tabla 13. Principios de Sistemas de Información

5.3.4 Tecnología

PRINCIPIO DE TECNOLOGÍA 1
Cambios basados en Requerimientos
RACIONAL
Los cambios a nivel de infraestructura deberán gestionarse a través con un RFC (Request For Change) los cuales, dentro de los criterios de aprobación, tendrán prioridad las solicitudes que atiendan de forma directa una necesidad, falla o plan de mejoramiento Este principio busca que los cambios de la infraestructura estén en su mayoría enfocados a atender las necesidades de la entidad. Esto de igual forma busca minimizar cambios que nazcan de iniciativas aisladas, que no apoyen objetivos del área de TI o que los beneficios del requerimiento no sean claros ni medibles. Con esto se busca aumentar la efectividad del área, al enfocar los esfuerzos del personal y dedicar los principales recursos de TI a las iniciativas estratégicas y que realmente apoyen el cumplimiento de los objetivos del área. En otro sentido, se busca ganar efectividad en TI al tener eficientes esquemas de análisis de los cambios para evitar efectos negativos no previstos en la implementación de cambios
IMPLICACIONES
Optimización del procedimiento de gestión de cambios y dentro del procedimiento de evaluación del requerimiento, profundizar el análisis del impacto basándose en la arquitectura de la infraestructura. Las aprobaciones de cambios deberán tener como principal parámetro, la alineación del requerimiento a las necesidades de la entidad. Los requerimientos de cambios, de igual forma deberán estar alineados con los principios de los otros dominios.

PRINCIPIO DE TECNOLOGÍA 2
Control de la diversidad técnica y de proveedores
RACIONAL

PRINCIPIO DE TECNOLOGÍA 2
Control de la diversidad técnica y de proveedores
La diversidad de plataformas y de tecnologías a nivel de infraestructura es controlada para minimizar la complejidad en la administración, así como la conectividad entre estas diferentes plataformas. La gestión de proveedores debe enfocarse a tener la menor cantidad de proveedores posibles a fin de cumplir con los procesos / funciones que requieren de apoyo de terceros, pero a un riesgo controlado El adquirir infraestructura de diferentes tecnologías, plataformas, fabricantes eleva la dificultad en su administración e integración con el resto de los elementos de la infraestructura. Esto conlleva aumento en los costos en la gestión de esta infraestructura y en los riesgos en su operación. No es posible definir un estándar a nivel de infraestructura, cuando la diversidad de plataformas es la generalidad
IMPLICACIONES
Se debe definir unas políticas y estándares a nivel de infraestructura que regule el crecimiento y adquisición de elementos de la infraestructura. Las decisiones para la implementación de nuevos elementos de infraestructura deberán ser analizadas bajo los estándares definidos. Mientras que sea posible, se deberán asignar nuevas actividades a proveedores ya existentes. Por esto, en todo momento se deberá evaluar el desempeño de los proveedores y los servicios que están prestando para identificar cuáles de estos deberán ser reemplazados y cuales podrán asumir nuevas cargas. Dentro del proceso de selección de nuevo software y plataformas, el área de TI y en concreto, los grupos de administración deberán ser los que tengan el mayor peso en la decisión.

PRINCIPIO DE TECNOLOGÍA 3
Interoperabilidad
RACIONAL
El software y el hardware que se adquiera deberán estar alineados con estándares y lineamientos que promuevan la interoperabilidad de datos, aplicaciones e infraestructura al interior de la entidad y con entidades externas que así lo requieran. Infraestructura que promueva y facilite la interoperabilidad, facilita el trabajo cooperativo, la unión de procesos / procedimientos con un bajo esfuerzo y con una alta efectividad. Se optimizan los costos asociados y la cantidad de personal involucrado en la interconexión de áreas / entidades.
IMPLICACIONES
Es necesario seguir los estándares y lineamientos que se hayan definido en términos de infraestructura e interoperabilidad así se genere un requerimiento por parte del negocio. Los estándares y lineamientos definidos deberán ser revisados periódicamente dado que los avances de tecnología pueden volver obsoletos las definiciones establecidas. Las plataformas de tecnología deberán ser identificadas y documentadas en detalle.

PRINCIPIO DE TECNOLOGÍA 4
Continuidad de Negocio / Continuidad de TI
RACIONAL

La continuidad de los servicios de TI deberá garantizarse y, por ende, se deberán exceder los compromisos que a nivel de disponibilidad se hayan establecido. La operación de la entidad y en concreto la disponibilidad de los servicios de TI que soporten procesos misionales, deberá garantizarse incluso cuando se presenten fallas críticas. Dada la creciente dependencia de la entidad sobre los servicios de TI, estos deberán garantizar su disponibilidad, confiabilidad y desempeño. Las fallas de hardware, fallas de software, desastres naturales, ataques a nivel de seguridad no deberán impactar la disponibilidad de los servicios de TI.
IMPLICACIONES
El apoyo de la infraestructura (software y hardware) sobre los procesos de la entidad genera una alta dependencia sobre esta tecnología. Es por esto que se deberán generar planes de contingencia que apoyen la restauración de los servicios de TI en caso de fallas críticas. Es necesario realizar un análisis de impacto sobre el negocio en caso de presentarse fallas críticas para determinar la prioridad en los servicios de TI, y de esta forma diseñar los planes de contingencia. Es necesario alinear los planes de contingencia con la gestión de riesgos de la entidad. Antes de diseñar un plan de contingencia, se debe implementar estrategias que, a nivel de arquitectura de infraestructura, creen plataformas resilientes y de alta disponibilidad.

PRINCIPIO DE TECNOLOGÍA 5
Cumplimiento con estándares y políticas
RACIONAL

PRINCIPIO DE TECNOLOGÍA 5
Cumplimiento con estándares y políticas
La entidad y en especial, el área de tecnología, deberán alinearse y procurar total cumplimiento a los estándares y lineamientos que a nivel de infraestructura se hayan definido. La entidad deberá adoptar todo marco normativo y estándar que por sector se defina a nivel de infraestructura tecnológica. La entidad, deberá seguir los lineamientos que a nivel interno y de gestión de T.I. se hayan definido. El seguimiento de éstas, derivarán en facilidad en la gestión de la infraestructura, óptima administración y mejor confiabilidad.
IMPLICACIONES
Las excepciones a las reglas definidas deberán tener justificaciones de muy alto nivel y en primera instancia, se deberán negar todos los requerimientos que no estén alineados con los estándares y lineamientos establecidos. Si se debe aprobar la excepción a una regla, se deberá analizar si de igual forma se deberá actualizar la regla. Se debe analizar periódicamente la pertinencia y nivel de actualización de los estándares para asegurar que en todo momento estos ofrezcan la utilidad y control esperado a la gestión de TI.

PRINCIPIO DE TECNOLOGÍA 6
Seguridad en Servicios de TI
RACIONAL
La información es protegida en su integridad, disponibilidad, confiabilidad y no repudio. Toda información debe permitir su trazabilidad y debe permitir que sistemas de auditoría y monitoreo validen su autenticidad. Los elementos de infraestructura (software y hardware) deben ser implementados y actualizados conforme a todas las normas, políticas y lineamientos definidos por la Gestión de Seguridad de la Información.

PRINCIPIO DE TECNOLOGÍA 6
Seguridad en Servicios de TI
Las actuales regulaciones y normas para el manejo de información exigen una debida gestión a nivel de seguridad que garanticen su disponibilidad, confiabilidad e integridad. Adicionalmente, prohíben el acceso no controlado a toda la información de la entidad. La información deberá ser gestionada de acuerdo con su clasificación y controles definidos. Los actuales medios de acceso a sistemas generan una nueva vulnerabilidad a las entidades, las cuales deberán ser mitigadas a través del diseño e implementación de políticas y controles de seguridad de la información. La información que pueda ser accedida y/o generada por terceros o por otras entidades, de igual forma, deberán ser protegidas por las políticas de seguridad de la información.
IMPLICACIONES
La información deberá ser clasificada y gestionada según esta tipificación. La información deberá ser recibida, generada, procesada, publicada y almacenada bajo las políticas y lineamiento definidos previa identificación de activos, riesgos y procesos. La seguridad de la información deberá ser implementada dentro de todos los sistemas de información como un aspecto fundamental. Es necesario publicar y capacitar a todo el personal de la entidad, incluidos los contratistas y proveedores, respecto de las políticas y controles de seguridad de la información. Es necesario contar con un sistema que gestione todos los accesos de los usuarios y sus privilegios. En los procesos de cambios y liberación de software, se deberán realizar actividades que aseguren que el nuevo software / hardware cumple con los lineamientos y políticas de seguridad.

PRINCIPIO DE TECNOLOGÍA 7
Independencia Tecnológica
RACIONAL
Las aplicaciones no dependerán de una plataforma o un software base específico, éstas deberán tener la posibilidad de funcionar en diferentes plataformas y versiones. La arquitectura tecnológica debe ser planeada para reducir el impacto que puede generar un cambio de plataforma sobre el negocio. El mantener una independencia de tecnológica, permite a TI desarrollar, adaptar y operar bajo uno buena relación costo / beneficio. Alternativamente, la tecnología se convierte en la motivación de los usuarios para su aprovechamiento en términos de servicios. El crecimiento y potencialización de una plataforma se facilita cuando no se está limitado a una marca o a un fabricante en específico. Las decisiones de diseño de plataformas y en especial, de servicios de TI serán independientes de una marca o un fabricante específico.
IMPLICACIONES
La implementación de este principio se debe apoyar en estándares abiertos y en conceptos de alta portabilidad. Los sistemas de información deben contemplar mecanismos de integración y/o intercambios de información simples y ágiles. Los sistemas de información deben ser diseñados independientes al hardware sobre el cual debe "correr". Las aplicaciones deberán apoyarse en software de capa media el cual debe ayudar a gestionar de forma separada el hardware, los datos y la capa de aplicaciones, pero unificándolos en forma de sistemas de información.

PRINCIPIO DE TECNOLOGÍA 8
Escalabilidad de Infraestructura
RACIONAL
Se debe permitir la evolución continua de los elementos de la infraestructura y la adición de componentes, sin perder desempeño ni disponibilidad de los servicios de TI que se soportan.

La infraestructura tecnológica es el motor de los servicios de TI y por ende debe soportar la actualización de estos. Su flexibilidad y facilidad de crecimiento (horizontal o vertical), debe ser una de sus grandes características. Los servicios de TI tienen como factor crítico de éxito la facilidad de escalabilidad de sus componentes para gestionar de forma óptima la demanda de servicios.
IMPLICACIONES
La infraestructura tecnológica deberá permitir la inclusión y eliminación de elementos permitiendo de esta forma gestión "horizontal" de la infraestructura. Los elementos de la infraestructura tecnológica deberán permitir la potencialización para una gestión "vertical" de la infraestructura. A parte de la configuración normal de la infraestructura, se deberá permitir la creación de particiones virtuales creando de esta forma, capas lógicas a nivel de infraestructura.

Tabla 14. Principios de Tecnología

5.4 Objetivos

Desde el punto de vista de objetivos estos se definen dentro del marco legal aplicable a los OAT como se muestra:

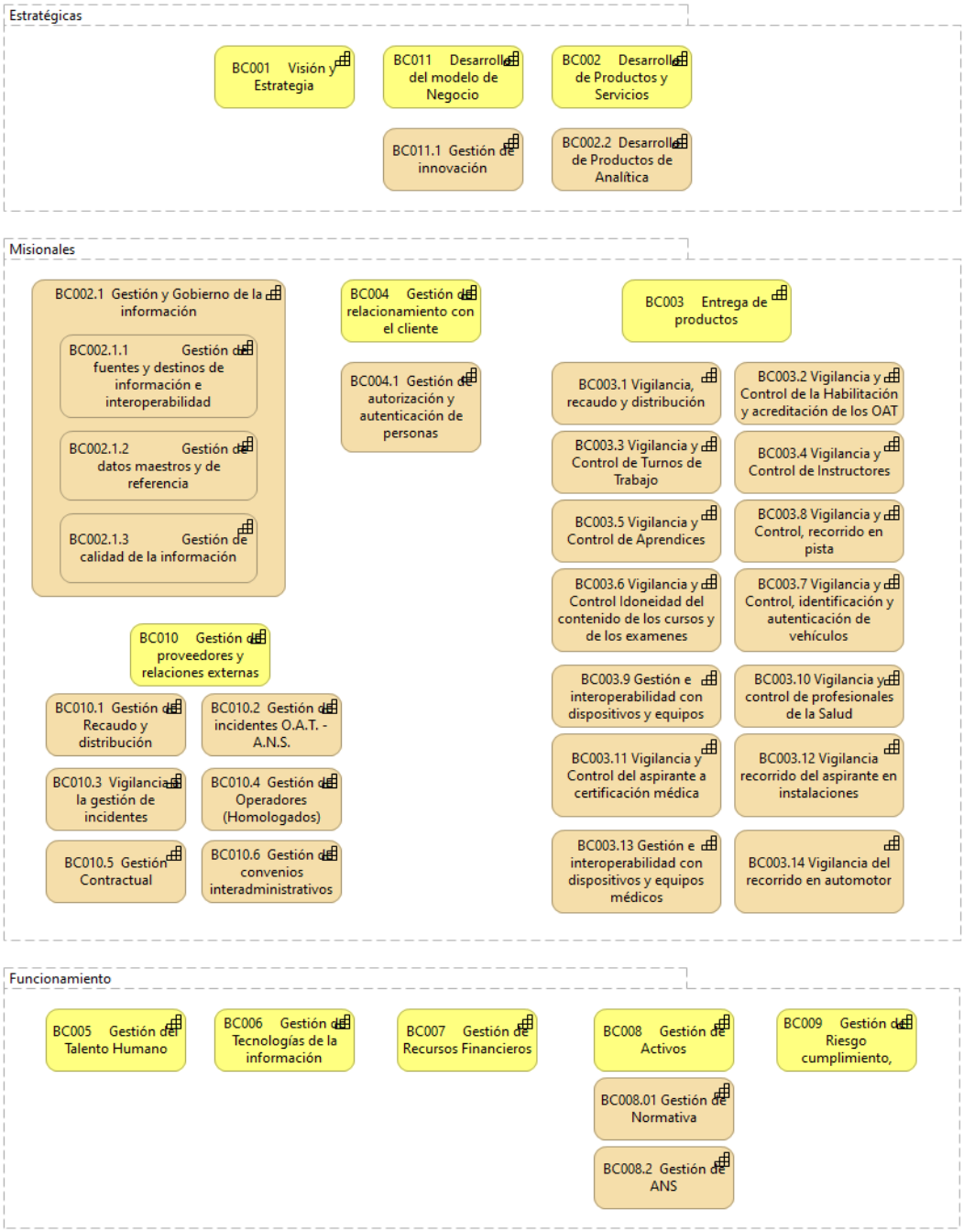
IDENTIFICADOR	NOMBRE	TIPO OAT	FUENTE
OE-001	Capacitación de personas que aspiran a conducir vehículos automotores o motocicletas	CEA	Resolución 60832 de 2016 Superintendencia de Transportes
OE-002	Servicio de escuela y casa cárcel para la rehabilitación de los infractores a las normas del Código de Tránsito	CIA	
OE-003	Realización de los exámenes teóricos y prácticos de conducción en un espacio preparado para estas actividades	CALE	Resolución 1349 de 2017 Ministerio de Transporte (MINTRANSPORTE)
OE- 004	Realización de la evaluación y certificación de la aptitud	CRC	Resolución 6246 de 2016

	física, mental y de coordinación motriz para conducir		Superintendencia de Puertos y Transportes
OE-005	Realizar las revisiones técnico mecánicas y de emisiones contaminantes de cada vehículo	CDA	Resolución 13830 de 2014 Superintendencia de Transportes

5.5 Mapa de capacidades

El mapa de capacidades es una estructura jerárquica que contiene la definición de todas aquellas facultades y competencias que la entidad debe ser capaz de realizar para implementar y mantener el SICOV. Este es el elemento central de la arquitectura de negocio, ya que permite conectar el modelo estratégico con el modelo operativo.

Ilustración 45 - Mapa de Capacidades



Fuente: Elaboración propia Grow Data 2021

Tabla 15 - Capacidades

ID	Nombre Capacidad	Descripción Capacidad
BC001	Visión y Estrategia	Esta capacidad permite abordar la visión y estrategia del SICOV contemplando los siguientes aspectos: Evaluación del entorno. Comprensión del mercado para identificar las soluciones requeridas por el cliente. Evaluación de la organización hacia dentro. Establecer la visión estratégica. Desarrollar la declaración de misión. Definir y evaluar las opciones estratégicas. Definir la estrategia de negocio. Alinear el diseño organizacional (funcional). Desarrollar y establecer las metas organizacionales. Desarrollar la estrategia regulatoria. Desarrollar, ejecutar y medir las iniciativas estratégicas.
BC002	Desarrollo de Productos y Servicios	Esta capacidad permite desarrollar los productos y servicios del SICOV con aspectos como: Gobernar el programa de desarrollo de productos y/o servicios. Gestionar patentes, derechos de autor y requerimientos regulatorios. Realizar vigilancia tecnológica para desarrollar nuevos productos y/o servicios. Desarrollar nuevos productos y/o servicios mediante prototipos. Incidir en el desarrollo de tarifas y esquemas de financiamiento para productos y/o servicios
BC002.1	Gestión y Gobierno de la información	Capacidad que habilita la obtención de información para cumplir la misionalidad del ecosistema SICOV controlada y de calidad
BC002.1.1	Gestión de fuentes y destinos de información e interoperabilidad	Gestionar la interoperabilidad de manera estandarizada y gobernada de acuerdo a la arquitectura de referencia de integración seleccionada.

ID	Nombre Capacidad	Descripción Capacidad
BC002.1.2	Gestión de datos maestros y de referencia	Gestionar los dominios de datos Maestros que deben ser gobernados (ej: Parámetros de los equipos de diagnóstico, Personas (en sus roles instructor, aprendiz, aspirante a certificado, etc.), establecimiento de sincronización con fuentes externas e internas.
BC002.1.3	Gestión de calidad de la información	Establecimiento de reglas de calidad y mecanismos de remediación para datos transaccionales de Vigilancia y control.
BC002.2	Desarrollo de Productos de Analítica	Generación de productos de analítica descriptiva, predictiva y prescriptiva que permitan cumplir con la misión del SICOV, capacidad de toma de decisiones consistentes sobre cómo obtener valor estratégico de los datos.
BC003	Entrega de productos	Esta capacidad permite gestionar la cadena de suministro y alinear el plan de compras con la estrategia, realizar la compra de materiales y/o servicios requeridos, gestionar las operaciones logísticas y de almacenamiento o inventarios, producir y/o contratar la entrega de productos y/o servicios.
BC003.1	Vigilancia, recaudo y distribución	Esta capacidad permite gestionar el recaudo, realizado por actores externos que deben ser vigilados, y la dispersión de los recursos de acuerdo con los lineamientos establecidos a los actores correspondientes: OAT, operador del SICOV, ANSV, recaudador.
BC003.2	Vigilancia y Control de la Habilitación y acreditación de los OAT	Se encarga de velar por el cumplimiento de los requisitos normativos, composición accionaria y cumplimiento de requisitos y certificaciones de cada uno de los OAT.
BC003.3	Vigilancia y Control de Turnos de Trabajo	Se encarga de validar que se realice una adecuada gestión de la fuerza de trabajo

ID	Nombre Capacidad	Descripción Capacidad
BC003.4	Vigilancia y Control de Instructores	Se encarga de asegurar que los instructores sean un recurso humano idóneo, mantener la información de instructores de manera gobernada, mantener historial.
BC003.5	Vigilancia y Control de Aprendices	Encargada de asegurar riesgos relacionados con la no asistencia a las sesiones teóricas y prácticas, la correcta presentación de los exámenes. Mantener la trazabilidad histórica de asistencia.
BC003.6	Vigilancia y Control Idoneidad del contenido de los cursos y de los exámenes	Encargada de mantener de una manera gobernada los contenidos y profundidad de los cursos, y mantener un gobierno de las bases de preguntas para la aplicación de los exámenes.
BC003.7	Vigilancia y Control, identificación y autenticación de vehículos.	Encargada de garantizar que el vehículo que se encuentra en el servicio es el que dice ser.
BC003.8	Vigilancia y Control, recorrido en pista	Capacidad que permite mantener la trazabilidad de las acciones del vehículo que hace el recorrido
BC003.9	Gestión e interoperabilidad con dispositivos y equipos para diagnóstico automotriz	Permite brindar las interfaces necesarias que permitan asegurar la información desde el dispositivo de diagnóstico para ser entregadas al sistema de gestión.
BC003.10	Vigilancia y control de profesionales de la Salud	Encargado de realizar que los profesionales de la salud sean un recurso humano idóneo. Mantener la información de los profesionales de manera gobernada, mantener historial.
BC003.11	Vigilancia y Control del aspirante a certificación médica	Capacidad que permite vigilar y mantener un gobierno de la información del paciente generada en el CRC.
BC003.12	Vigilancia recorrida del aspirante en instalaciones	Capacidad de obtener trazabilidad en el recorrido del aspirante por las instalaciones del OAT.

ID	Nombre Capacidad	Descripción Capacidad
BC003.13	Gestión e interoperabilidad con dispositivos y equipos médicos	Permite brindar las interfaces necesarias que permitan asegurar la información desde el dispositivo de diagnóstico médico para ser entregadas al sistema de gestión.
BC003.14	Vigilancia del recorrido en automotor	Encargada de monitorear los recorridos de los automotores mientras se imparte la formación práctica.
BC004	Gestión de relacionamiento con el cliente	Capacidad que permite desarrollar la estrategia de servicio al cliente, la estrategia de satisfacción/fidelización del cliente, gestionar los incidentes del servicio (continuidad). gestionar quejas, peticiones y reclamos, generar reportes de incidentes y riesgos a entidades regulatorias y evaluar la satisfacción del cliente
BC004.1	Gestión de autorización y autenticación de personas	Capacidad que permite garantizar que un usuario es quien dice ser y que está autorizado a recibir el servicio.
BC005	Gestión del Talento Humano	Capacidad que permite gestionar el talento humano encargado de la vigilancia y el control.
BC006	Gestión de Tecnologías de la información	Gestionar Obsolescencia tecnológica de los componentes, Gestionar el mantenimiento de las arquitecturas del SICOV.
BC007	Gestión de Recursos Financieros	Gestionar los recursos financieros de la operación del SICOV.
BC008	Gestión de Activos	Gestión de Inventarios, CMDB en tiempo real, NOC Dispositivos para la vigilancia y control: - Cámaras - PAD de firmas - Sistemas de posicionamiento (GPS) - Huellero - Canal dedicado - Servidores - Cableado
BC008.1	Gestión normativa	Gestión de las normas aplicables en el SICOV.

ID	Nombre Capacidad	Descripción Capacidad
BC008.2	Gestión de ANS	Gestión de los Acuerdos de Niveles de Servicio ofrecidos por el operador del SICOV.
BC009	Gestión del Riesgo cumplimiento, contingencia y resiliencia	Gestión del cumplimiento de los ANS, los requerimientos, los planes de contingencia y continuidad del negocio del operador del SICOV.
BC010	Gestión de proveedores y relaciones externas	Capacidad para gestionar los diferentes actores del sistema SICOV.
BC010.1	Gestión de Recaudo y distribución	Capacidad para gestionar los diferentes aliados de recaudo, de manera gobernada. (En arquitectura de solución puede plantearse como un componente transversal, tercerizado no manejado por los OATS.)
BC010.2	Gestión de incidentes O.A.T., A.N.S.	Se debe garantizar una adecuada prestación del servicio de Vigilancia y Control, se requiere la capacidad de gestionar incidentes que impidan la vigilancia y control de los OATS e impidan su operación.
BC010.3	Vigilancia a la gestión de incidentes.	Si la gestión la realizan los homologados se debe establecer una función de vigilancia que establezca de manera clara las condiciones de servicio (A.N.S.) con los O.A.T. Pedir tableros de control específicos que visibilicen la oportunidad de los homologados
BC010.4	Gestión de Homologados	Capacidad para mantener comunicación e interacción con los homologados
BC010.5	Gestión Contractual	Se encarga de garantizar las condiciones específicas con los homologados.
BC010.6	Gestión de convenios interadministrativos	Se encarga de realizar la gestión de convenios con proveedores o consumidores de información
BC011	Desarrollo del modelo de Negocio	Capacidad que permite gestionar los procesos de negocio, los cambios y el conocimiento del SICOV para su evolución en el tiempo.

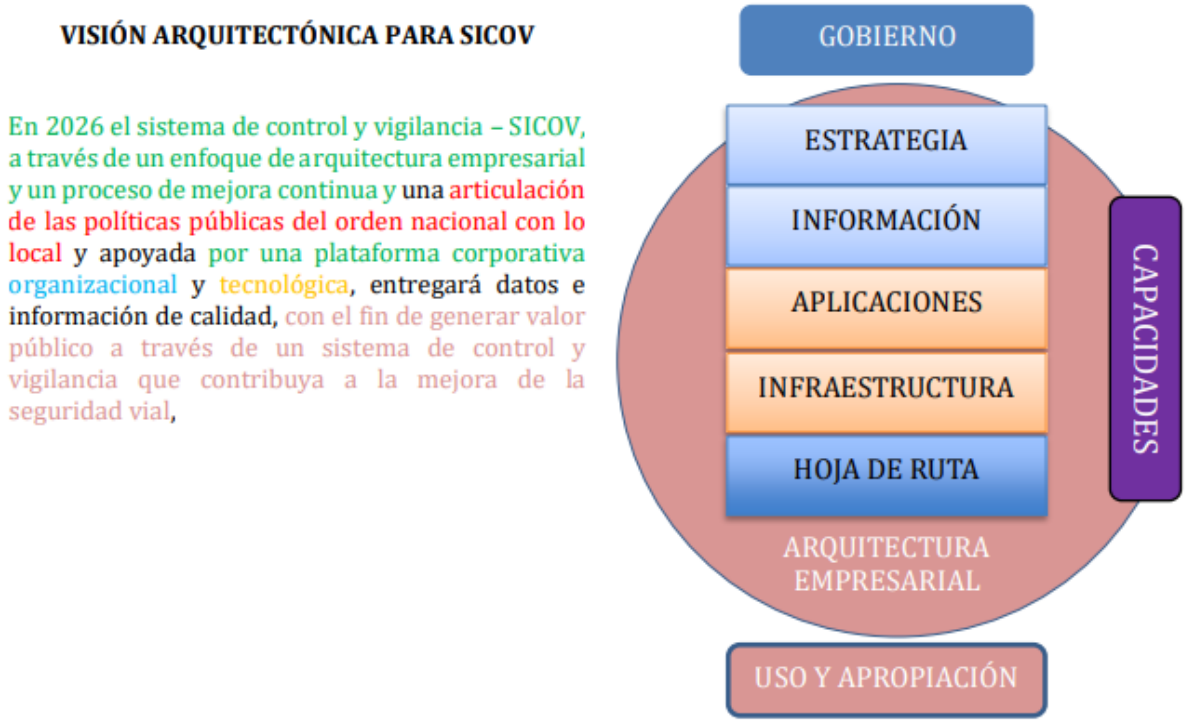
ID	Nombre Capacidad	Descripción Capacidad
BC011.1	Gestión de innovación	Capacidad que habilita la identificación e implementación de oportunidades de mejora e innovación del SICOV

Fuente: Elaboración propia Grow Data 2021

6 Arquitectura objetivo TO BE

La visión de Arquitectura Empresarial para el SICOV, integra las expectativas de los interesados clave, así como las preocupaciones identificadas para de esta forma estructurar requerimientos de alto nivel que deberán ser desarrollados a través de los diferentes dominios de la arquitectura.

Ilustración 46 – Visión de arquitectura empresarial SICOV



Fuente: Grow Data SAS, 2021

Esta visión de arquitectura establece el contexto de diseño para la creación de la arquitectura de estado futuro (TOBE).

6.1 Arquitectura de negocio

6.1.1 Arquitectura de Estado Futuro (TOBE)

El SICOV tiene una serie de interacciones con otras entidades del Estado Colombiano como se muestra en la siguiente figura:

Ilustración 47 – Modelo de interacción del SICOV con otras entidades

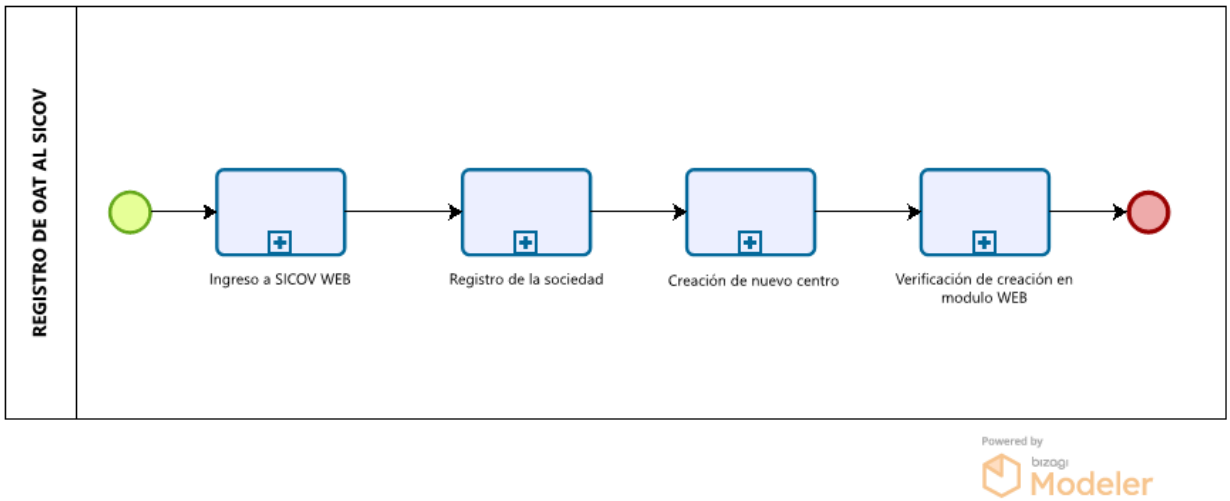
Fuente: Elaboración propia Grow Data 2021

6.1.1.1 Diagramas BPMN (N4)

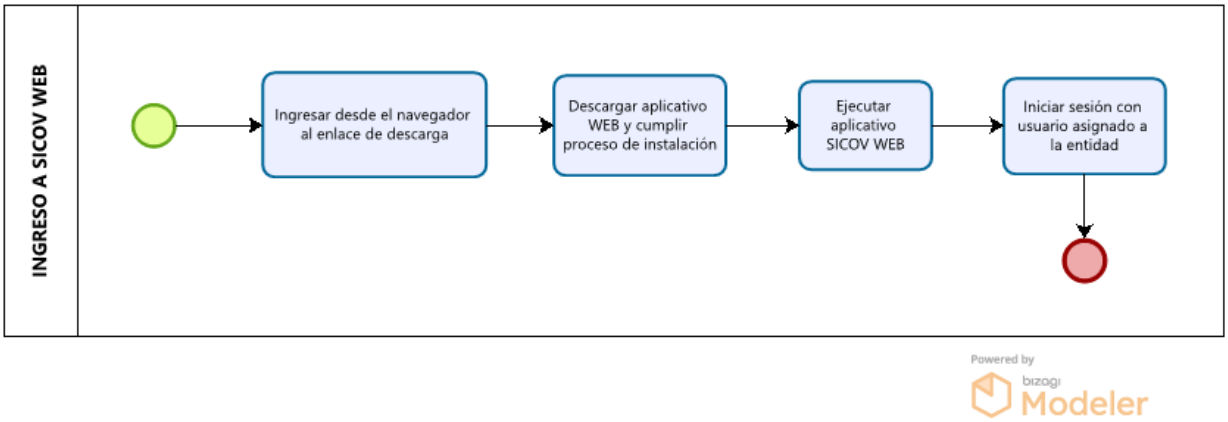
En los siguientes diagramas se muestra el modelamiento de los procesos en estado futuro por cada tipo de OAT.

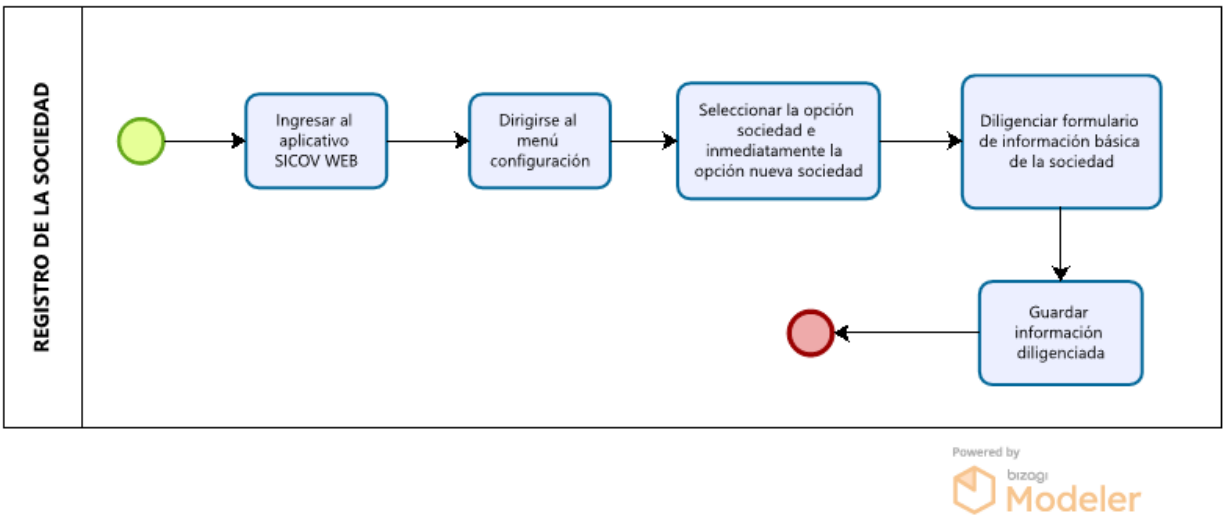
Estos procesos se complementan con los anexos en BPMN que se adjuntan a este documento y los anexos sobre los controles.

PROCESO DE REGISTRO DE OAT EN SICOV

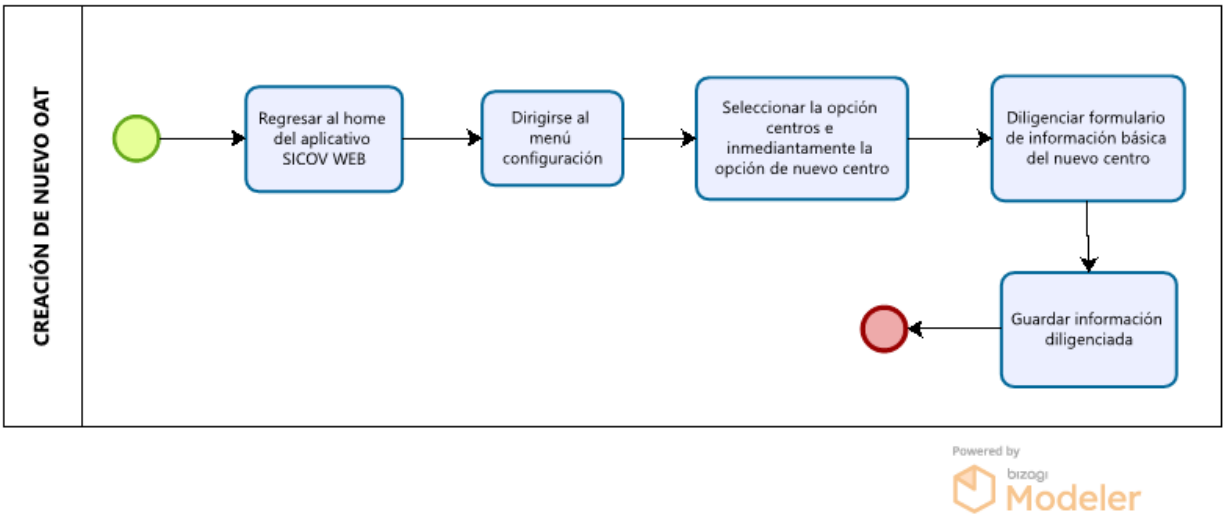


A continuación, se presentan los procedimientos asociados al proceso mostrado en la figura anterior:

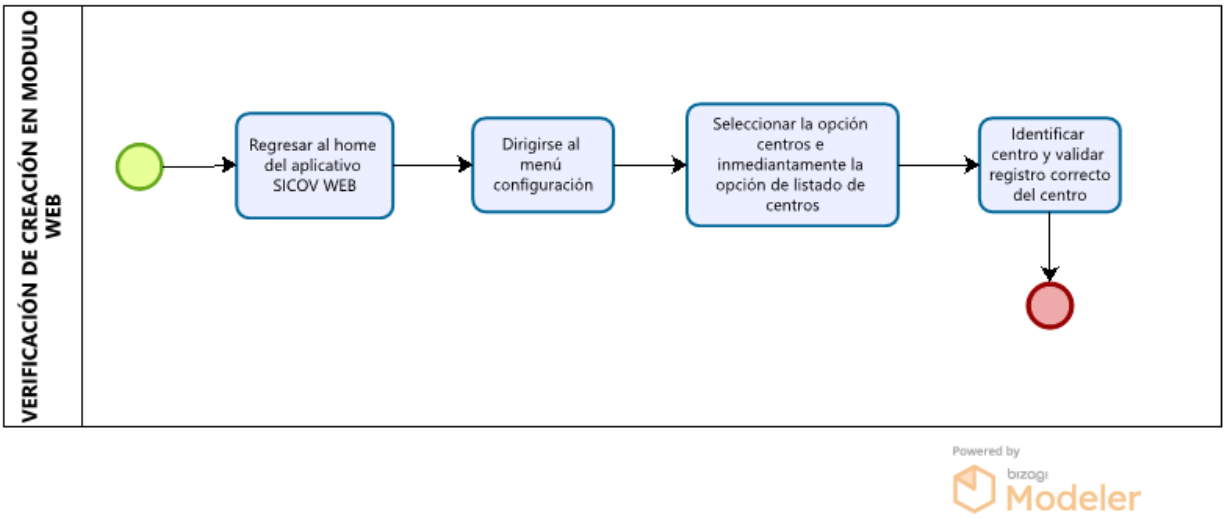




En el registro de la sociedad se verifican aspectos como: Nombre de la sociedad, NIT, código de verificación, matrícula mercantil, acreditación y se adjunta el certificado de acreditación, nombre del representante legal y su identificación, actividad económica y responsabilidad fiscal. Sin el cumplimiento de estos requisitos no se puede continuar con la creación del OAT.

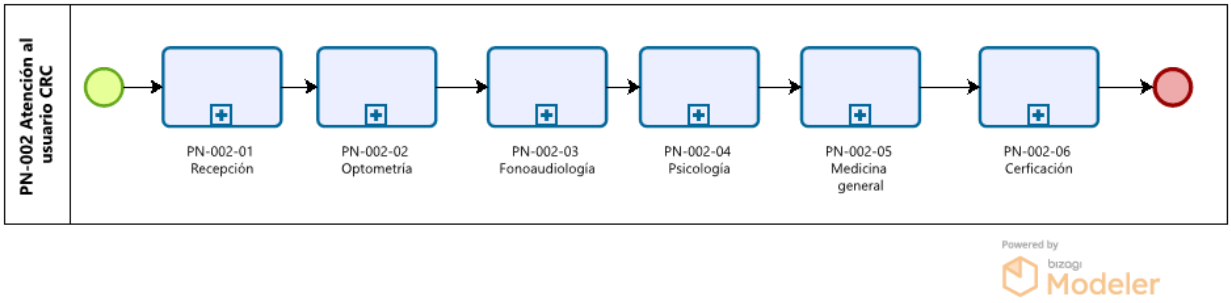


En la creación de un nuevo OAT, asociado a una sociedad registrada, en el paso anterior, se verifican aspectos como: departamento, ciudad, dirección física del OAT, teléfonos de contacto, nombre del centro, registro mercantil, resolución del Ministerio de Transporte, Fecha de la resolución de MinTransporte, registro en el RUNT (ID-RUNT), ubicación geolocalizada por GPS (latitud, longitud), imágenes de logotipos y sellos de identificación del centro, verificación de acreditación (código acreditación, fecha otorgamiento, fecha renovación, fecha de vencimiento).



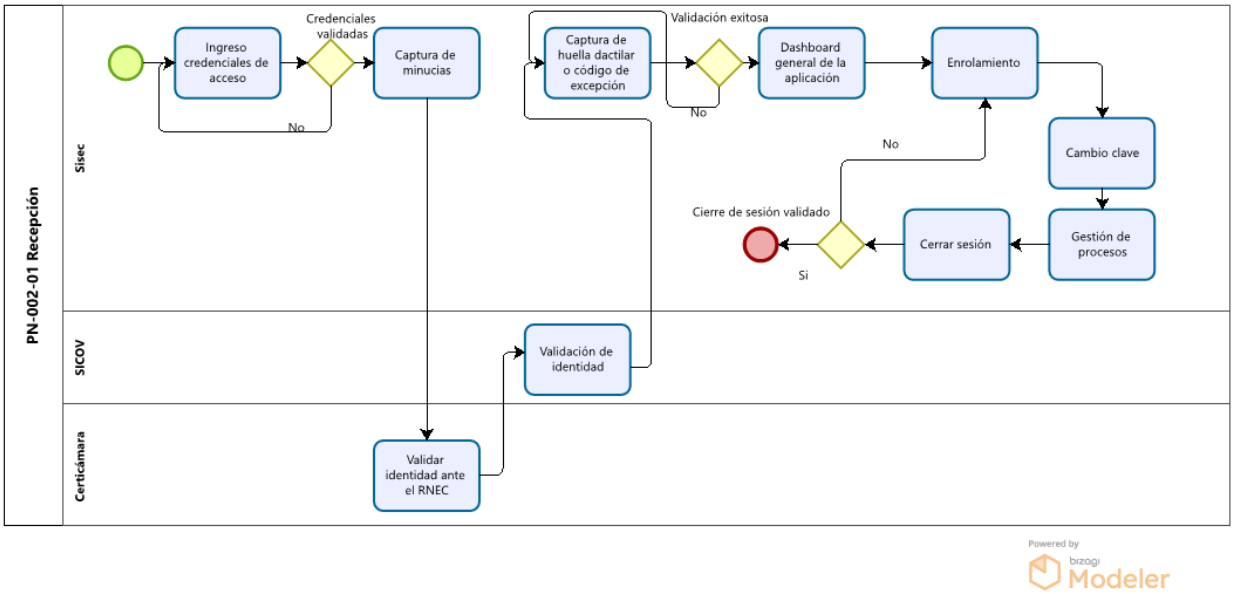
Por último, se debe verificar que todo el registro fue realizado correctamente.

PROCESO CRC



Este proceso inicia con la recepción de la persona que será atendida, pasando por cada una de las etapas de evaluación médica y terminando con la emisión del certificado de aptitud.

A continuación, se presentan los procedimientos asociados al proceso mostrado en la figura anterior:



En este primer procedimiento, se identifican las actividades a desarrollar en la primera etapa de recepción, donde se registran tanto el funcionario como la persona que será atendida.

Para el caso de la excepción por problemas en la identificación biométrica se determina lo siguiente:

El mecanismo de excepción es uno solo cuando no se puede verificar la biometría y es que la persona presente certificado notarial de acuerdo a lo establecido en la ley.

La regulación de la biometría en Colombia surgió con la ley 527 del año 1999 y el decreto 2.364 del 2012. Estas reglas posibilitan usar biometría en medios electrónicos para procesos de verificación de identidad y para la firma de documentos electrónicos.

La huella dactilar como mecanismo de identificación está vigente en el artículo 18 del decreto Ley Antitrámites. Ante ello, "tienen las entidades públicas y ciertos particulares cotejar la identidad del titular de la huella con base de datos de la Registraduría".

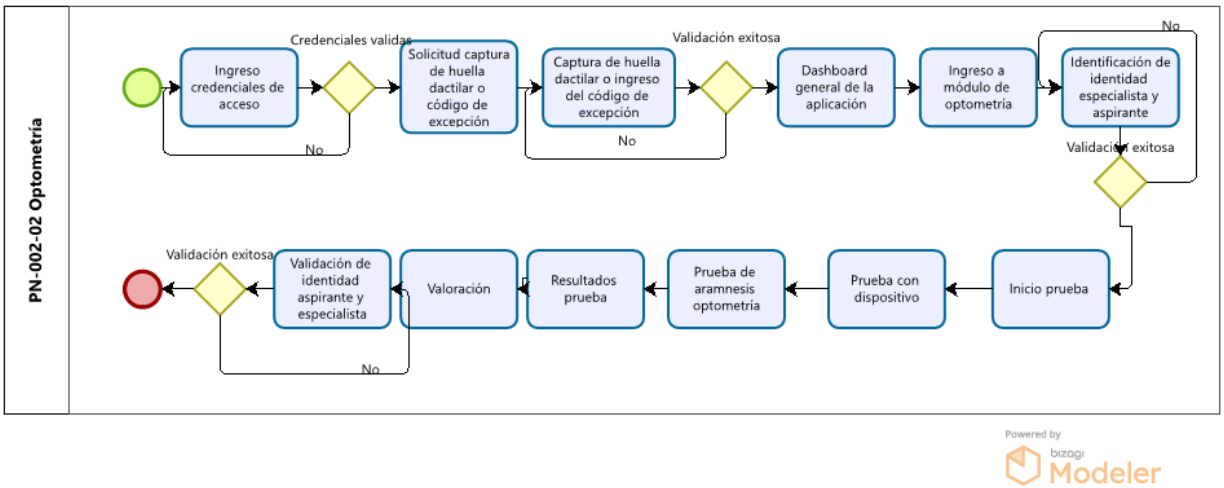
Actualmente tiene bases de datos en: el Registro Nacional del Estado Civil, que contiene huellas dactilares y fotos biométricas y en la BIOMIG de Migración Colombia, que contiene registros del iris.

Que el artículo 18 del Decreto-ley 0019 de 2012 determinó que en los trámites y actuaciones que se cumplan ante las entidades públicas y los particulares que ejerzan funciones administrativas en los que se exija la obtención de la huella dactilar como medio de identificación inmediato de la persona, esta se hará por medios electrónicos y que las referidas entidades y particulares contarán con los medios tecnológicos de interoperabilidad necesarios para cotejar la identidad del titular de la huella con la base de datos de la Registraduría Nacional del Estado Civil;

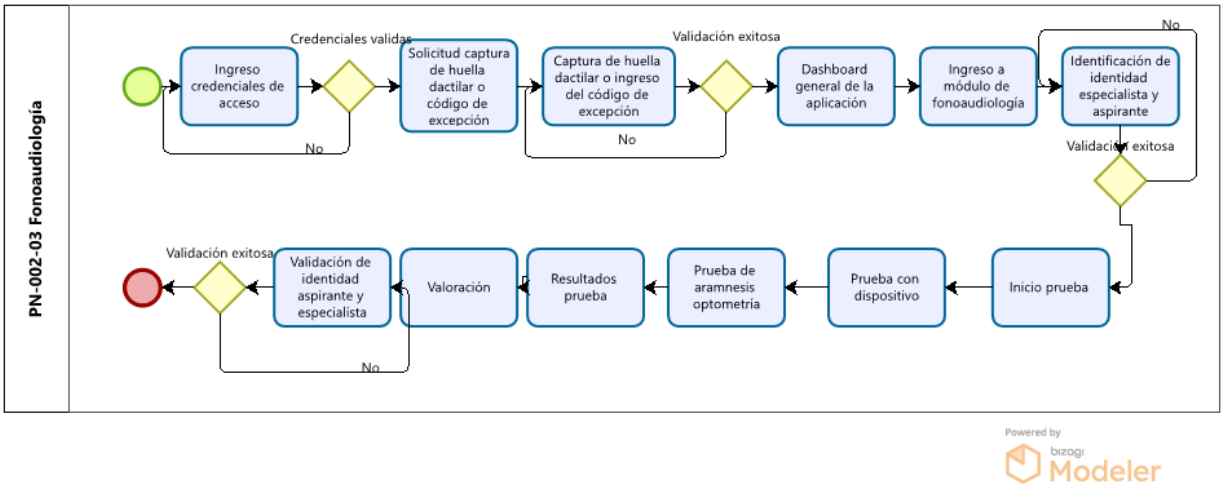
Que conforme con el parágrafo 2° del mencionado artículo 18 del Decreto-ley 0019 de 2012, los notarios están obligados a implementar la infraestructura tecnológica para prestar el servicio de identificación biométrica en línea en aquellos trámites en los que, de conformidad con las disposiciones legales vigentes, se exija la huella dactilar como medio de identificación, para lo cual es necesario contar con una retribución al amparo de la función social y la seguridad jurídica del país;

Que, conforme a lo anterior, la imposición de la huella dactilar será remplazada por su captura mediante la utilización de medios electrónicos.

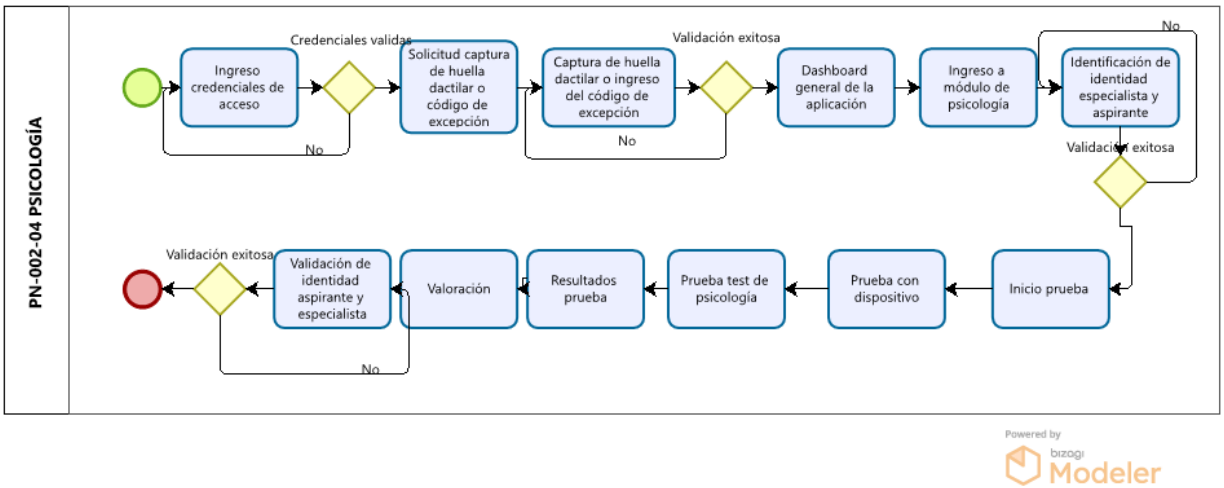
Esta excepción aplica de la misma forma para todas las actividades de los diferentes procedimientos donde se realiza esta verificación biométrica.



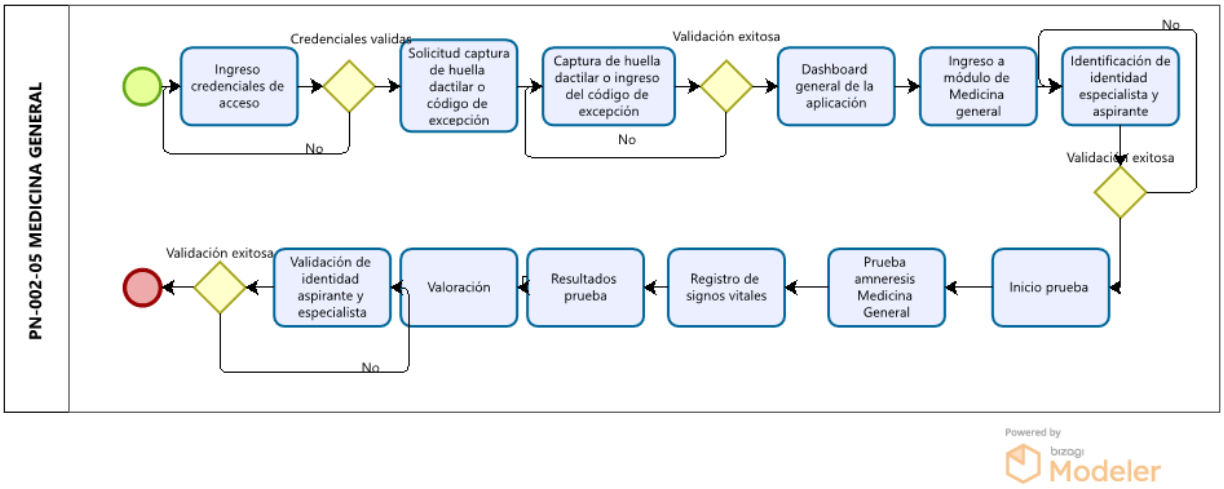
En este procedimiento se realiza la primera prueba, que es de optometría en donde inicialmente se realiza la validación tanto del especialista médico como de la persona que será atendida, se realizan la prueba, se valida nuevamente al final las credenciales de identificación y se pasa a la siguiente prueba.



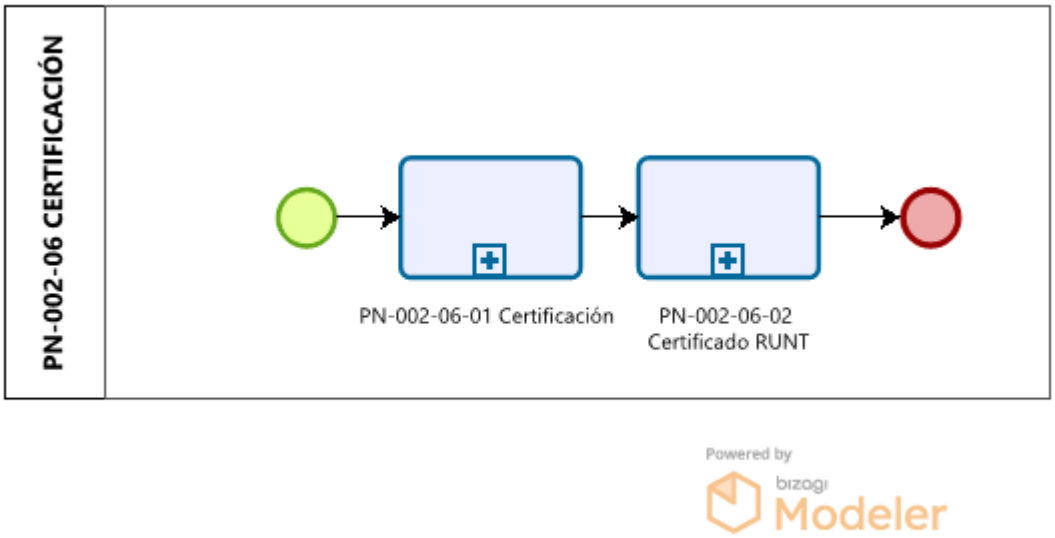
En este procedimiento se realiza la siguiente prueba, que es de fonoaudiología en donde inicialmente se realiza la validación tanto del especialista médico como de la persona que será atendida, se realizan la prueba, se valida nuevamente al final las credenciales de identificación y se pasa a la siguiente prueba.



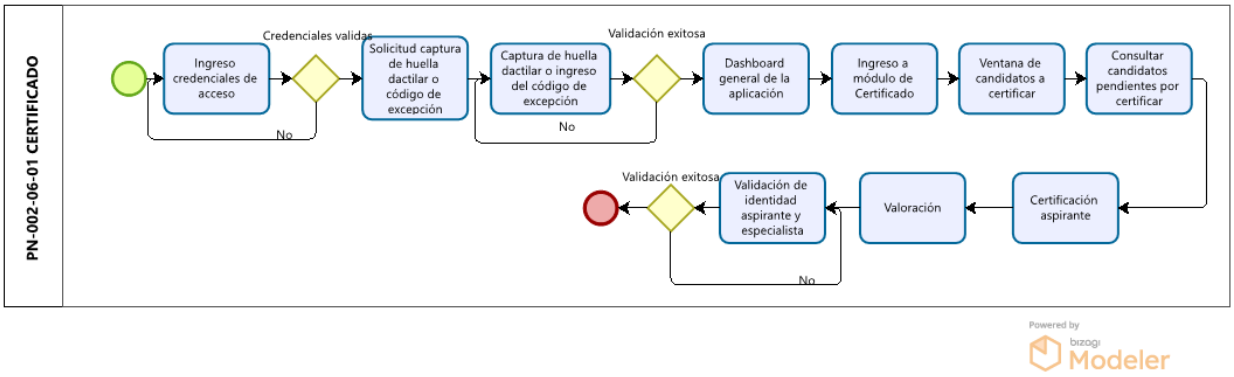
En este procedimiento se realiza la siguiente prueba, que es de sicología en donde inicialmente se realiza la validación tanto del especialista médico como de la persona que será atendida, se realizan la prueba, se valida nuevamente al final las credenciales de identificación y se pasa a la siguiente prueba.



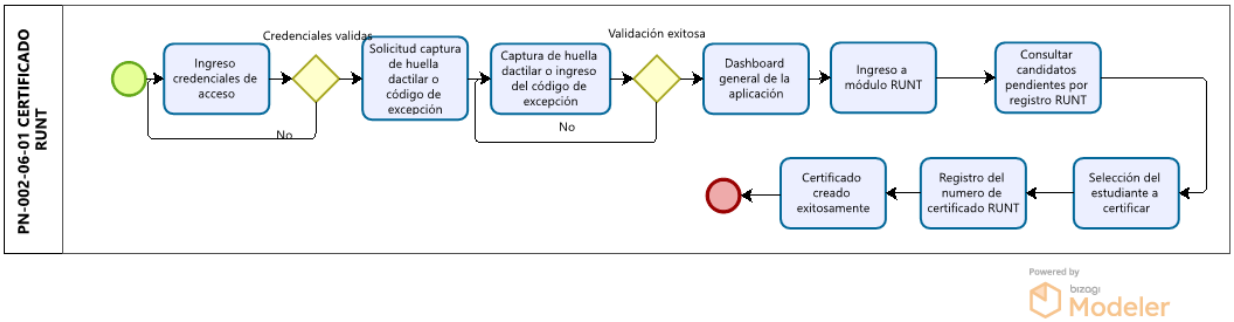
En este procedimiento se realiza la siguiente prueba, que es de medicina general en donde inicialmente se realiza la validación tanto del especialista médico como de la persona que será atendida, se realizan la prueba, se valida nuevamente al final las credenciales de identificación y se pasa al siguiente procedimiento.



En este procedimiento inicialmente se genera el certificado y posteriormente se carga esta información al RUNT.

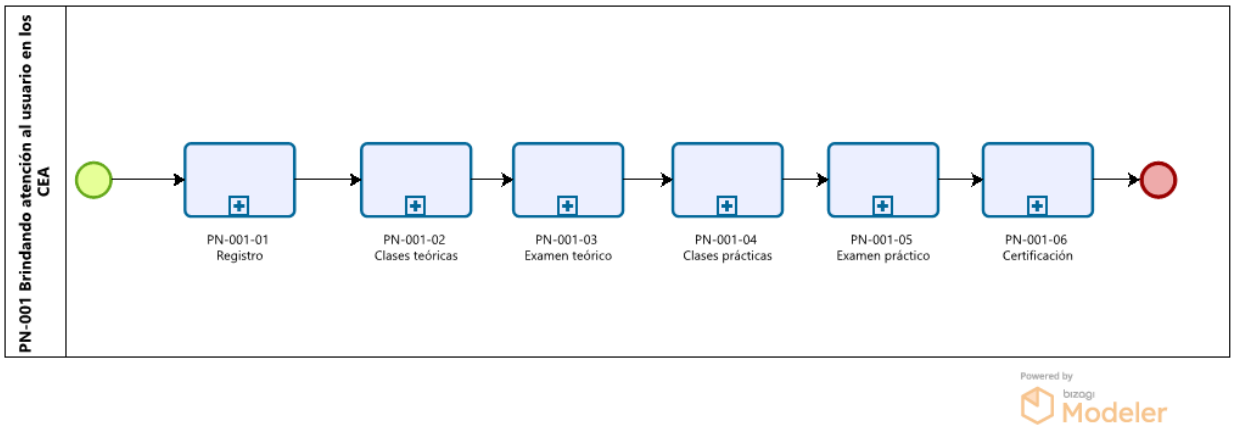


En la primera etapa de generación del certificado, se ingresan las credenciales de acceso y se valida la biometría del médico que emite el certificado, se verifican los datos correctos y se emite el certificado, al final se valida nuevamente la información biométrica del médico que emite el certificado.



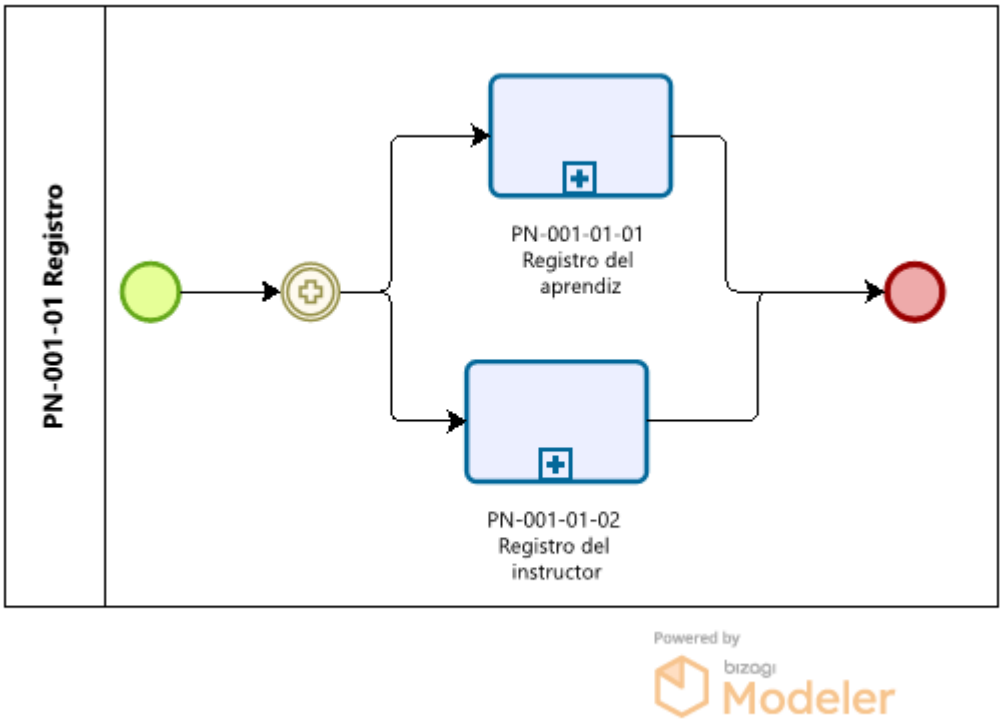
Posteriormente, se validan nuevamente las credenciales de acceso al inicio y al final, se trae la información del certificado generado, se conecta con el RUNT y se carga el certificado a este sistema para terminar el procedimiento.

<u>PROCESO CEA</u>

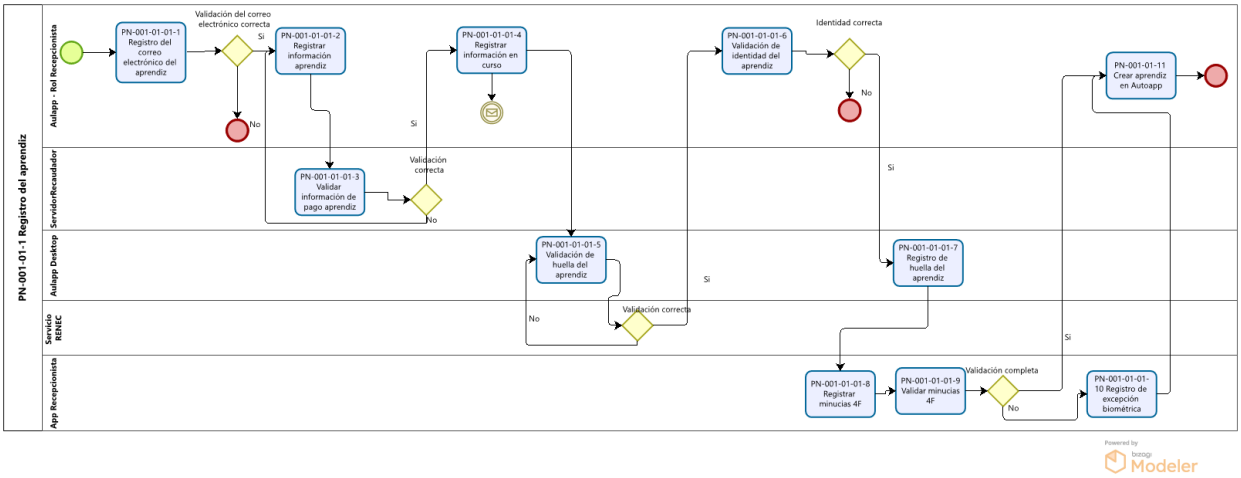


Este proceso inicia con el registro de la persona que será atendida, la ejecución de clase y sus exámenes respectivos para finalizar con la certificación.

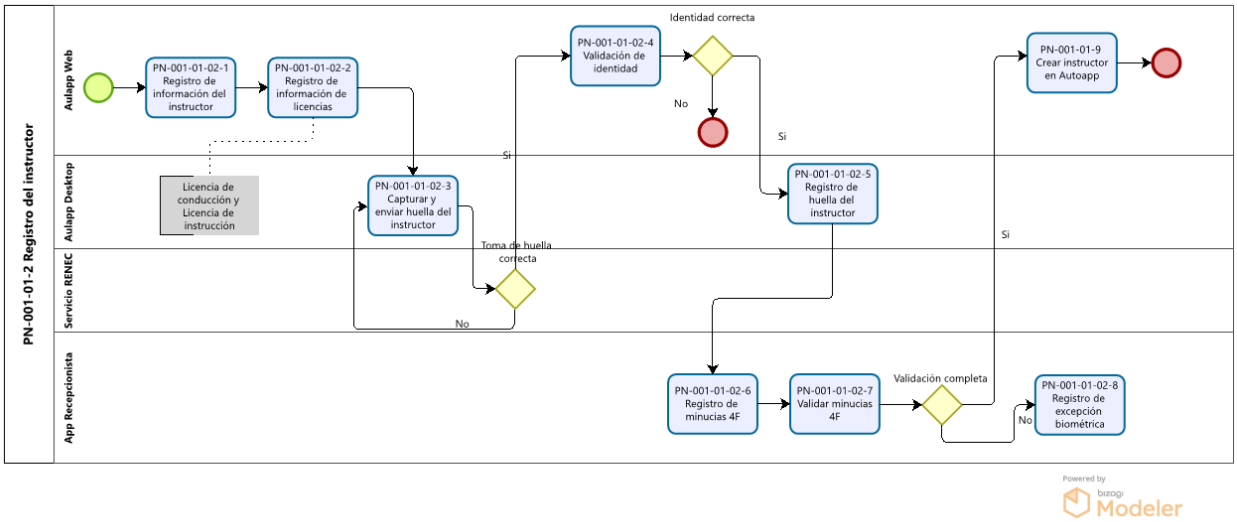
A continuación, se presentan los procedimientos asociados al proceso mostrado en la figura anterior:



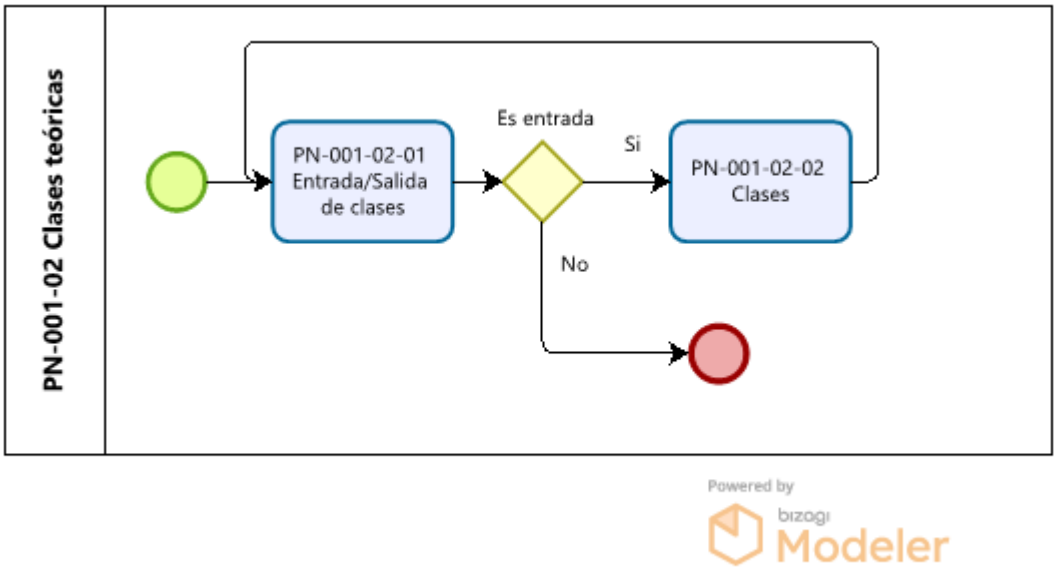
Este procedimiento de registro contiene dos partes: el registro de la persona que será atendida y el registro del instructor.

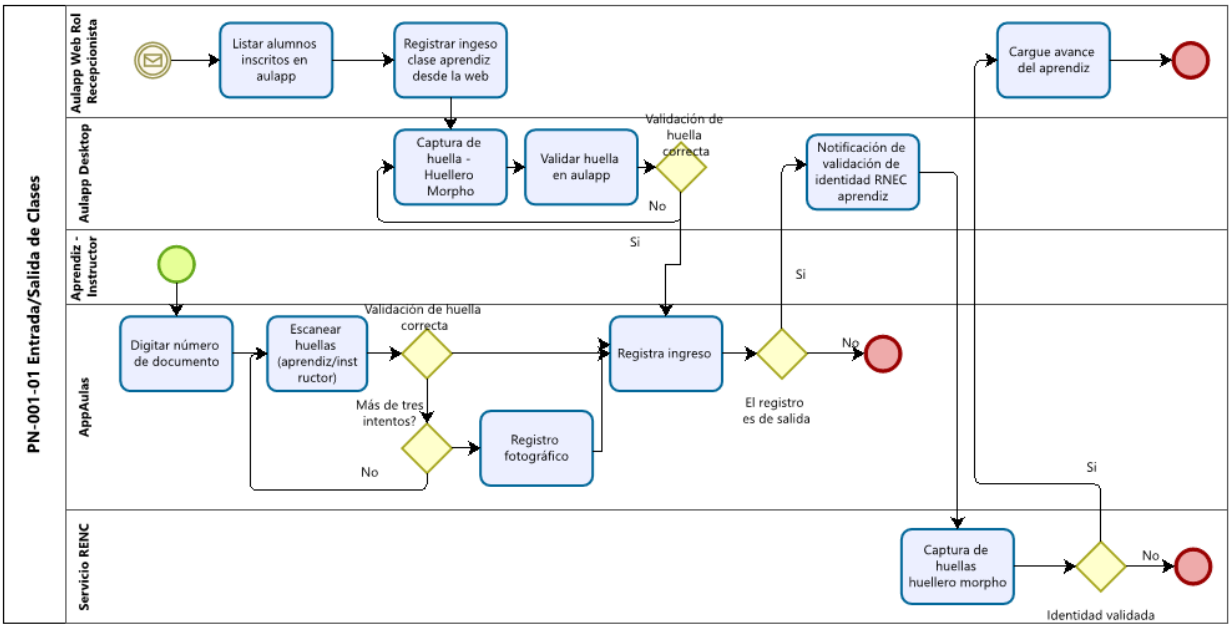


Para la persona que será atendida se valida su identidad, se valida el pago del PIN y se programan las fechas de atención de clases.

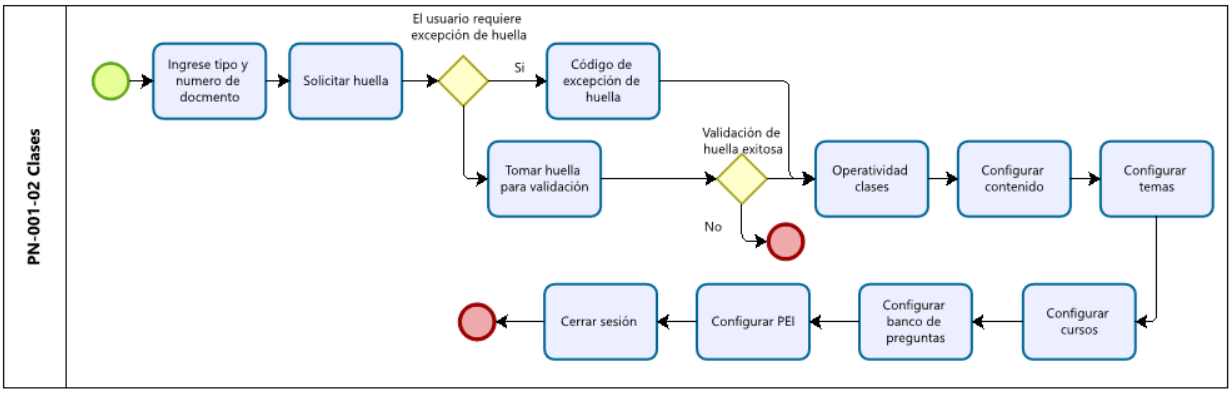


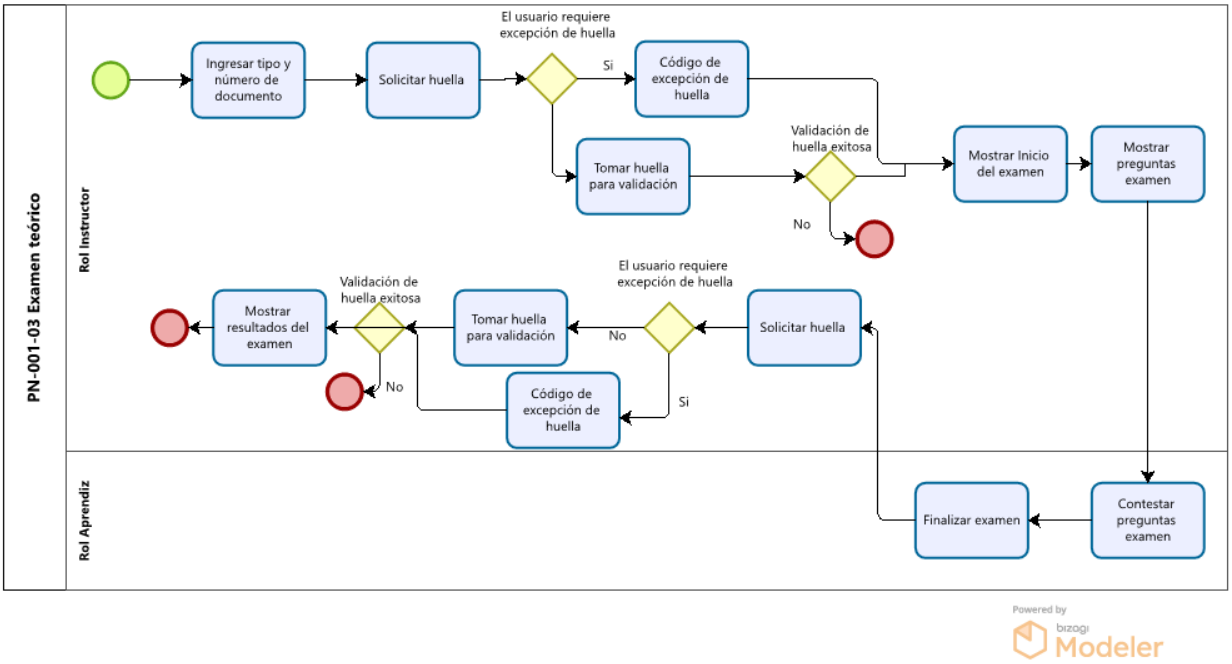
Para el instructor se valida su identidad, se valida con licencias de conducción e instrucción y se crea al instructor como recurso disponible para ser utilizado en la realización de las clases.



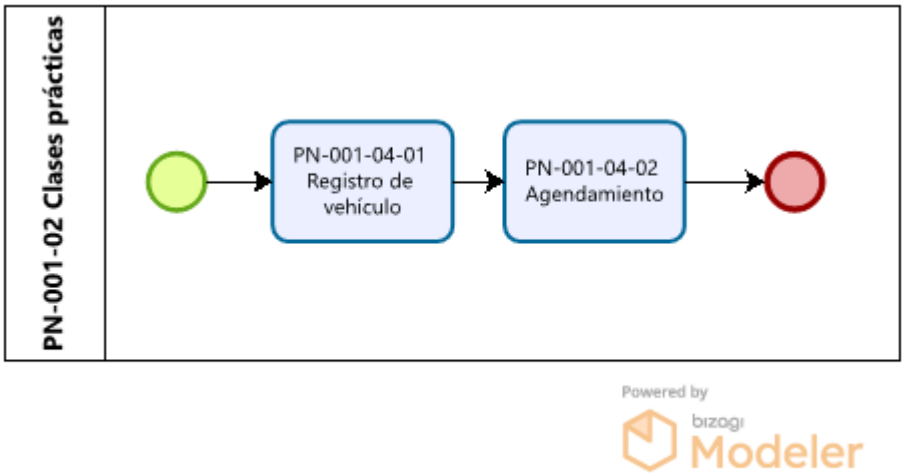


En este procedimiento se valida la asistencia de las personas que serán atendidas en el curso, de acuerdo a programación previa, se valida identidad de instructor y personas al principio y al final de la ejecución de la clase.

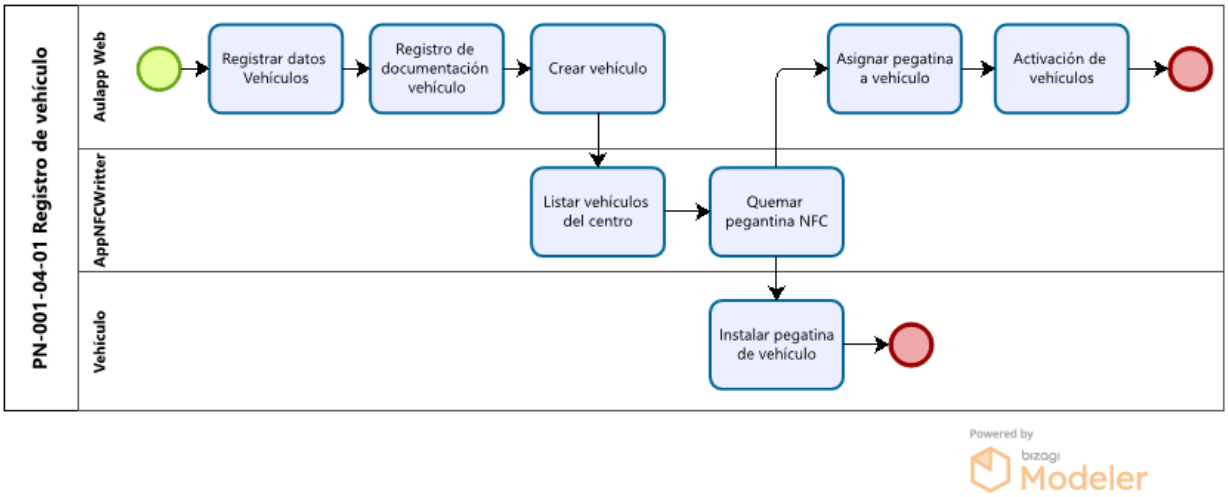




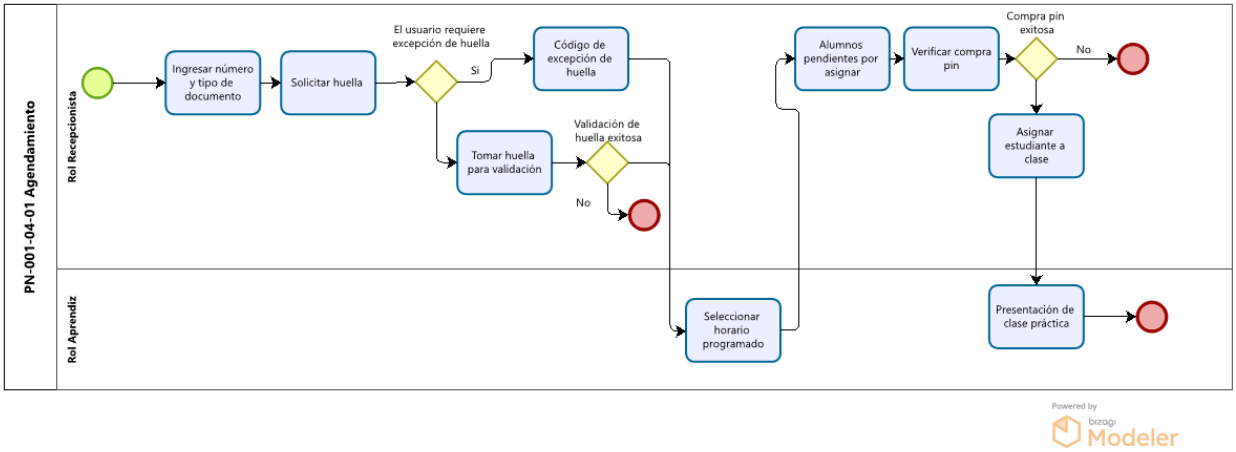
En este procedimiento se valida la asistencia de las personas que serán atendidas en el examen, de acuerdo a programación previa, se valida identidad de instructor y personas al principio y al final de la ejecución del examen.



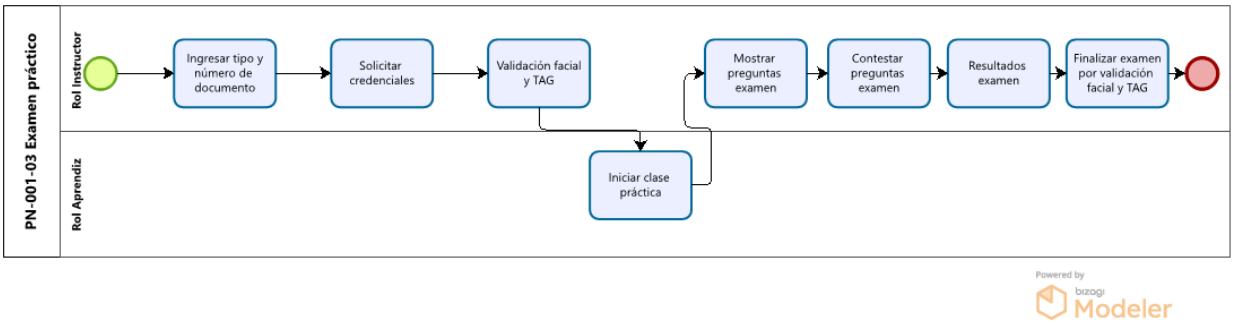
Para este procedimiento de clases prácticas se realiza el registro del vehículo y la programación de las clases.



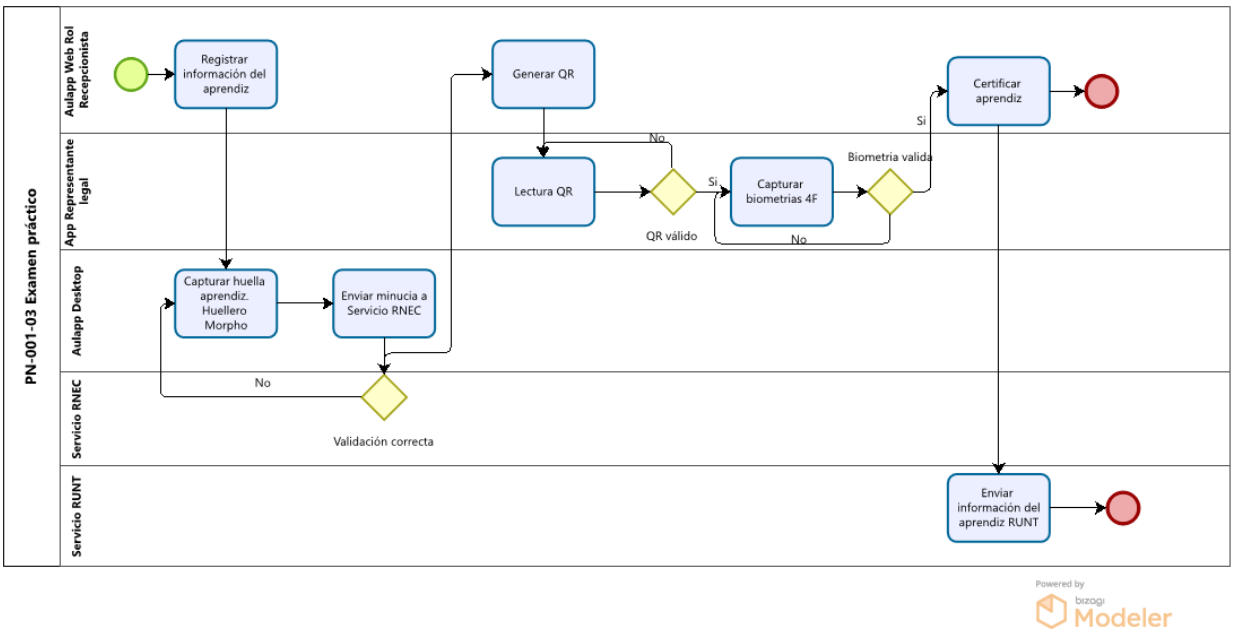
Para el registro del vehículo se valida que cuente con la documentación en regla de acuerdo a la ley, se le asigna un código único de identificación que queda registrado en un chip NFC que se asigna al vehículo y se activa en el sistema.



En este procedimiento se agenda la clase práctica, se validan identidades de persona que será atendida, del instructor, se valida PIN y se realiza la clase práctica.

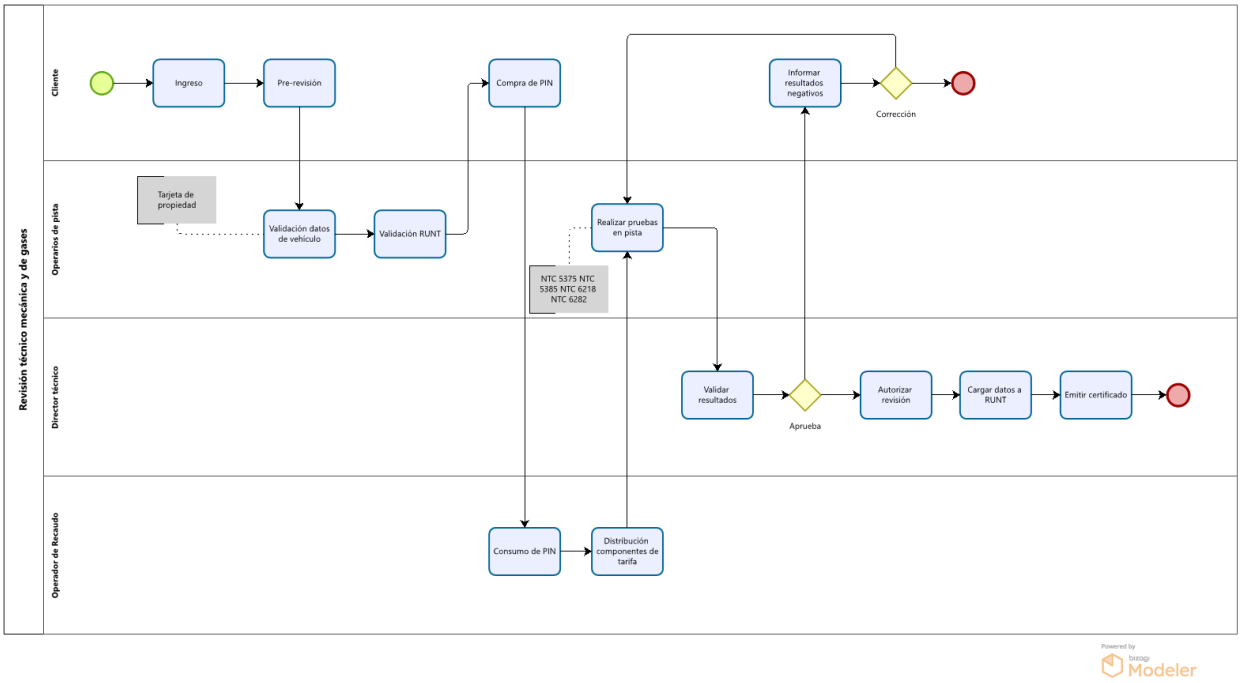


En este procedimiento se valida la asistencia de las personas que serán atendidas en el examen, de acuerdo a programación previa, se valida identidad de instructor y personas al principio y al final de la ejecución del examen.



PROCESO CDA

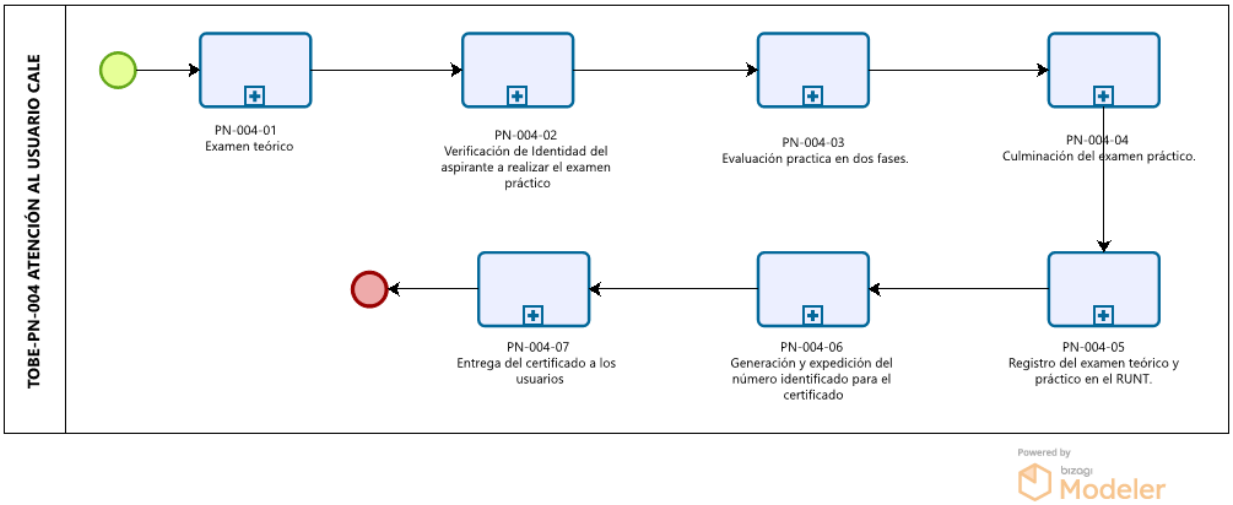
El proceso del CDA inicia con la llegada de tipo de vehículo que será evaluado a pista, se realizan las validaciones de tarjeta de propiedad del vehículo y verificación de estos datos con el RUNT para continuar con la ejecución de pruebas y terminar con la emisión del certificado de revisión técnico mecánica y de gases.

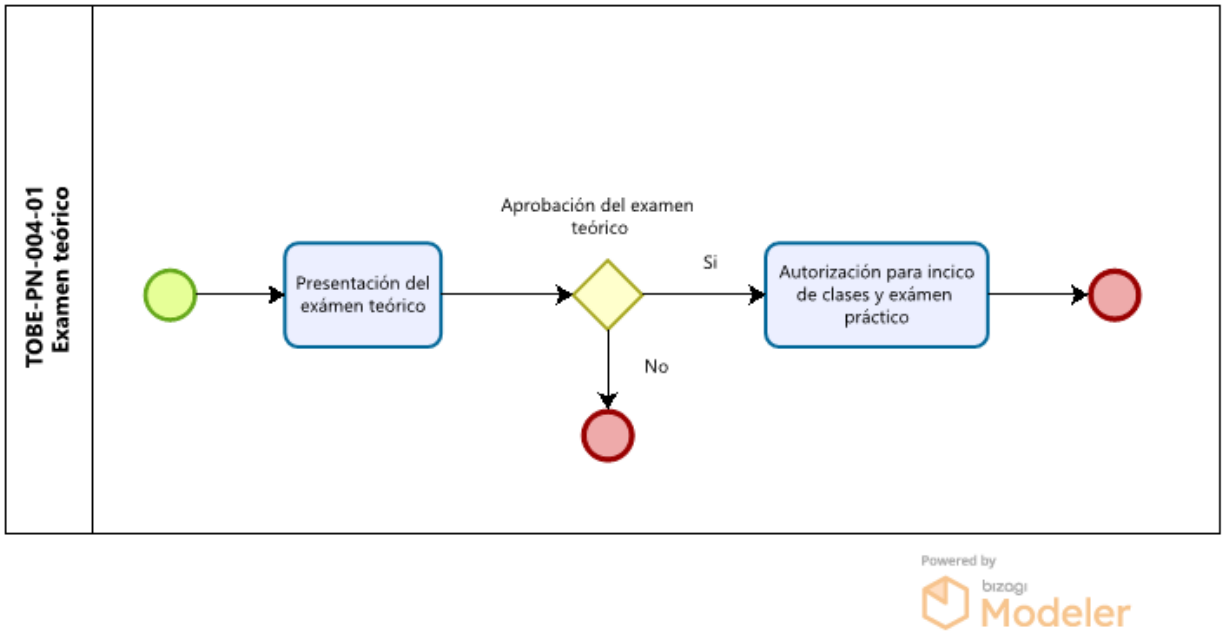


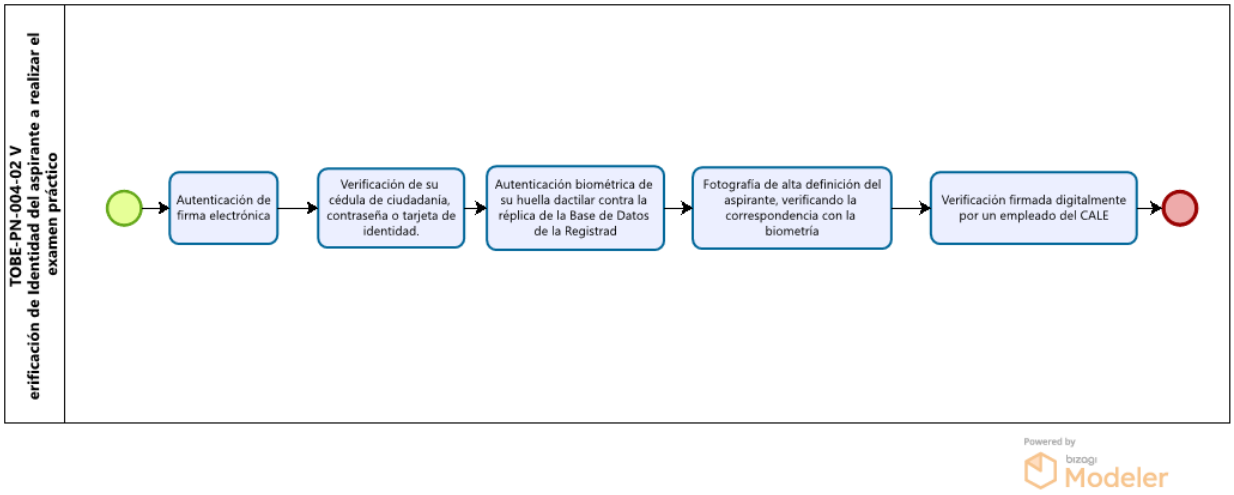
Los procedimientos a ejecutar en el CDA se encuentran en las normas NTC 5375, NTC 5385, NTC 6218 y NTC 6282.

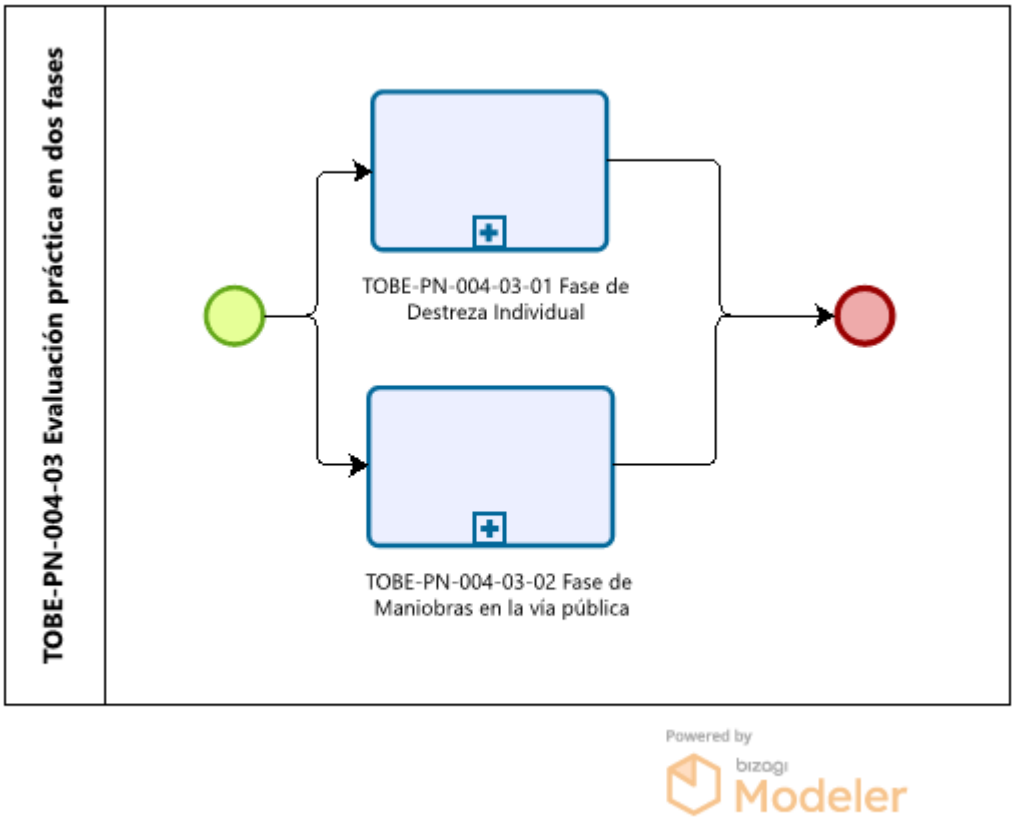
<u>PROCESO CALE</u>

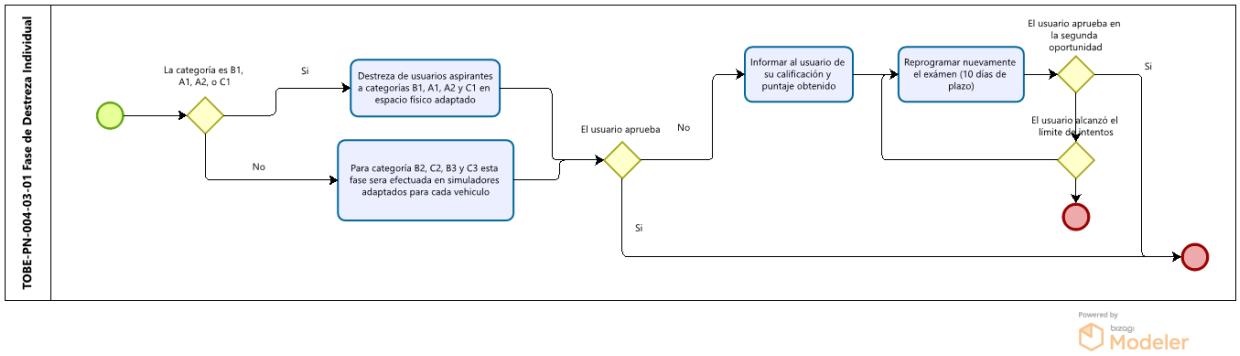
El proceso y los procedimientos asociados del CALE están determinados en la legislación vigente dado que este tipo de OAT no se encuentra en operación.


TOBE-PN-004 ATENCIÓN AL USUARIO CALE
PN-004-01
Examen teórico
PN-004-02
Verificación de Identidad del aspirante a realizar el examen práctico
PN-004-03
Evaluación practica en dos fases.
PN-004-04
Culminación del examen práctico.
PN-004-05
Registro del examen teórico y práctico en el RUNT.
PN-004-06
Generación y expedición del número identificado para el certificado
PN-004-07
Entrega del certificado a los usuarios
Powered by
bizagi
Modeler


TOBE-PN-004-01
Examen teórico
Presentación del exámen teórico
Aprobación del examen teórico
Si
No
Autorización para incico de clases y exámen práctico
Powered by
bizagi
Modeler

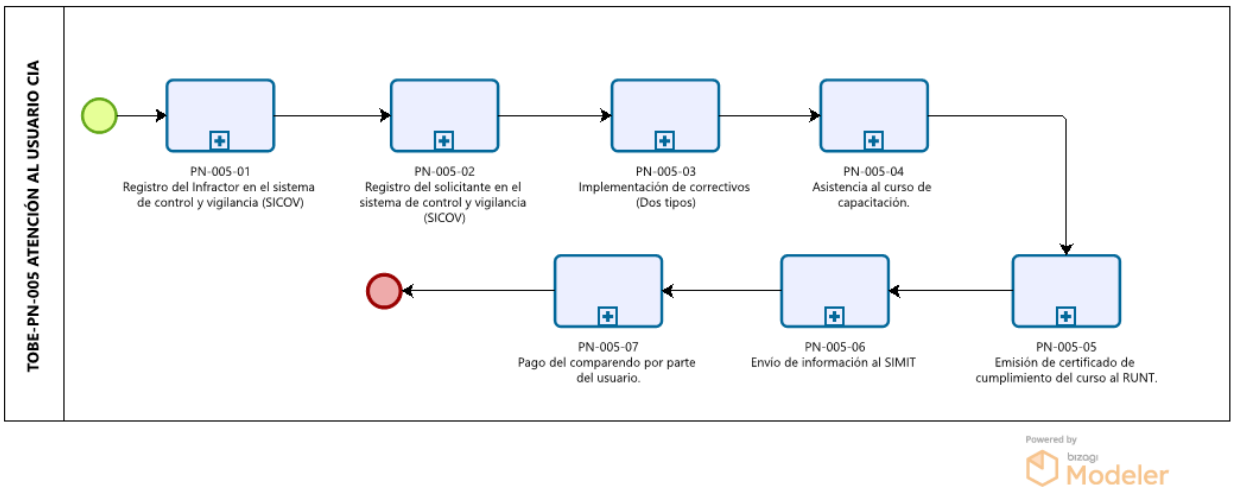

TOBE-PN-004-02 V
erificación de Identidad del aspirante a realizar el examen práctico
Autenticación de firma electrónica
Verificación de su cédula de ciudadanía, contraseña o tarjeta de identidad.
Autenticación biométrica de su huella dactilar contra la réplica de la Base de Datos de la Registrad
Fotografía de alta definición del aspirante, verificando la correspondencia con la biometría
Verificación firmada digitalmente por un empleado del CALE
Powered by
bizagi
Modeler

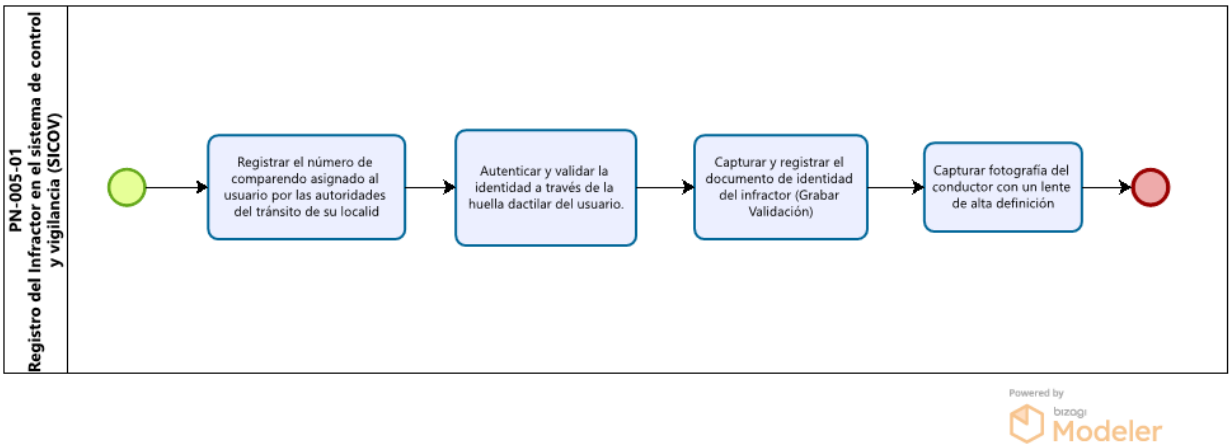

TOBE-PN-004-03 Evaluación práctica en dos fases
TOBE-PN-004-03-01 Fase de Destreza Individual
TOBE-PN-004-03-02 Fase de Maniobras en la vía pública
Powered by
bizagi
Modeler

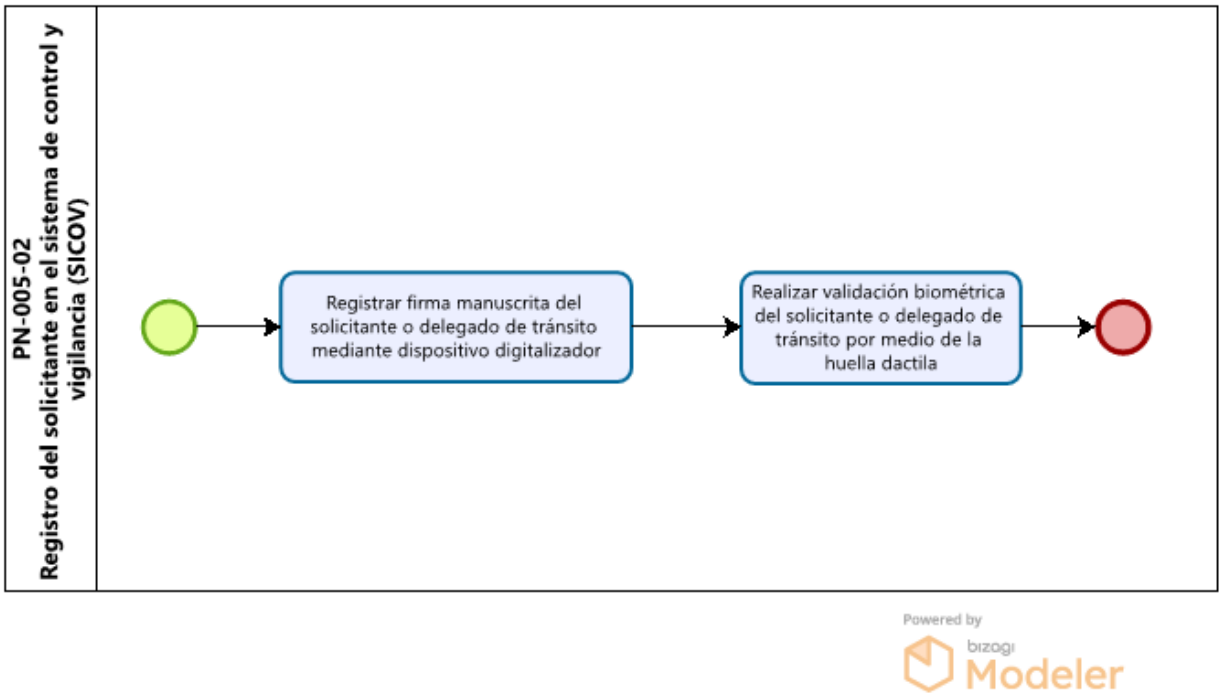


PROCESOS CIA

El proceso y los procedimientos asociados del CIA están determinados en la legislación vigente dado que este tipo de OAT no se encuentra en operación.







6.1.1.2 Servicios de negocio

Los servicios de negocio para el estado futuro se extienden tomando como base el estado actual, pero incorporando servicios adicionales que permiten enlazar los componentes de negocio con los componentes de los dominios tecnológicos como son

datos, aplicaciones, tecnología y seguridad. A continuación, se muestra el catálogo de servicios.

Dominio del servicio	Tipo de servicio	Descripción Tipo de servicio	Componente del Tipo de servicio	Descripción del componente
1.0 Servicio al cliente	1.1 Relaciones con el cliente	Este tipo de servicio se utiliza para planificar, programar y controlar las actividades entre el cliente y la empresa, tanto antes como después de un producto o servicio que se ofrece.	1.1.1 Gestión de Call Center	Se utiliza para manejar las ventas y/o servicios vía call center al cliente final
			1.1.2 Análisis de la información de cliente	Este componente permite el análisis de los clientes de la organización, así como la calificación de información de terceros en la relación con los clientes de la organización
			1.1.3 Mercadeo y ventas	Este componente permite realizar la promoción de un producto o servicio y la captación de nuevos clientes
			1.1.4 Gestión de productos	Este componente permite la creación

Dominio del servicio	Tipo de servicio	Descripción Tipo de servicio	Componente del Tipo de servicio	Descripción del componente
				y mantenimiento de productos y servicios
			1.1.5 Gestión de marcas	Este componente permite dar soporte a la aplicación de un nombre comercial de un producto o servicio, así como desarrollar el conocimiento de este
			1.1.6 Gestión de cuentas de clientes	Este componente permite dar soporte al mantenimiento y entrega de los servicios o productos de la Organización asociadas a una cuenta de cliente.

Dominio del servicio	Tipo de servicio	Descripción Tipo de servicio	Componente del Tipo de servicio	Descripción del componente
			1.1.7 Gestión de perfiles y contactos	Este componente permite proporcionar una visión global y comprensiva de la interacción con todos los clientes, incluido, llamadas, correo electrónico, correspondencia y reuniones. De igual forma, prevee el mantenimiento de la cuenta del cliente, empresa e información personal

Dominio del servicio	Tipo de servicio	Descripción Tipo de servicio	Componente del Tipo de servicio	Descripción del componente
			1.1.8 Gestión de relaciones con proveedores y asociados	Este componente permite proporcionar un marco para promover la colaboración efectiva entre una organización y sus proveedores y asociados, en particular los miembros de la cadena de suministro (por ejemplo, canal y alianzas, distribuidores, agentes, intermediarios y concesionarios), otros terceros que soportan las operaciones y la prestación de servicios a

Dominio del servicio	Tipo de servicio	Descripción Tipo de servicio	Componente del Tipo de servicio	Descripción del componente
				clientes de una organización; incluye la evaluación del desempeño de los proveedores y asociados, si es necesario
			1.1.9 Retroalimentación del cliente	Este componente se utiliza para recopilar, analizar y tramitar las observaciones y comentarios de los clientes de la Organización
			1.1.10 Encuestas	Este componente se utiliza para recopilar información útil de los clientes de la Organización

Dominio del servicio	Tipo de servicio	Descripción Tipo de servicio	Componente del Tipo de servicio	Descripción del componente
	1.2 Preferencias del cliente	Este tipo de servicio se utiliza para desarrollar las capacidades de la organización para cambiar la interfaz de usuario y la forma en que se muestran los datos al cliente.	1.2.1 Personalización	Este componente permite cambiar una interfaz de usuario y la forma como se muestran los datos
			1.2.2 Suscripciones	Este componente permite al cliente unirse a un foro, lista de servicios o lista de correo
			1.2.3 Alertas y Notificaciones	Este componente permite a un cliente ser contactado en relación con la subscripción o servicios de interés
	1.3 Asistencia al cliente	Este tipo de servicio se utiliza para desarrollar las capacidades que permiten a los clientes buscar proactivamente la asistencia y el	1.3.1 Ayuda en Línea	Este componente provee una interface electrónica para asistencia al cliente
			1.3.2 Tutorías en Línea	Este componente provee una interface

Dominio del servicio	Tipo de servicio	Descripción Tipo de servicio	Componente del Tipo de servicio	Descripción del componente
		servicio de la organización.		electrónica para asistir e instruir a los clientes
			1.3.3 Autoservicio	Este componente permite a los clientes de la Organización inscribirse para un servicio en particular por iniciativa propia
			1.3.4 Reservas y Registros	Este componente permite la inscripción electrónica y confirmación de los servicios
			1.3.5 Soporte Multilengua	Este componente permite el acceso a los datos en información en varios idiomas
			1.3.6 Solicitud de Asistencia	Este componente permite dar soporte al cliente en sitio o

Dominio del servicio	Tipo de servicio	Descripción Tipo de servicio	Componente del Tipo de servicio	Descripción del componente
				vía medios electrónicos (p.e. mesa de ayuda, servicios de asistencia remota, etc.)
			1.3.7 Programación	Este componente permite definir el conjunto de capacidades que apoyan el plan para la realización del trabajo o servicio para satisfacer las necesidades de los clientes de una organización
2.0 Automatización de Procesos	2.1 Localización y Flujo de Trabajo	Las capacidades dentro de este tipo de servicio ofrecen vigilancia automática y el	2.1.1 Seguimiento del Proceso	Permitir el seguimiento de las actividades dentro del ciclo económico

Dominio del servicio	Tipo de servicio	Descripción Tipo de servicio	Componente del Tipo de servicio	Descripción del componente
		envío de documentos a los usuarios responsables de trabajar con ellos para apoyar cada paso del ciclo de negocios.	2.1.2 Manejo de Casos	Gestionar el ciclo de vida de una reclamación o investigación particular dentro de una organización para incluir la creación, el enrutamiento, la localización, la asignación y el cierre de un caso, así como la colaboración entre los responsables de casos
			2.1.3 Resolución de Conflictos	Apoyar la conclusión de la discordia o diferencias dentro del ciclo económico
	2.2 Enrutamiento y Agendamiento	Las capacidades dentro de este tipo de servicio	2.2.1 Gestión de Correspondencia Entrante	Gestionar la comunicación externa iniciada

Dominio del servicio	Tipo de servicio	Descripción Tipo de servicio	Componente del Tipo de servicio	Descripción del componente
		proporcionan direccionamiento automático y la asignación, la asignación de tiempo para una acción o evento en particular.		entre una organización y sus grupos de interés
			2.2.2 Gestión de Correspondencia de Salida	Gestionar la comunicación interna iniciada entre una organización y sus grupos de interés
3.0 Gestión de Negocio	3.1 Gestión de procesos de negocio	Las capacidades dentro de este tipo de servicio regulan las actividades que rodean el ciclo de negocio de una organización a través de los procesos.	3.1.1 Gestión del Cambio	Este componente controla el proceso de actualizaciones o modificaciones a los documentos existentes, software o procesos de negocio de una organización
			3.1.2 Gestión de la Configuración	Este componente controla los entornos de hardware y software, así como los documentos de una organización

Dominio del servicio	Tipo de servicio	Descripción Tipo de servicio	Componente del Tipo de servicio	Descripción del componente
			3.1.3 Gestión de Requisitos	Este componente recopila, analiza y responde a las necesidades y requisitos de los esfuerzos de una organización
			3.1.4 Gestión de Programa / Proyecto	Este componente administra y controla un esfuerzo específico de una organización
			3.1.5 Gestión de Gobierno / Política	Este componente influye y determina las decisiones, acciones, reglas de negocio y otros asuntos dentro de una organización
			3.1.6 Gestión de la Calidad	Este componente determina el nivel que un producto o servicio satisface los

Dominio del servicio	Tipo de servicio	Descripción Tipo de servicio	Componente del Tipo de servicio	Descripción del componente
				requisitos de los clientes.
			3.1.7 Gestión de Reglas de Negocio	Este componente Administra los procesos empresariales que apoyan a la organización y sus políticas
			3.1.8 Gestión de Riesgos	Este componente apoya la identificación, análisis, evaluación y tratamiento de riesgos en lo que respecta a una meta, tarea, decisión a corto, mediano y largo plazo.
	3.2 Gestión organizacional	Las capacidades dentro de este tipo de servicio apoyan tanto la colaboración	3.2.1 Grupo de Trabajo	Este componente da soporte de múltiples usuarios que trabajan en tareas relacionadas

Dominio del servicio	Tipo de servicio	Descripción Tipo de servicio	Componente del Tipo de servicio	Descripción del componente
		como la comunicación dentro de una organización.	3.2.2 Gestión de Red	Este componente controla y mantiene una red de comunicaciones con el fin de diagnosticar problemas y recopilar estadísticas.
	3.3 Gestión de Inversiones	Las Capacidades dentro de este tipo de servicio gestionan los activos financieros y el capital de una organización.	3.3.1 Planificación y Gestión Estratégica	Este componente soporta la determinación de objetivos a largo plazo y la identificación del mejor enfoque para el logro de esos objetivos
			3.3.2 Gestión de Portafolio	Este componente soporta la administración de un grupo de inversiones mantenidas por una organización

Dominio del servicio	Tipo de servicio	Descripción Tipo de servicio	Componente del Tipo de servicio	Descripción del componente
			3.3.3 Gestión del rendimiento	Este componente mide la eficacia de los activos y el capital financiero de una organización
	3.4 Gestión de la Cadena de Suministro	Las capacidades dentro de este tipo de servicio planean, programan y controlan la cadena de suministro y las interacciones entre proveedores y funciones, que permiten hacer o ensamblar materiales y productos a través de la cadena (p.e. del fabricante al mayorista, del	3.4.1 Compras	Este componente soporta la gestión de órdenes de compra de productos y servicios
			3.4.2 Gestión de Abastecimiento	Este componente soporta el suministro de bienes o servicios, así como el seguimiento y el análisis de costos de estos bienes
			3.4.3 Gestión de inventario	Este componente provee el equilibrio entre los niveles de servicio al cliente con la inversión en inventarios

Dominio del servicio	Tipo de servicio	Descripción Tipo de servicio	Componente del Tipo de servicio	Descripción del componente
		mayorista al minorista y del minorista al cliente o consumidor final).	3.4.4 Gestión de catálogos	Este componente apoya la lista de productos o servicios que ofrece una organización disponible
			3.4.5 Pedidos / Compras	Este componente permite la colocación de pedido de un producto o servicio
			3.4.6 Seguimiento de Solicitud, Facturación y Aprobación	Este componente soporta la identificación del estado de una orden dentro del ciclo de compras de la organización.
			3.4.7 Sistemas online	Este componente soporta el equivalente a la gestión de compras mediante medios electrónicos en donde se colocan

Dominio del servicio	Tipo de servicio	Descripción Tipo de servicio	Componente del Tipo de servicio	Descripción del componente
				órdenes y se realizan trámites de compras
			3.4.8 Gestión de Almacenes	Este componente gestiona el almacenamiento y el movimiento de materiales dentro de un almacén, incluye los procesos de: recepción de materiales, preparación de pedidos, embalaje, etiquetado y entrega con la descarga de inventarios.
			3.4.9 Gestión de devoluciones	Este componente recoge, analiza y resuelve devoluciones o cancelaciones de servicios

Dominio del servicio	Tipo de servicio	Descripción Tipo de servicio	Componente del Tipo de servicio	Descripción del componente
			3.4.10 Logística y Transporte	Este componente provee el manejo eficiente de cargas, medios de transporte (aéreo, marítimo, fluvial, terrestre) y la gestión del tráfico de los despachos.
4.0 Servicios de Contenidos, Documentales, Archivo y Conocimiento	4.1 Gestión de Contenido	Las capacidades dentro de este tipo de servicio a gestionan el almacenamiento, mantenimiento y recuperación de los documentos y la información de un sistema o sitio web	4.1.1 Creación de Contenido	Este componente permite la creación de tutoriales, cursos, sitios web, CD ROMS, y otros programas interactivos
			4.1.2 Revisión y Aprobación de Contenido	Este componente permite la aprobación de programas interactivos
			4.1.3 Etiquetado y agregado	Este componente permite apoyar la identificación de contenido

Dominio del servicio	Tipo de servicio	Descripción Tipo de servicio	Componente del Tipo de servicio	Descripción del componente
				específico dentro de un conjunto más amplio de contenidos para la creación de colecciones y resúmenes
			4.1.4 Publicación de contenidos y entrega	Este componente permite la propagación de programas interactivos
			4.1.5 Gestión de derechos de autor	Controla y regula el derecho de autor como un conjunto de normas jurídicas y principios que afirman los derechos morales y patrimoniales que la ley concede a los autores, por el solo hecho de la creación de una obra literaria,

Dominio del servicio	Tipo de servicio	Descripción Tipo de servicio	Componente del Tipo de servicio	Descripción del componente
				artística, musical, científica o didáctica, esté publicada o inédita.
	4.2 Gestión Documental	Las capacidades dentro de este tipo de servicio controlan la captura y el mantenimiento de los documentos y archivos de la Organización	4.2.1 Digitalización de documentos y lectura OCR (reconocimiento óptico de caracteres)	Este componente permite el soporte de la digitalización de documentos
			4.2.2 Documento de Referencia	Este componente apoya la redirección a otros documentos e información relacionada para contenido
			4.2.3 Revisión de Documentos	Este componente apoya el control de versiones y edición de contenidos y documentos
			4.2.4 Biblioteca/Almacenamiento	Este componente soporta el

Dominio del servicio	Tipo de servicio	Descripción Tipo de servicio	Componente del Tipo de servicio	Descripción del componente
				almacenamiento de datos y archivo
			4.2.5 Revisión y aprobación del documento	Este componente apoya la edición y la aprobación de los documentos antes de liberarlos para consulta y uso
			4.2.6 Conversión de Documentos	Este componente soporta el cambio de archivos de un tipo de formato a otro
			4.2.7 Indexación	Este componente soporta la recuperación rápida de los documentos a través de una construcción de numeración estructurada
			4.2.8 Clasificación	Este componente soporta la configuración y

Dominio del servicio	Tipo de servicio	Descripción Tipo de servicio	Componente del Tipo de servicio	Descripción del componente
				clasificación de los diferentes tipos de documentos
	4.3 Gestión del Conocimiento	Las capacidades dentro de este tipo de servicio permiten identificar, recoger y transformar documentos, informes y otras fuentes en información significativa que se convierta en un activo de la organización (know-how de la organización).	4.3.1 Recuperación de Información	Este componente permite el acceso a los datos y la información para uso por parte de la organización y sus partes interesadas
			4.3.2 Mapeo de la Información / Taxonomía	Este componente soporta la creación y el mantenimiento de las relaciones entre las entidades de datos, estándares de nomenclatura y clasificación
			4.3.3 Intercambio de Información	Este componente soporta el uso de los documentos y datos en un entorno multi-usuario para el uso

Dominio del servicio	Tipo de servicio	Descripción Tipo de servicio	Componente del Tipo de servicio	Descripción del componente
				por parte de la organización y sus grupos de interés
			4.3.4 Categorización	Este componente permite la clasificación de los datos y la información en capas específicas o tipos de soporte a la organización
			4.3.5 Ingeniería de Conocimiento	Este componente soporta la transformación de los conocimientos de un experto en una base de conocimiento a través de un sistema experto
			4.3.6 Captura de Conocimiento	Este componente facilita la recolección de datos e información

Dominio del servicio	Tipo de servicio	Descripción Tipo de servicio	Componente del Tipo de servicio	Descripción del componente
			4.3.7 Distribución del conocimiento y entrega	Este componente soporta la transferencia de conocimiento al cliente final
			4.3.8 Documentos Inteligentes	Este componente soporta la interacción de la información y los procesos (lógica de negocio), las reglas de uso entre los usuarios finales (p.e. la lógica y uso del documento esta parametrizada dentro del propio documento y se gestiona de acuerdo con estos parámetros)
	4.4 Gestión de Archivos	Las capacidades dentro de este tipo de servicio permiten	4.4.1 Registro vinculación/asociación	Este componente soporta la correlación entre los datos lógicos y

Dominio del servicio	Tipo de servicio	Descripción Tipo de servicio	Componente del Tipo de servicio	Descripción del componente
		almacenar, proteger, archivar, clasificar y retirar los documentos y la información.		conjuntos de información
			4.4.2 Retiro de Documentos	Este componente soporta la terminación o cancelación de documentos utilizados por la organización y sus clientes
			4.4.3 Gestión de derechos digitales	Este componente soporta las reclamaciones y la propiedad del capital intelectual y artefactos pertenecientes a una organización
5.0 Servicios de Análisis de Negocios	5.1 Análisis y estadísticas	Las capacidades dentro de este tipo de servicio examinan cuestiones de negocios, los	5.1.1 Matemático	Este componente soporta la formulación y el análisis matemático de modelos probabilísticos para fenómenos

Dominio del servicio	Tipo de servicio	Descripción Tipo de servicio	Componente del Tipo de servicio	Descripción del componente
		problemas y sus soluciones		aleatorios, el desarrollo y la investigación de métodos y principios para la inferencia estadística
			5.1.2 Estructural	Este componente soporta el uso de flujo de datos y diagramas de modelado de datos para la aplicación de un análisis sistemático de los datos
			5.1.3 Forense	Este componente soporta el análisis de los elementos físicos utilizando la ciencia y la tecnología para fines legales y de investigación

Dominio del servicio	Tipo de servicio	Descripción Tipo de servicio	Componente del Tipo de servicio	Descripción del componente
	5.2 Visualización	Las capacidades dentro de este tipo de servicio convierten los datos en forma de gráficos o imágenes.	5.2.1 Gráficos	Este componente soporta la presentación de la información en forma de diagramas o tablas
			5.2.2 Imágenes	Este componente soporta la creación de películas o imágenes electrónicas de imágenes o formularios en papel.
			5.2.3 Multimedia	Este componente soporta la representación de la información en más de una forma, incluir texto, audio, gráficos, gráficos animados y video de movimiento completo

Dominio del servicio	Tipo de servicio	Descripción Tipo de servicio	Componente del Tipo de servicio	Descripción del componente
			5.2.4 Mapas / Referenciación Geoespacial / Sistemas de Información Geográfica / GPS	Este componente proporciona la representación de la posición de la información a través de atributos como la elevación, latitud y longitud, y a través de coordenadas geográficas
			5.2.5 CAD	Este componente soporta el diseño asistido por computador
	5.3 Descubrimiento de Conocimiento	Las capacidades dentro de este tipo de servicio facilitan la identificación de información útil a partir de datos.	5.3.1 Minería de Datos	Este componente provee el descubrimiento eficiente de patrones valiosos y las relaciones dentro de una gran colección de datos

Dominio del servicio	Tipo de servicio	Descripción Tipo de servicio	Componente del Tipo de servicio	Descripción del componente
			5.3.2 Modelado	Este componente desarrolla las descripciones para explicar adecuadamente los datos pertinentes a los efectos de predicción, detección de patrones, la exploración o de la organización general de los datos
			5.3.3 Simulación	Este componente utiliza modelos simulados para imitar procesos reales
	5.4 Inteligencia de Negocio	Las capacidades dentro de este tipo de servicio proporcionan la información que	5.4.1 Gestión/previsión de la demanda	Este componente facilita la predicción de la producción suficiente para

Dominio del servicio	Tipo de servicio	Descripción Tipo de servicio	Componente del Tipo de servicio	Descripción del componente
		pertenece a la historia, el estado actual o proyecciones futuras de una organización.		satisfacer las ventas de una organización, de un producto o servicio
			5.4.2 Tablero de Control (Balance Scorecard)	Este componente soporta la inclusión y el análisis de los impactos positivos y negativos asociados a una decisión a través de los indicadores de la organización
			5.4.3 Soporte de Decisiones y Planificación	Este componente soporta el análisis de la información y predicción del impacto de las decisiones antes de que se lleven a cabo
	5.5 Informes	Las capacidades dentro de este tipo de servicio	5.5.1 Ad Hoc	Este componente soporta el uso de informes dinámicos

Dominio del servicio	Tipo de servicio	Descripción Tipo de servicio	Componente del Tipo de servicio	Descripción del componente
		organizan los datos en información útil		en función de las necesidades
			5.5.2 Estandarizada	Este componente soporta el uso de los informes preconcebidos o pre-escritos
			5.5.3 OLAP	Este componente soporta el análisis de la información que se ha resumido en vistas multidimensionales y jerarquías
6.0 Servicios Back Office	6.1 Gestión de Datos	Las capacidades dentro de este tipo de servicio ofrecen el uso, el procesamiento y la administración general de la información no estructurada.	6.1.1 Intercambio de Datos	Este componente soporta el intercambio de información entre múltiples sistemas o aplicaciones; incluye la verificación de los datos transmitidos que se recibieron inalterados

Dominio del servicio	Tipo de servicio	Descripción Tipo de servicio	Componente del Tipo de servicio	Descripción del componente
			6.1.2 Data Mart	Este componente soporta a un subconjunto de un almacén de datos para un solo departamento o función dentro de una organización
			6.1.3 Data Warehouse	Este componente soporta el archivado y almacenamiento de grandes volúmenes de datos
			6.1.4 Gestión de Metadatos	Este componente soporta el mantenimiento y administración de datos que describe los datos
			6.1.5 Limpieza de Datos	Este componente soporta la eliminación de datos incorrectos o

Dominio del servicio	Tipo de servicio	Descripción Tipo de servicio	Componente del Tipo de servicio	Descripción del componente
				innecesarios de una fuente de datos
			6.1.6 Extracción y Transformación	Este componente soporta la manipulación y el cambio de los datos
			6.1.7 Carga y Archivo	Este componente soporta la población de un origen de datos con datos externos
			6.1.8 Recuperación de Datos	Este Componente soporta la restauración y la estabilización de los conjuntos de datos a un estado coherente deseado
			6.1.9 Clasificación de Datos	Este componente permite la clasificación de los datos
	6.2 Recursos Humanos	Las capacidades dentro de este	6.2.1 Reclutamiento	Este componente soporta la

Dominio del servicio	Tipo de servicio	Descripción Tipo de servicio	Componente del Tipo de servicio	Descripción del componente
		tipo de servicio prevén la contratación y gestión de personal.		identificación y contratación de los empleados de una organización
			6.2.2 Gestión de currículum	Este componente soporta el mantenimiento y la administración de un empleado, experiencia de trabajo y las cualificaciones
			6.2.3 Desarrollo de Carrera y Retención	Este componente soporta el seguimiento de los resultados, así como el crecimiento profesional, avance y la retención de los empleados de una organización
			6.2.4 Reportes de Tiempo	Este componente soporta la

Dominio del servicio	Tipo de servicio	Descripción Tipo de servicio	Componente del Tipo de servicio	Descripción del componente
				presentación, aprobación y ajuste de horas de trabajo de un empleado
			6.2.5 Gestión de Incentivos	Este componente soporta el reconocimiento de los logros de los empleados de una organización
			6.2.6 Gestión de Beneficios	Este componente soporta la inscripción y participación en la compensación de una organización programas de beneficios
			6.2.7 Gestión de Retiro	Este componente soporta el pago de beneficios a los jubilados

Dominio del servicio	Tipo de servicio	Descripción Tipo de servicio	Componente del Tipo de servicio	Descripción del componente
			6.2.8 Administración de personal	Este componente soporta la adaptación entre los empleados y el potencial de las oportunidades de una organización, así como la modificación, adición y mantenimiento general de una información específica del empleado en la organización
			6.2.9 Entrenamiento/Capacitación	Este componente soporta la construcción activa de competencias de los empleados, para incluir la gama de capacitación de desarrollo

Dominio del servicio	Tipo de servicio	Descripción Tipo de servicio	Componente del Tipo de servicio	Descripción del componente
				profesional a la formación general
			6.2.10 Seguridad y Salud	Este componente soporta la seguridad y el bienestar físico de los empleados de una organización
			6.2.11 Gestión de Viajes	Este componente soporta el tránsito y la movilidad de los empleados de una organización con fines empresariales
	6.3 Gestión Financiera	Las capacidades dentro de este tipo de servicio proporcionan las prácticas contables y	6.3.1 Facturación y Contabilidad	Este componente soporta la carga, recopilación y presentación de las cuentas de una organización

Dominio del servicio	Tipo de servicio	Descripción Tipo de servicio	Componente del Tipo de servicio	Descripción del componente
		procedimientos que permitan el manejo de los ingresos, la financiación y los gastos.	6.3.2 Crédito/Cargo	Este componente soporta el uso de tarjetas de crédito o transferencias electrónicas de fondos para el pago y colección de productos o servicios
			6.3.3 Gestión de Gastos	Este componente soporte a la gestión y el reembolso de los gastos pagados por los empleados o por la organización
			6.3.4 Nómina y Salarios	Este componente soporta el involucramiento a la administración y determinación de la remuneración de los empleados
			6.3.5 Pago/Liquidación	Este componente soporta el proceso

Dominio del servicio	Tipo de servicio	Descripción Tipo de servicio	Componente del Tipo de servicio	Descripción del componente
				de cuentas por pagar
			6.3.6 Cobro de deudas	Este componente soporta el proceso de cuentas por cobrar
			6.3.7 Gestión de Ingresos	Este componente soporta la asignación y re-inversión de recursos monetarios por medio de créditos o del capital de trabajo en una organización
			6.3.8 Controles Internos	Este componente soporta los métodos y procedimientos utilizados por la organización para salvaguardar sus activos, producen datos contables precisos e informes,

Dominio del servicio	Tipo de servicio	Descripción Tipo de servicio	Componente del Tipo de servicio	Descripción del componente
				contribuyen a operaciones eficientes, y alentar al personal a que se adhieran a las políticas de gestión y requisitos de la misión
			6.3.9 Auditoría	Este componente soporta el examen y verificación de los registros para precisar el cumplimiento de los requisitos legales, éticos, contables y aplicables a la organización por entes externos o por entes internos.
			6.3.10 Gestión de costos por actividades	Este componente soporta un conjunto específico y definido de tareas relacionadas con

Dominio del servicio	Tipo de servicio	Descripción Tipo de servicio	Componente del Tipo de servicio	Descripción del componente
				las finanzas para un objetivo dado
			6.3.11 Conversión de Moneda	Este componente soporta los cálculos y la diferencia entre múltiples medios de intercambio monetarios
	6.4 Gestión de Activos y Materiales	Las capacidades dentro de este tipo de servicios proporcionan apoyo a la adquisición, la supervisión y el seguimiento de los activos de una organización.	6.4.1 Administración de Propiedades y Activos	Este componente soporta la identificación, planificación y asignación de recursos, físicos y de capital de la organización
			6.4.2 Identificación y catalogación de activos	Este componente soporta la identificación, catalogación y las especificaciones de los activos disponibles

Dominio del servicio	Tipo de servicio	Descripción Tipo de servicio	Componente del Tipo de servicio	Descripción del componente
			6.4.3 Transferencia de activos	Este componente soporta el movimiento, asignación y reposición de activos
			6.4.4 Gestión de Instalaciones	Este componente soporta la construcción, gestión y mantenimiento de las instalaciones para la organización
			6.4.5 Gestión Informática / Automatización	Este componente soporta la identificación, actualización, distribución y sustitución de dispositivos físicos, incluyendo los servidores y equipos de sobremesa, que se utilizan para

Dominio del servicio	Tipo de servicio	Descripción Tipo de servicio	Componente del Tipo de servicio	Descripción del componente
				facilitar la prestación de productos y/o servicios, y actividades orientadas a procesos
	6.5 Desarrollo e Integración	Las capacidades dentro de este tipo de servicio proporcionan la comunicación entre las aplicaciones de hardware/software y las actividades asociadas con el despliegue de aplicaciones de software.	6.5.1 Sistemas legados	Este componente soporta la comunicación entre la nueva generación de tecnología, hardware/software y aplicaciones; y la generación instalada de tecnología, hardware/software y aplicaciones.
			6.5.2 Integración de Aplicaciones Empresariales	Este componente soporta el rediseño de los sistemas de información dispares en un solo

Dominio del servicio	Tipo de servicio	Descripción Tipo de servicio	Componente del Tipo de servicio	Descripción del componente
				sistema que utiliza un conjunto común de estructuras de datos y reglas
			6.5.3 Integración de Datos	Este componente soporta la organización de los datos de fuentes de datos separadas en una sola fuente utilizando el middleware o bus de integración de aplicaciones, así como la modificación de los modelos de datos del sistema para capturar información nueva dentro de un solo sistema
			6.5.4 Instrumentación y Pruebas	Este componente soporta a la validación de las

Dominio del servicio	Tipo de servicio	Descripción Tipo de servicio	Componente del Tipo de servicio	Descripción del componente
				aplicaciones o la capacidad del sistema y solución de necesidades
			6.5.5 Desarrollo de Software	Este componente soporta la creación tanto gráfica como transaccional de aplicaciones de software
	6.6 Gestión de capital humano y Fuerza de trabajo	Las capacidades dentro de este tipo de servicio prevén la planificación y supervisión del personal de una organización	6.6.1 Planificación y asignación de recursos	Este componente soporta la determinación de la dirección estratégica, la identificación y establecimiento de programas y procesos y la asignación de recursos (capital y trabajo) entre esos programas y procesos

Dominio del servicio	Tipo de servicio	Descripción Tipo de servicio	Componente del Tipo de servicio	Descripción del componente
			6.6.2 Gestión por competencias	Este componente soporta la competencia de los empleados en la entrega de productos o servicios de una organización
			6.6.3 Directorio de Fuerza Laboral / Localizador	Este componente soporta la base de datos de los empleados y su paradero
			6.6.4 Equipo de Gestión / Organización	Este componente soporta a la estructura de la jerarquía y la identificación de los empleados dentro de los subgrupos de una organización
			6.6.5 Gestión Contingente de Fuerza de Trabajo	Este componente soporta la continuidad de las operaciones de

Dominio del servicio	Tipo de servicio	Descripción Tipo de servicio	Componente del Tipo de servicio	Descripción del componente
				negocio de una organización a través de la identificación de personal de la organización para atención de incidentes y emergencias
			6.6.6 Optimización de la fuerza de trabajo	Este componente soporta la contratación y la reestructuración de los empleados y sus roles dentro de la organización
7.0 Servicios de Apoyo	7.1 Gestión de Seguridad	Las capacidades dentro de este tipo de servicio protegen los sistemas de información, la información y las instalaciones	7.1.1 Identificación y autenticación	Este componente soporta la obtención de información sobre los usuarios que intentan iniciar sesión en un sistema o aplicación con fines de seguridad y

Dominio del servicio	Tipo de servicio	Descripción Tipo de servicio	Componente del Tipo de servicio	Descripción del componente
		físicas de una organización.		la validación de los usuarios
			7.1.2 Control de Acceso	Este componente soporta la gestión de los permisos para iniciar sesión en una computadora, aplicación, servicio o red; incluye la gestión de usuarios y los privilegios de administración. Adicionalmente permite los controles de acceso físicos a las instalaciones de la organización

Dominio del servicio	Tipo de servicio	Descripción Tipo de servicio	Componente del Tipo de servicio	Descripción del componente
			7.1.3 Criptografía	Este componente soporta el uso y manejo de los sistemas de cifrado, incluido el cifrado y procesos de descifrado, para garantizar la confidencialidad e integridad de los datos
			7.1.4 Gestión de Firma Digital	Este componente soporta el uso y manejo de la firma electrónica para el apoyo autenticación e integridad de los datos; incluye infraestructura de clave pública (PKI)
			7.1.5 Prevención de Intrusión	Este componente Incluye las pruebas de intrusión y otras medidas para

Dominio del servicio	Tipo de servicio	Descripción Tipo de servicio	Componente del Tipo de servicio	Descripción del componente
				prevenir el acceso no autorizado a un sistema de información
			7.1.6 Detección de Intrusos	Este componente soporta la detección de acceso no autorizado a un sistema de información
			7.1.7 Respuesta a Incidentes	Este componente proporciona respuesta activa y la remediación de un incidente de seguridad que ha permitido acceso no autorizado a un sistema de información
			7.1.8 Captura de fichero de auditoría y análisis	Este componente soporta la identificación y el seguimiento de las

Dominio del servicio	Tipo de servicio	Descripción Tipo de servicio	Componente del Tipo de servicio	Descripción del componente
				actividades dentro de una aplicación, sistema, o redes (manejo de logs)
			7.1.9 Certificación y Acreditación	Este componente soporta la certificación y acreditación de la información
			7.1.10 Gestión de MSI y presentación de Informes	Este componente soporta la Gestión y presentación de informes de conformidad con el Manual de Seguridad de Información (MSI)
			7.1.11 Protección de Virus	Este componente proporciona el servicio antivirus para prevenir, detectar y remediar la infección de activos informáticos

Dominio del servicio	Tipo de servicio	Descripción Tipo de servicio	Componente del Tipo de servicio	Descripción del componente
	7.2 Colaboración	Las capacidades dentro de este tipo de servicio permiten la comunicación simultánea y el intercambio de contenidos, horarios, mensajes e ideas dentro de una organización.	7.2.1 Correo electrónico (e-mail)	Este componente soporta la transmisión de notas y mensajes a través de una red
			7.2.2 Foros de Discusión	Este componente soporta el registro continuo de los comentarios y opiniones sobre un tema o asunto determinado. Los ejemplos incluyen: blogs, tablones de anuncios y Twitter
			7.2.3 Biblioteca de documentos	Este componente la agrupación y el archivo de los archivos y registros en el servidor
			7.2.4 Calendario compartido	Este componente permite a todo un equipo, así como las personas para ver, añadir y

Dominio del servicio	Tipo de servicio	Descripción Tipo de servicio	Componente del Tipo de servicio	Descripción del componente
				modificar cada uno de los demás horarios, reuniones y actividades
			7.2.5 Gestión de Tareas	Este componente soporte a una empresa o función específica asignada a un empleado
			7.2.6 Redes Sociales	Este componente apoya la capacidad de compartir contenido y construir relaciones.
	7.3 Búsqueda	Las capacidades dentro de este tipo de servicio prevé la consulta de sondeo y de los datos específicos de una fuente de datos	7.3.1 Consultas	Este componente soporta la recuperación de apoyo a los registros que cumplan los criterios de selección de

Dominio del servicio	Tipo de servicio	Descripción Tipo de servicio	Componente del Tipo de servicio	Descripción del componente
				consultas específicas
			7.3.2 Clasificación de precisión	Este componente soporta la selección y recuperación de registros clasificados para optimizar la precisión en las búsquedas
			7.3.3 Clasificación	Este componente soporta la selección y recuperación de registros organizados por características compartidas en contenido o contexto
			7.3.4 Coincidencia de patrones	Este componente soporta la recuperación de los registros generados a partir de una

Dominio del servicio	Tipo de servicio	Descripción Tipo de servicio	Componente del Tipo de servicio	Descripción del componente
				fuente de datos mediante la imputación de características basadas en patrones dentro del contenido o contexto
	7.4 Comunicación	Las capacidades dentro de este tipo de servicio transmiten datos, mensajes e información en múltiples formatos y protocolos.	7.4.1 Comunicación en tiempo real (chats)	Este componente soporta la capacidad de conferencia entre dos o más usuarios en una red de área local o de Internet
			7.4.2 Mensajería instantánea	Este componente soporta la conferencia a través de mensajería instantánea (mensajes de texto) a través de una red de área local o

Dominio del servicio	Tipo de servicio	Descripción Tipo de servicio	Componente del Tipo de servicio	Descripción del componente
				Internet entre dos o más personas
			7.4.3 Audioconferencia	Este componente soporta las sesiones de comunicación de audio entre las personas que se encuentran geográficamente distantes
			7.4.4 Videoconferencia	Este componente soporta las sesiones de comunicación de vídeo de apoyo entre las personas que se encuentran geográficamente distantes
			7.4.5 Gestión de Noticias y eventos	Este componente monitorea servidores, estaciones de trabajo y los

Dominio del servicio	Tipo de servicio	Descripción Tipo de servicio	Componente del Tipo de servicio	Descripción del componente
				dispositivos de red para determinar eventos rutinarios y no rutinarios y gestionar avisos a usuarios
			7.4.6 Gestión de la Comunidad	Este componente soporta a la administración de grupos en línea que comparten intereses comunes
			7.4.7 Integración Informática / Telefonía	Este componente soporta la conectividad entre servidores, hardware/software y equipos de telecomunicaciones en un solo sistema lógico
			7.4.8 Comunicaciones de Voz	Este componente proporciona comunicaciones de telefonía u otros

Dominio del servicio	Tipo de servicio	Descripción Tipo de servicio	Componente del Tipo de servicio	Descripción del componente
				medios de transmisión de voz
	7.5 Gestión de Tecnología	Las capacidades dentro de este tipo de servicios dan apoyo a la administración y mantenimiento de los activos de tecnología de la organización, incluyendo el hardware, software, infraestructura, licencias y componentes del servicio que conforman dichos activos.	7.5.1 Gestión de licencias	Este grupo soporta la adquisición, actualización y seguimiento de los contratos legales de uso y licenciamiento para los sistemas de software y aplicaciones
			7.5.2 Sistemas de Control Remoto	Este componente soporta el monitoreo, administración y uso de las aplicaciones y sistemas empresariales desde locaciones fuera del entorno del sistema.

Dominio del servicio	Tipo de servicio	Descripción Tipo de servicio	Componente del Tipo de servicio	Descripción del componente
			7.5.3 Monitoreo de recursos del sistema	Este componente soporta el equilibrio y la asignación de recursos de memoria, uso, espacio en disco y rendimiento de las computadoras y sus aplicaciones
			7.5.4 Distribución de software	Este componente soporta la utilización, instalación y actualización de programas informáticos, aplicaciones y componentes de servicio

Dominio del servicio	Tipo de servicio	Descripción Tipo de servicio	Componente del Tipo de servicio	Descripción del componente
			7.5.5 Computación en la nube	Los servicios en la nube son servicios que se utilizan a través de Internet. Puede implementarse según los siguientes modelos de nube: Nube pública Este tipo de nube ofrece sus servicios a cualquier usuario de internet. Sus servidores y almacenamiento pertenecen al proveedor del servicio y el cliente sólo paga generalmente por el espacio de almacenamiento o el ancho de banda que consumen.

Dominio del servicio	Tipo de servicio	Descripción Tipo de servicio	Componente del Tipo de servicio	Descripción del componente
				Nube privada Estas nubes ofrecen sus servicios a un número limitado de usuarios a través de una red de una empresa. Esta red puede localizarse en las propias instalaciones de la empresa o en las de un proveedor externo. Nube híbrida Como su propio nombre indica, este tipo de nube es fruto de una combinación de las dos anteriores. En esta se almacenan datos en nubes públicas o privadas

Dominio del servicio	Tipo de servicio	Descripción Tipo de servicio	Componente del Tipo de servicio	Descripción del componente
				en función de las necesidades. Por ejemplo, se puede guardar la información más delicada en la nube privada y la menos crítica en la pública o también usar la nube pública para cuando haya picos de trabajo que exijan un mayor rendimiento. Multicloud Se trata de una opción que está siendo adoptada por muchas entidades y que consiste en varias nubes entre las que se desplazan los

Dominio del servicio	Tipo de servicio	Descripción Tipo de servicio	Componente del Tipo de servicio	Descripción del componente
				distintos servicios y que pueden trabajar simultáneamente. Con multicloud los clientes se blindan ante posibles interrupciones del servicio.
			7.5.6 Seguimiento de incidentes de TI	Este componente soporta la recepción y seguimiento de las cuestiones y problemas notificados por los usuarios en el uso de los sistemas de TI, incluyendo las llamadas al servicio de asistencia (Help-Desk)

Dominio del servicio	Tipo de servicio	Descripción Tipo de servicio	Componente del Tipo de servicio	Descripción del componente
	7.6 Gestión de Formularios	Las capacidades dentro de este tipo de servicios dan apoyo a la creación, modificación y uso de los documentos físicos o electrónicos que se utilizan para capturar información dentro del ciclo de negocio.	7.6.1 Creación de formularios	Este componente soporta el diseño y la generación de formularios electrónicos o físicos y plantillas para su uso dentro del ciclo de negocio de la organización y las partes interesadas
			7.6.2 Modificación de Formularios	Este componente soporta el mantenimiento de los formularios electrónicos o físicos, plantillas y su respectivos elementos y campos de uso.

6.2 Arquitectura de sistemas de información TO-BE

El equipo consultor de Grow Data presentó en el documento "DOC-13 Modelo de operación SICOV CONTRATO 287 DE 2021" las dos alternativas identificadas para el modelo operativo del SICOV. En dicho documento se evaluó que el futuro SICOV fuera centralizado o que fuera federado. El modelo centralizado se refiere a un único SICOV que opere sobre todos los tipos de OAT, mientras que el modelo federado se refiere a un SICOV para cada tipo de OAT.

Los ventajas y desventajas de cada uno de los modelos operativos se analizaron en los otros componentes del proyecto y el resultado final arrojo que el mejor modelo operativo para el SICOV es el modelo centralizado. En las siguientes secciones se presenta para el modelo centralizado los cuatro elementos que describen la arquitectura de sistemas de información que soporten dicho modelo mientras que para el modelo federado se presenta la arquitectura conceptual y la de solución.

En esta sección se presentan los elementos que describen la arquitectura de los sistemas de información objetivo TO-BE para el modelo centralizado de acuerdo con lo establecido en el anexo 1 del contrato 287 de 2021.

- Arquitectura conceptual (Blue Print) de la arquitectura de sistemas de información
- Arquitectura de solución
- Diagrama de interoperabilidad de los sistemas y/o aplicaciones
- Catálogo de servicios de intercambio de información de información

6.2.1 Arquitectura conceptual para el modelo centralizado

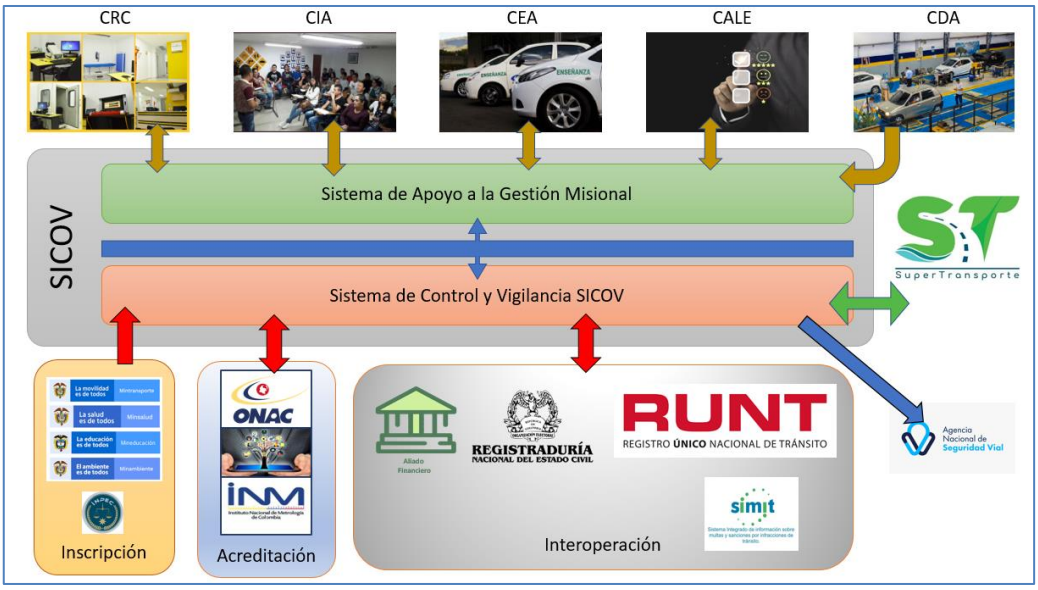
6.2.1.1 Arquitectura de sistemas de información TO BE centralizado

En la Ilustración 49 Diagrama conceptual SICOV, se presenta el modelo elaborado por Grow Data para ilustrar el sistema del SICOV.

En la parte superior del diagrama se encuentran los OAT sujetos a inspección y vigilancia 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.

El SICOV está conformado por dos componentes principales, el sistema de apoyo a la

Ilustración 48 Diagrama conceptual SICOV



Fuente: Elaboración propia Grow Data 2021

gestión misional y el sistema de control y vigilancia SICOV.

De acuerdo con lo establecido en el modelo centralizado, cada uno de los OAT tendrá una interacción directamente con el sistema de apoyo a la gestión misional del SICOV que le proporcionará apoyo directamente en la ejecución de actividades de sus procesos administrativos y 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 o equipos técnicos para evaluación de vehículos automotores serán realizadas a través del sistema de control del SICOV.

De otra parte, las acciones de revisión 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.

6.2.1.2 Arquitectura de referencia para los sistemas de información del SICOV.

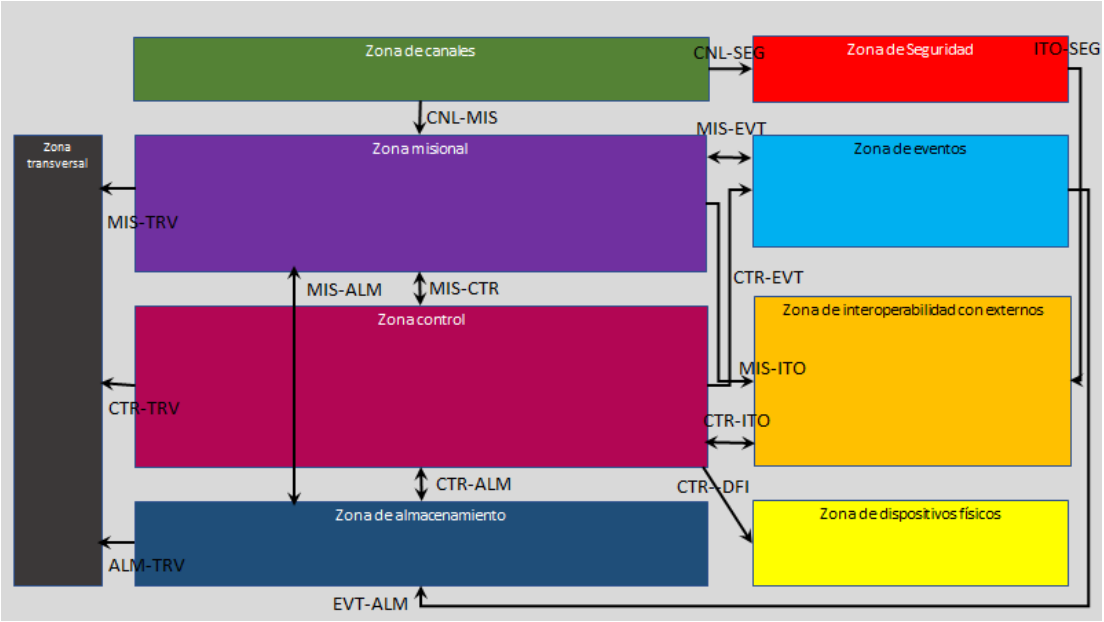
La arquitectura de referencia tiene como propósito orientar los procesos de construcción de arquitecturas de solución que atiendan preocupaciones específicas de interesados y den respuesta a requerimientos concretos.

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 cado 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 **¡Error! No se encuentra el origen de la referencia.**, se presenta de forma gráfica la a rquitectura desarrollada por Grow Data para el SICOV.

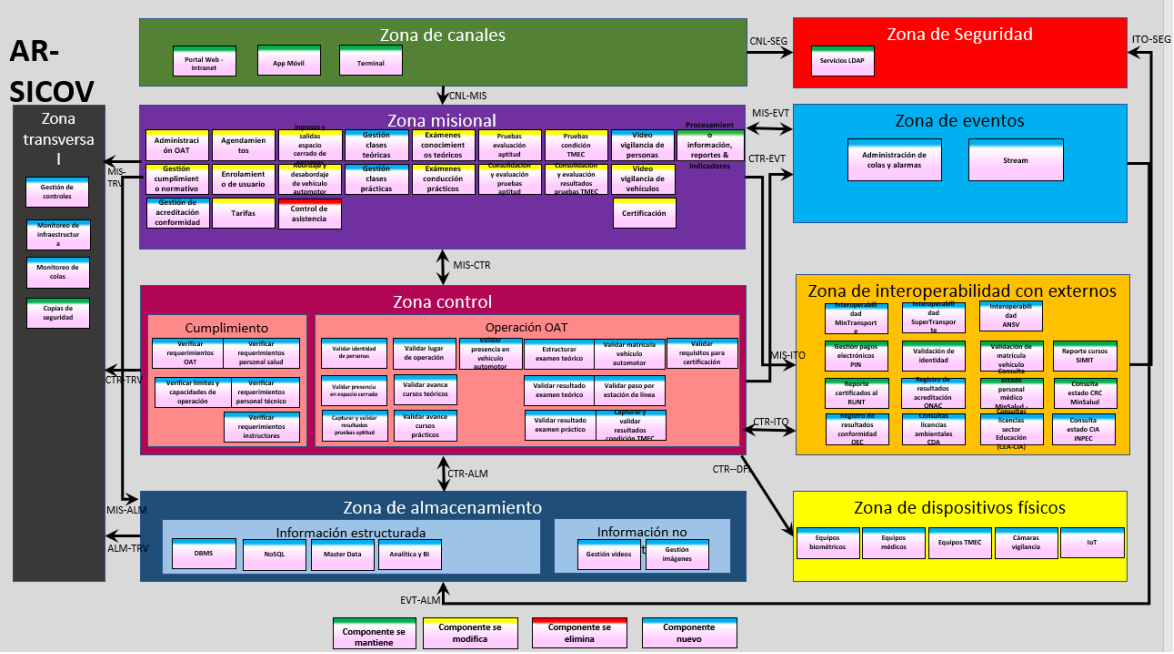
Ilustración 49 Arquitectura de referencia sistemas de información SICOV



Fuente: Elaboración propia Grow Data 2021

En la Ilustración 51 Arquitectura de referencia componentes por zona SICOV se presenta de forma gráfica los principales componentes de cada una de las zonas definidas en la arquitectura de referencia. Más adelante se presentan ilustraciones ampliadas que permiten visualizar con mayor facilidad la estructura de cada zona.

Ilustración 50 Arquitectura de referencia componentes por zona SICOV



Fuente: Elaboración propia Grow Data 2021

6.2.1.2.1 Descripción de zonas

A continuación, se describen cada una de las zonas que conforman la arquitectura de referencia del SICOV centralizado y luego se describen sus componentes

6.2.1.2.1.1 Zona de canales

Los canales se refieren a los medios de acceso a las funcionalidades disponibles en el SICOV para los usuarios. La zona de canales tiene como objetivo presentar agrupados los componentes necesarios que brinden los accesos adecuados al SICOV.

En esta zona se encuentran los portales web, las apps móviles y los sistemas PQRS para la ciudadanía en general. En la zona de canales se ubican los siguientes componentes.

Ilustración 51 Arquitectura de referencia componentes zona canales

Fuente: Elaboración propia Grow Data 2021

- El portal web que permita el acceso de los usuarios del SICOV de los OAT basado en explorador a las funcionalidades provistas para soportar las actividades administrativas y misionales del OAT.
    - Las conexiones que se establezcan por este canal deben garantizar el cumplimiento de los aspectos de seguridad necesarios. Cifrado extremo a extremo
    - Los portales deberán soportar uso de los principales navegadores del mercado tanto actuales como futuros.
- App móvil que permita el acceso a usuarios del OAT que deban realizar sus actividades asociadas a la prestación de los servicios del OAT en espacios no cubiertos por redes locales LAN o Wifi o que deban moverse por espacios exteriores al OAT
    - Las apps móviles deberán contar con todos los aspectos de seguridad establecidos.

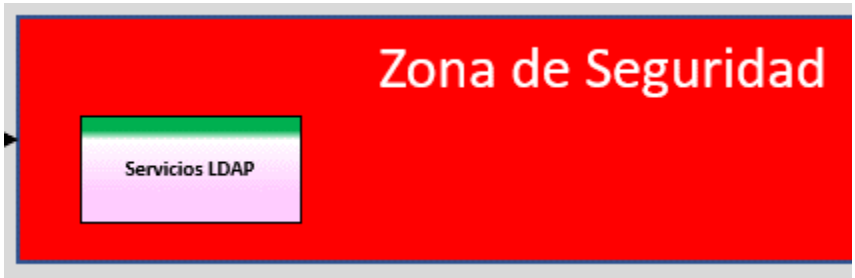
- Terminal para acceder vía consola a levantar o bajar servicios o procesos del SICOV que se ejecuten en backend.
    - Las conexiones deberán ser contar con los aspectos de seguridad establecidos.

6.2.1.2.1.2 Zona de seguridad

La zona de seguridad tiene como objetivo establecer los componentes que garanticen la seguridad en el acceso a los componentes del SICOV. En ella se agrupan los componentes responsables de proveer servicios de autorización o autenticación para controlar y centralizar el acceso a las demás funcionalidades.

La zona de seguridad cuenta fundamentalmente con el servicio de autorización y autenticación y permite validar cualquier acceso al SIVOC desde la zona de canales o desde la zona de interoperabilidad con terceros. El componente principal de esta zona son los servicios LDAP. En esta zona se deben incorporar componentes que puedan surgir a futuro y que brinden mejores condiciones de seguridad para el acceso a los componentes del SICOV.

Ilustración 52 Arquitectura de referencia componentes zona de seguridad



Fuente: Elaboración propia Grow Data 2021

6.2.1.2.1.3 Zona transversal

El objetivo de la zona transversal es garantizar la identificación y la reutilización de elementos comunes para todo el SICOV. En ella se agrupan servicios utilitarios que pueden interactuar con los componentes de otras zonas.

En la zona transversal se ubican inicialmente los siguientes componentes.

Ilustración 53 Arquitectura de referencia componentes zona transversal

Fuente: Elaboración propia Grow Data 2021

- Gestión de controles. Este componente es tal vez el más importante de todo el SICOV. Este componente permite de forma dinámica la activación y desactivación de controles a nivel general para todo el SICOV o de manera particular un control específico para un OAT. También permite administrar las tolerancias de cada control para cada OAT. Este componente puede ayudar a la SuperTransporte como máxima autoridad en materia de control a flexibilizar o endurecer los controles con el paso del tiempo para ajustarse a la evolución natural que se pueda presentar.
- Monitoreo de la infraestructura. En esencia este servicio permite determinar la disponibilidad de los componentes que son críticos para la operación de los OAT y para la ejecución de las acciones de control. Entre otros monitorea los servicios de control. Su función incluye persistir a través de la zona de almacenamiento – DBMS, los registros de auditoría de eventos sobre la infraestructura. Como estándar para los mensajes de registro, se deberá usar el facto syslog (https://es.wikipedia.org/wiki/Syslog).
- Monitoreo de colas. Este componente verifica permanentemente el estado de las colas en la zona de eventos y genera alarmas ante situaciones de no

disponibilidad. Su función incluye persistir a través de la zona de almacenamiento – DBMS, los registros de auditoría de cada evento del sistema y las alarmas generadas desde sus componentes de manera asíncrona, evitando así bloqueos en el sistema. Como estándar para los mensajes de registro, se deberá usar el facto syslog (https://es.wikipedia.org/wiki/Syslog).

- El servicio de copias de seguridad gestiona las copias de respaldo siguiendo un esquema que garantice completamente la recuperación total.

6.2.1.2.1.4 Zona misional

La zona misional tiene como objetivo estructurar los componentes de apoyo administrativo y misional de los OAT. Esta zona 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.

La zona misional también contiene los componentes que soportan procesos de apoyo en la etapa de montaje y durante la operación que determinan el cumplimiento de los aspectos normativos de cumplimiento obligatorio para los OAT.

Ilustración 54 Arquitectura de referencia componentes zona misional

Fuente: Elaboración propia Grow Data 2021

- El componente de administración del OAT soporta las actividades de dar de alta el OAT ante el SICOV y de registrar toda la información necesaria para la operación y para demostrar el cumplimiento de los aspectos normativos.

- El componente de gestión de cumplimiento normativo permite determinar si un OAT cumplió la normativa para entrar en operación y mantiene esa condición durante la operación.
- El componente de gestión de acreditación o conformidad permite determinar de forma permanente el estado de los procesos de acreditación o certificación de los OAT.
- El componente de agendamiento permite ofrecer los espacios de tiempo disponibles de cada OAT para prestar servicios a los usuarios.
- El componente de enrolamiento de usuario permite iniciar la prestación del servicio solicitado por el usuario al OAT verificando la disponibilidad de PIN ajustado a los aspectos tarifarios establecidos en las normas vigentes.
- El componente de tarifas permite incorporar al SICOV las tarifas establecidas por cada OAT
- El componente de ingresos y salidas de personas en espacios cerrados permite determinar las personas (empleados del OAT o usuarios) que ingresan a un espacio físico en un OAT destinado a la prestación del servicio.
- El componente de abordaje y desabordaje de personas de vehículos automotores permite determinar que el usuario y el instructor o el evaluador abordaron un vehículo automotor para la prestación del servicio solicitado.
- El componente de gestión de clases teóricas permite registrar los temas cubiertos en cada clase impartida hasta completar los contenidos mínimos exigidos por norma.
- El componente de gestión de clases prácticas permite registrar los aspectos cubiertos en cada clase impartida hasta completar todas las habilidades requeridas.
- El componente de exámenes de conocimientos teóricos permite evaluar que el usuario realmente aprendió y comprendió los contenidos mínimos aprobatorios para aspirar a la licencia de conducción.
- El componente de exámenes de conducción prácticos permite evaluar que el usuario realmente adquirió las habilidades en conducción mínimas para aspirar a la licencia de conducción.
- El componente de pruebas de evaluación de aptitud permite evaluar que el usuario cumple y en qué condiciones los requisitos de aptitudes mínimos aprobatorios para aspirar a la licencia de conducción

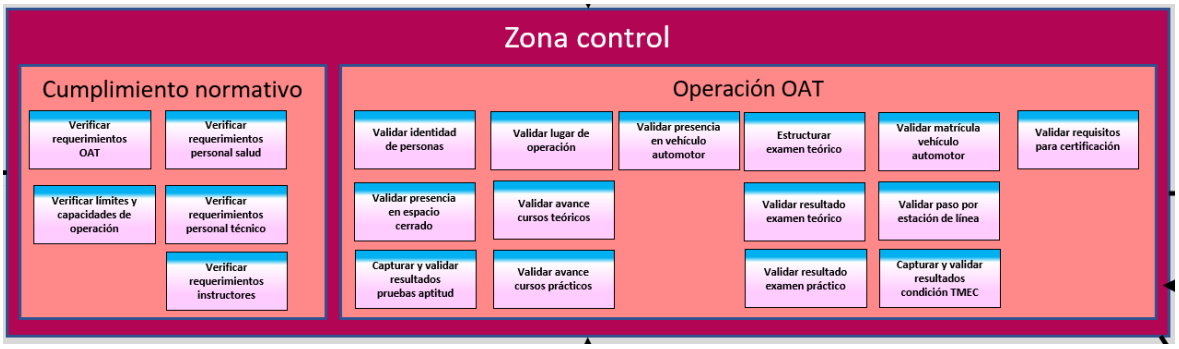
- El componente de consolidación y evaluación pruebas aptitud permite determinar de forma integral que un usuario es o no apto para conducir y en que condiciones o con que restricciones.
- El componente de pruebas condición TMEC permite determinar si un vehículo automotor cumple con un determinado aspecto técnico sujeto a verificación en el CDA.
- El componente de consolidación y evaluación resultados pruebas TMEC permite determinar si un vehículo automotor está en condiciones para transitar por las vías colombianas.
- El componente de video vigilancia de personas permite verificar que una persona estuvo presente en el OAT durante el tiempo que duraron las actividades propias a la prestación del servicio en el OAT.
- El componente de video vigilancia de vehículos permite verificar que un vehículo automotor recorrió la pista de revisión completamente y fue sometido a cada una de las pruebas obligatorias.
- El componente de certificación permite con base en los resultados de las actividades propias de cada OAT establecer si el usuario o el vehículo objeto de la evaluación puede ser certificado o no de acuerdo con el servicio solicitado.
- El componente de procesamiento información, reportes & indicadores permite obtener los resultados detallados, consolidados y convertidos de la operación del OAT con propósitos de análisis y mejoramiento continuo.

6.2.1.2.1.5 Zona control

El objetivo de la zona de control es ofrecer los medios necesarios para la implementación de cualquier tipo de control del SICOV. 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.

La zona de control juega un papel fundamental en el SICOV puesto que contiene los componentes y servicios que implementan las acciones de inspección y control de los aspectos normativos y de operación. Estos servicios se dividen en dos grupos.

Ilustración 55 Arquitectura de referencia componentes zona de control



Fuente: Elaboración propia Grow Data 2021

6.2.1.2.1.5.1 Cumplimiento normativo

- Verificar requerimientos OAT permite de forma automática comprobar que el OAT cumple los requerimientos mediante la revisión de los registros iniciales, así como sus actualizaciones.
- Verificar límites y capacidades de operación permite identificar si un OAT está operando dentro de los límites autorizados o no.
- Verificar requerimientos relativos al personal salud permite identificar si los servidores del CRC están habilitados para prestar los servicios según el registro oficial en el RETHUS.
- Verificar requerimientos relativos al personal técnico permite identificar si el personal técnico de un CDA cumple el perfil exigido por norma
- Verificar requerimientos relativos a los instructores permite identificar si los instructores de un CEA o un CIA cumplen con los requisitos exigidos por norma.

6.2.1.2.1.5.2 Operación OAT

- Validar identidad de personas es el servicio que permite determinar que un usuario del OAT es realmente quien dice ser de acuerdo con el documento de identidad presentado.

- Validar presencia en espacio cerrado permite verificar que el usuario se presentó en el OAT para acceder personalmente al servicio ofrecido.
- Capturar y validar resultados pruebas aptitud permite solicitar, recibir, almacenar y asegurar las mediciones correspondientes a un aspirante en evaluación desde un dispositivo médico, que indica la situación del aspirante.
- Validar lugar de operación permite identificar desde que punto geográfico se está prestando el servicio a un usuario por parte de un OAT y verificarlo contra el sitio autorizado para operación
- Validar avance cursos teóricos permite determinar que tanto ha avanzado y que tanto le falta a un aprendiz para completar el total de temas y contenidos mínimos exigidos.
- Validar avance cursos prácticos permite determinar que tanto ha avanzado y que tanto le falta a un aprendiz para completar el total de habilidades de conducción mínimas exigidas.
- Validar presencia en vehículo automotor permite determinar si un vehículo automotor realmente transitó por toda la pista de revisión y fue sometido a las pruebas establecidas.
- Estructurar examen teórico permite garantizar que la prueba de examinación cubre los temas establecidos en el programa aprobado al OAT.
- Validar resultado examen teórico permite determinar si el usuario obtuvo el puntaje mínimo aprobatorio establecido en la norma.
- Validar resultado examen práctico permite determinar si el usuario adquirió las habilidades en conducción mínimas aprobatorias establecida por norma.
- Validar matrícula vehículo automotor permite verificar que el vehículo automotor inspeccionado corresponde realmente al número de matrícula (placa) con el que se identificó para recibir el servicio.
- Validar paso por estación de línea permite garantizar que el vehículo automotor se sometió a todas las pruebas establecidas
- Capturar y validar resultados condición TMEC permite establecer con base en los resultados de las pruebas de forma inequívoca que el vehículo puede transitar por las vías colombianas.
- Validar requisitos para certificación permite establecer si los resultados obtenidos y el estado del OAT permiten expedir el certificado al usuario.

6.2.1.2.1.6 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 optimizar los procesos.

La zona misional de interoperabilidad del SICOV contiene los siguientes componentes. Las características de cada servicio se encuentran descritas en los numerales 6.2.2.2 Diagrama de interoperabilidad de los sistemas o aplicaciones y 6.2.2.3 Catálogo de servicios de intercambio de información TO BE.

Ilustración 56 Arquitectura de referencia componentes zona interoperabilidad con externos

Fuente: Elaboración propia Grow Data 2021

6.2.1.2.1.7 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.

Ilustración 57 Arquitectura de referencia componentes zona de eventos

Fuente: Elaboración propia Grow Data 2021

- 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.

6.2.1.2.1.8 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 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.

La zona de dispositivos permite el envío de datos desde dispositivos físicos hacia el SICOV de forma controlada y segura.

Ilustración 58 Arquitectura de referencia componentes zona de dispositivos físicos

Fuente: Elaboración propia Grow Data 2021

- Equipos biométricos que permiten obtener aspectos biométricos del usuario para validar su identidad.
- Equipos médicos que permiten realizar mediciones o evaluaciones relativas a la condición específica del aspirante.
- Equipos medición condiciones TMEC que permiten realizar mediciones o evaluaciones relativas a la condición específica del vehículo automotor en evaluación,

- Cámaras de vigilancia que permiten tomar y registrar evidencias multimedia de la presencia y comportamiento de personas o vehículos en determinadas zonas del OAT.

6.2.1.2.1.9 Zona de almacenamiento

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

La zona de almacenamiento contiene servicios que permiten la persistencia de la información.

Ilustración 59 Arquitectura de referencia componentes zona de almacenamiento

Fuente: Elaboración propia Grow Data 2021

- Información estructurada.
  - El servicio DBMS permite la persistencia de los datos transaccionales requeridos por componentes misionales, de control y de eventos. De igual forma, este servicio administrará los registros de auditoria provenientes de la zona transversal para el monitoreo de los eventos, alarmas y la infraestructura de aplicaciones.
  - El servicio NoSQL permite gestión flexible para requerimientos especiales.
  - El servicio Master Data permite el flujo de información hacia un repositorio global.

- El componente de analítica y BI ofrece servicios para implementación de métodos avanzados en identificación de relaciones e implementación de alarmas.

- Información no estructurada ofrece servicios para gestión de información multimedia como videos e imágenes.

6.2.1.2.2 Caracterización de conectores

A continuación, se define mediante la caracterización de conectores, la forma en que las zonas se van a comunicar entre sí, estableciendo la gobernanza a nivel de interoperabilidad interna que debe cumplir cualquier aplicación o producto tecnológico que quiera integrarse a la solución.

6.2.1.2.2.1 Conector CNL-SEC

Este conector unidireccional con origen en la zona de canales y destino la zona de seguridad establece que todos los accesos que se otorguen por medio de los canales deberán ser autenticados y autorizados a nivel de solución por los servicios de seguridad invocados desde la zona de canales.

6.2.1.2.2.2 Conector CNL-MIS

Este conector unidireccional con origen la zona de control y destino la zona misional, para dar respuesta a una solicitud recibida por un canal, debe consumir servicios expuestos en la solución misional que soporten las actividades del OAT. Un ejemplo de servicio misional es la realización de un examen de audiometría a un aspirante en un CRC.

6.2.1.2.2.3 Conector MIS-CTR

Este conector bidireccional entre la zona misional y la zona de control debe permitir que desde la zona de control se implementen acciones bien sea por solicitud de un componente misional consumiendo un servicio expuesto en la capa de control o por que se activa desde la zona de control como resultado del monitoreo de las actividades misionales.

6.2.1.2.2.4 Conector MIS-ALM

Este conector bidireccional entre la zona misional y la zona de almacenamiento debe permitir el acceso a los servicios centralizados de almacenamiento de datos misionales como pueden ser bases de datos en datacenter local, almacenamiento en la nube, almacenamiento de información no estructurada.

6.2.1.2.2.5 Conector CTR-ALM

Este conector bidireccional entre la zona de control y la zona de almacenamiento debe permitir el acceso a los servicios centralizados de almacenamiento estructurado y no estructurado para la persistencia de los controles efectuados en los repositorios adecuados.

6.2.1.2.2.6 Conector MIS-TRV

Este conector unidireccional con origen en la zona misional y destino la zona transversal, debe permitir que desde la zona transversal se implementen acciones de monitoreo a los componentes misionales.

6.2.1.2.2.7 Conector CTR-TRV

Este conector unidireccional con origen en la zona de control y destino la zona transversal, debe permitir que desde la zona transversal se implementen acciones de monitoreo a los componentes de control.

6.2.1.2.2.8 Conector ALM-TRV

Este conector unidireccional con origen en la zona de almacenamiento y destino la zona transversal, debe permitir que desde la zona transversal se implementen acciones comunes a todos los servicios, consumiendo un servicio expuesto en la capa transversal. Un ejemplo de servicio transversal para la zona de almacenamiento puede ser el servicio de solicitar copia de seguridad antes de un proceso masivo de actualización de información.

6.2.1.2.2.9 Conector MIS-ITO

Este conector bidireccional entre la zona misional y la zona de interoperabilidad debe permitir que desde la zona misional se consuman servicios que automatizan procesos misionales no sujetos a control.

6.2.1.2.2.10 Conector CTR-ITO

Este conector bidireccional entre la zona de control y la zona de interoperabilidad debe permitir que desde la zona de control se implementen acciones de control consumiendo un servicio expuesto por un tercero en la capa de interoperabilidad para implementar algún control establecido como por ejemplo una validación biométrica. También debe ser posible que un tercero implemente acciones al consumir un servicio expuesto en la zona de control.

6.2.1.2.2.11 Conector ITO-SEC

Este conector unidireccional con origen en la zona de interoperabilidad y destino la zona de seguridad establece que todos los accesos que se otorguen por medio de servicios de interoperabilidad deberán ser autenticados y autorizados a nivel de solución por los servicios de seguridad invocados desde la zona de interoperabilidad.

6.2.1.2.2.12 Conector CTR-DFI

Este conector unidireccional con origen en la zona de control y destino la zona de dispositivos físicos debe permitir que desde la zona de control se reciban datos enviados desde el dispositivo. Un ejemplo puede ser los drivers para recibir información de un huellero.

6.2.1.2.2.13 Conector CTR-EVT

Este conector unidireccional con origen en la zona de control y destino la zona de eventos debe permitir que los componentes de la zona de control hagan uso de los servicios de notificaciones o alarmas para alertar sobre la ocurrencia de determinados eventos.

6.2.1.2.2.14 Conector MIS-EVT

Este conector bidireccional entre la zona misional y la zona de eventos debe permitir que, desde la zona misional, los componentes de la zona de control hagan uso de los servicios de notificaciones o alarmas para alertar sobre la ocurrencia de determinados eventos. Igualmente se debe permitir que desde la zona de eventos se consuman servicios expuestos por componentes de la zona misional, alertando de la ocurrencia de eventos.

6.2.1.2.2.15 Conector EVT-ALM

Este conector unidireccional con origen en la zona de evento y destino la zona de almacenamiento debe permitir que los componentes de la zona de almacenamiento habiliten la persistencia de las colas.

6.2.2 Arquitectura de solución objetivo para el modelo centralizado

Los componentes de la solución, necesitarán proporcionar datos a otros componentes a medida que suceden los eventos dentro de la gestión del SICOV. Estos datos se conocen como mensajería, que al ser asincrónica es una forma eficaz de desacoplar a los remitentes de los consumidores (componentes SICOV) y evitar bloquear al remitente para que espere una respuesta. La aplicación de este concepto, se puede generalizar hacia la comunicación entre los subsistemas (SGM y el Sistema de control y vigilancia), lo mismo, que hacia componentes externos o de función transversal.

6.2.2.1 Arquitectura de Sistemas de Información TO-BE centralizado

En la Ilustración 61 Modelo operativo recomendado para el SICOV, se presenta conceptualmente la solución para implementar.

Ilustración 60 Modelo operativo recomendado para el SICOV

Fuente: Elaboración propia Grow Data 2021

Tomando como base la arquitectura de referencia presentada previamente, los aspectos claves para diseñar la arquitectura de solución son aquellos relativos a la implementación de los controles para el SICOV.

6.2.2.1.1 Estructuración de los controles a implementar en el SICOV.

El principal factor que se tuvo en cuenta para el diseño de la arquitectura de solución del SICOV fue la necesidad de permitir el manejo dinámico de los controles de tal forma que se puedan crear nuevos controles, modificar los existentes e incluso eliminar controles.

También se consideró la necesidad de activar o desactivar la aplicación de los controles de tal forma que se puedan manejar situaciones coyunturales en periodos de tiempo limitados como puede ser la no disponibilidad de algún servicio crítico para la operación en el que se base la aplicación del control.

De otra parte, se consideró la necesidad de determinar umbrales de tolerancia en la implementación de los controles de tal forma que se puedan racionalizar los costos de operación, por ejemplo, flexibilizando los umbrales con base en la administración del riesgo asociado.

En la siguiente Ilustración 62 Estructura de control para el SICOV se presenta gráficamente la estructura general de un control que debe ser tenida en cuenta para su aplicación e implementación en el SICOV.

Ilustración 61 Estructura de control para el SICOV

Nombre del control y dominio de aplicación	
Escenario Descripción detallada de los principales aspectos a considerar previos al evento o situación que establezca la necesidad de aplicar el control sobre el punto de control en el proceso vigilado. • Aspecto descriptivo 1 • ... • Aspecto descriptivo n • Regla negocio 1 • Regla de negocio n	

Eventos
• Evento 1 de negocio
• ...
• Evento n de negocio
 	
• Alarma 1
• ...
• Alarma n
	Entidades
	• Control
	• Hipótesis
	• Estado
	• Parámetros
	  • Estándares
	  • Normativas
	  • Umbrales de riesgo
	• Resultado (Evaluación de la hipótesis)

Interoperabilidad – Integración • Contrato 1 interoperabilidad con tercero • ... • Contrato n interoperabilidad con tercero	Umbrales de tolerancia • Niveles de aceptación del control

Fuente: Elaboración propia Grow Data 2021

El escenario describe detalladamente los aspectos a considerar previos al evento que establece la necesidad de aplicar el control en la actividad del proceso vigilado. En esta sección se enumeran los aspectos relevantes a la acción de control. En la sección de eventos, se enumeran los eventos que permiten la interacción entre los componentes misionales y los de componentes de control de la arquitectura de solución y las alarmas que se podrían activar en respuesta a los eventos.

En la sección de entidades se presentan las entidades de negocios implicadas en la aplicación del control e incluyen el control en sí, la hipótesis a verificar, el estado del control y el resultado de su evaluación. Para permitir la implementación flexible, en las entidades se incluyen los parámetros que afectan directamente la evaluación de la hipótesis de tal forma que puedan ser dinámicos.

En la sección de interoperabilidad se enumeran los servicios de interoperabilidad y sus respectivos contratos que intervienen en la aplicación del control. Finalmente, en la sección de umbrales de tolerancia se describen los niveles de aceptación de los resultados de evaluación del control para facilitar su aplicación e implementación.

6.2.2.1.2 Controles por incluir en la arquitectura de solución.

En el documento denominado "DOC-Controles a implementar SICOV Contrato 287 de 2021" se presenta la lista de los controles específicos que se identificaron para implementar la solución del SICOV.

Adicionalmente en el repositorio ARCHI - Archimate Modelling del proyecto, se encuentran modelados los controles identificados, agrupados por características similares que servirán de base para realizar una implementación específica.

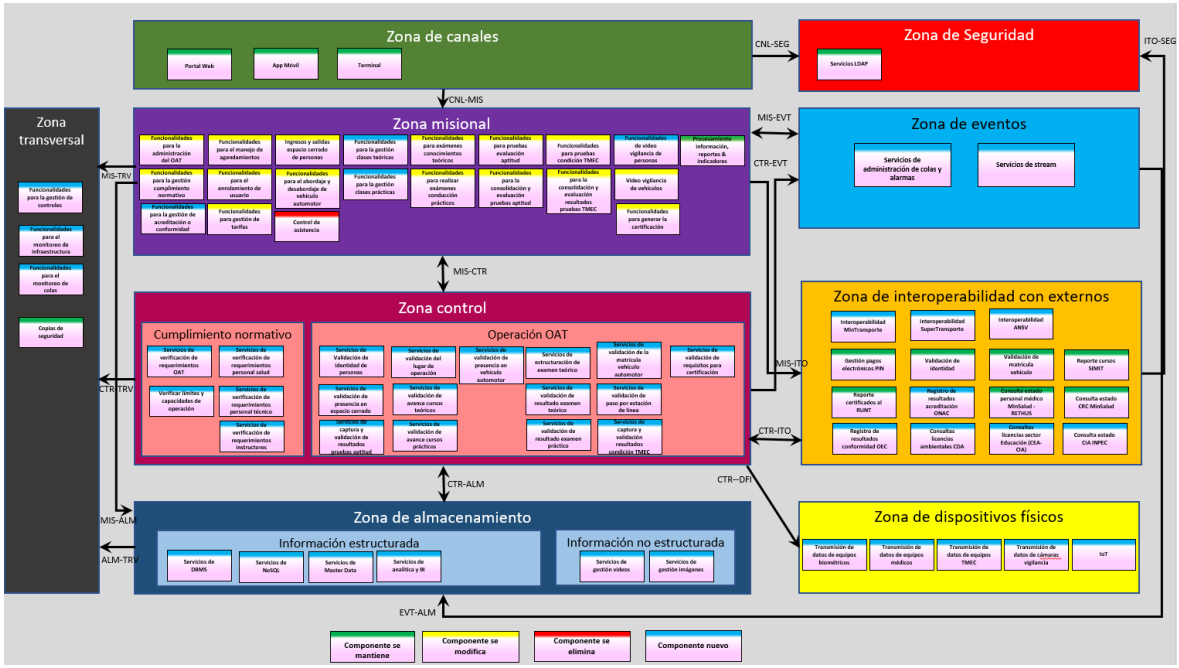
6.2.2.1.3 Diagrama arquitectura de solución SICOV.

La arquitectura de solución para el SICOV se genera a partir de la arquitectura de referencia definida previamente. En esencia cada componente se desagrega de acuerdo con su naturaleza. Los componentes de la zona misional y los de la zona transversal se desagregan en funcionalidades específicas que permiten su implementación, en algunos casos el componente se implementa con una sola funcionalidad.

Para el caso de los componentes de las zonas de control y de eventos se desagregan en servicios que deben ser accedidos por medio de interfaces desde los componentes de otras zonas que los invocan.

En la Ilustración 63 Arquitectura de solución SICOV se presenta de forma gráfica los

Ilustración 62 Arquitectura de solución SICOV



Fuente: Elaboración propia Grow Data 2021

elementos que hacen parte de la solución del SICOV centralizado.

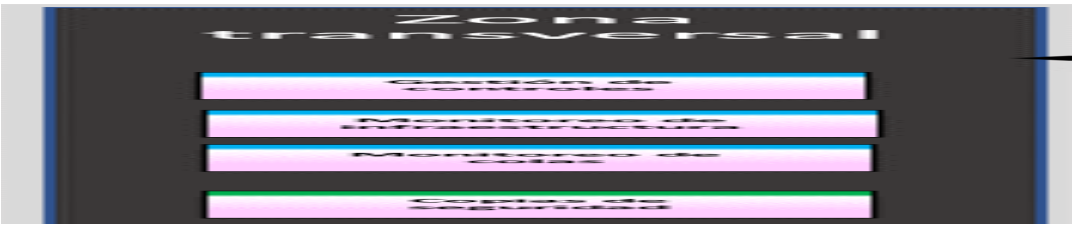
En las siguientes secciones, con base en la definición de las zonas y componentes de la arquitectura de referencia, se presentan los diferentes elementos que materializan la solución.

En términos generales, los elementos de solución para cada zona de referencia se implementan a nivel de solución con base en funcionalidades especificas agrupadas en módulos, o con servicios expuestos que pueden interactuar con las funcionalidades.

6.2.2.1.3.1 Zona de canales

Para el caso de la zona de canales en la arquitectura de solución, los elementos

Ilustración 63 Arquitectura de solución componentes zona canales



Fuente: Elaboración propia Grow Data 2021

coinciden con los componentes de referencia. Por lo tanto, a nivel de solución se deberán implementar canales específicos que permitan a los usuarios del SICOV acceder a las funcionalidades de la zona misional, mediante un portal web o mediante las apps móviles en los casos específicos que se requiera.

El acceso a través de terminales está limitado a los administradores del SICOV que requieren acceder a servicios expuestos a través de ese medio.

6.2.2.1.3.2 Zona seguridad

A nivel de solución, se deberán implementar servicios específicos LDAP que

Ilustración 64 Arquitectura de solución componentes zona de seguridad

Fuente: Elaboración propia Grow Data 2021

proporcionen y garanticen la seguridad en todos los accesos a las funcionalidades y los servicios del SICOV.

6.2.2.1.3.3 Zona transversal

Las soluciones para la zona transversal deberán incluir los siguientes elementos.

Ilustración 65 Arquitectura de solución componentes zona transversal

Fuente: Elaboración propia Grow Data 2021

6.2.2.1.3.3.1 Gestión de controles

- Funcionalidades para la creación/modificación de controles dentro del SICOV.
- Funcionalidades para la activación/desactivación de controles del SICOV.
- Funcionalidades para la actualización de tolerancias de los controles del SICOV.

6.2.2.1.3.3.2 Monitoreo de la infraestructura

- Funcionalidades para incorporar/ajustar/eliminar elementos al proceso de monitoreo de infraestructura de control del SICOV.

6.2.2.1.3.3.3 Monitoreo de colas

- Funcionalidades para incorporar/ajustar/eliminar elementos al proceso de monitoreo de colas de mensajería del SICOV.

6.2.2.1.3.4 Zona misional

La zona misional contiene las funcionalidades que soportan las actividades operativas de los procesos misionales de los OAT, así como los procesos de apoyo en la etapa de montaje y durante la operación que determinan el cumplimiento de los aspectos normativos de cumplimiento obligatorio para los OAT.

Ilustración 66 Arquitectura de solución componentes zona misional

Fuente: Elaboración propia Grow Data 2021

6.2.2.1.3.4.1 Administración

- Funcionalidades para registrar y actualizar la información relevante del OAT.
- Funcionalidades para dar de alta, actualizar o dar de baja usuarios del SICOV propios del OAT.
- Funcionalidades para registrar/actualizar capacidades de operación del OAT

- Funcionalidades para registrar/actualizar equipos de apoyo misional propios del OAT

6.2.2.1.3.4.2 Cumplimiento normativo

- Funcionalidades para registrar registrar/actualizar información de cumplimiento normativo.

6.2.2.1.3.4.3 Gestión de acreditación o conformidad

- Funcionalidades para registrar los resultados de las visitas para acreditación por parte del ONAC a un OAT
- Funcionalidades para gestión de las auditorías a OAT acreditados por la ONAC
- Funcionalidades para registrar los resultados de las visitas para certificación por parte del OEC a un OAT
- Funcionalidades para gestión de las auditorías a OEC acreditados por la ONAC
- Funcionalidades para registro/actualización de resultados de calibración de equipos de apoyo misional del OAT.

6.2.2.1.3.4.4 Gestión de agendamientos

- Funcionalidades para programar espacios de tiempo disponible para la prestación de servicios por el OAT.
- Funcionalidades para reservar/actualizar citas por parte de los usuarios de los servicios del OAT para acceder al servicio.

6.2.2.1.3.4.5 Gestión de enrolamiento

- Funcionalidades para registrar un usuario para la prestación del servicio del OAT.
- Funcionalidades para validar biométricamente ante RNEC la identidad del usuario o funcionario del OAT.
- Funcionalidades para validar por medios alternos la identidad del usuario o funcionario del OAT.

6.2.2.1.3.4.6 Gestión de tarifas

- Funcionalidades para actualizar las tarifas al público registradas por los OAT.

6.2.2.1.3.4.7 Gestión de ingresos y salidas de espacios cerrados

- Funcionalidades para determinar las personas (empleados del OAT o usuarios) que ingresan a un espacio físico en un OAT destinado a la prestación del servicio mediante método biométrico dactilar o fotografía.
- Funcionalidades para determinar las personas (empleados del OAT o usuarios) que salen de un espacio físico en un OAT destinado a la prestación del servicio mediante método biométrico dactilar o fotografía.

6.2.2.1.3.4.8 Gestión de abordaje y desabordaje de vehículos automotores

- Funcionalidades para verificar el abordaje de un vehículo por medios biométricos apoyados en app móvil.
- Funcionalidades para verificar la permanencia a bordo de un vehículo por medios biométricos apoyados en app móvil.
- Funcionalidades para verificar el desabordaje de un vehículo por medios biométricos apoyados en app móvil.

6.2.2.1.3.4.9 Gestión de proceso de enseñanza

- Funcionalidades para el seguimiento del avance de clases teóricas permite registrar los temas cubiertos en cada clase impartida hasta completar los contenidos mínimos exigidos por norma.
- Funcionalidades para el seguimiento del avance de clases prácticas permite registrar los aspectos cubiertos en cada clase impartida hasta completar todas las habilidades requeridas.
- Funcionalidades para realización de exámenes de conocimientos teóricos permite evaluar de forma efectiva que el usuario realmente aprendió y comprendió los contenidos mínimos aprobatorios para aspirar a la licencia de conducción.
- Funcionalidades para realización de exámenes de conducción prácticos permite evaluar de forma efectiva que el usuario realmente adquirió las habilidades en conducción mínimas para aspirar a la licencia de conducción.

6.2.2.1.3.4.10 Gestión de proceso de enseñanza

- Funcionalidades de soporte a la realización de pruebas de evaluación de aptitud que permitan evaluar que el usuario cumple y en qué condiciones los requisitos de aptitudes mínimos aprobatorios para aspirar a la licencia de conducción
- Funcionalidades que soporten le integración con equipos médicos para determinar la condición de los vehículos automotores de forma controlada y segura.
- Funcionalidades de soporte a la consolidación y evaluación pruebas aptitud permite determinar de forma integral que un usuario es o no apto para conducir y en qué condiciones o con que restricciones.

6.2.2.1.3.4.11 Gestión de pruebas RTMEC

- Funcionalidades que soporten la realización de pruebas de condición TMEC permite determinar si un vehículo automotor cumple con un determinado aspecto técnico sujeto a verificación en el CDA.

- Funcionalidades que soporten le integración con equipos técnicos para determinar la condición de los vehículos automotores de forma controlada y segura.
- Funcionalidades para la consolidación y evaluación resultados pruebas TMEC permite determinar si un vehículo automotor está en condiciones para transitar por las vías colombianas.

6.2.2.1.3.4.12 Gestión de pruebas RTMEC

- Funcionalidades de video vigilancia de personas permite verificar que una persona estuvo presente en el OAT durante el tiempo que duraron las actividades propias a la prestación del servicio en el OAT.
- Funcionalidades de video vigilancia de vehículos permite verificar que un vehículo automotor recorrió la pista de revisión completamente y fue sometido a cada una de las pruebas obligatorias.
- Funcionalidades que permitan el procesamiento y extracción y estructuración de elementos individuales que faciliten la demostración de la permanencia en zona de servicio de los OAT.

6.2.2.1.3.4.13 Certificaciones

- Funcionalidades que permitan con base en los resultados de las actividades propias de cada OAT, establecer si el usuario o el vehículo objeto de la evaluación puede ser certificado o no de acuerdo con el servicio solicitado.
- Funcionalidades que permitan el registro en el RUNT de los resultados de cada proceso del OAT.

6.2.2.1.3.4.14 Certificaciones

- Funcionalidades de mesa de ayuda permite que los usuarios del SIVOC dispongan de apoyo para solucionar los problemas que se presenten durante la operación en el SIVOC. Abrir, modificar, atender y cerrar tiquetes de solicitud de apoyo.

6.2.2.1.3.4.15 Procesamiento de información

- Funcionalidades de procesamiento información, reportes & indicadores permite obtener los resultados detallados, consolidados y convertidos de la operación del OAT con propósitos de análisis y mejoramiento continuo.

6.2.2.1.3.5 Zona Control

La estructura y definición detallada de cada control se encuentra en el documento "DOC-Controles a implementar SICOV Contrato 287 de 2021". En este documento se encuentran los aspectos requeridos para la implementación de cada control. En el se describe el control, sus eventos asociados, las reglas de negocio, las interoperabilidades que requieren, la integración con dispositivos de apoyo y los umbrales que le aplican.

La zona de control en esencia contiene los servicios que implementan cada uno de los controles del SICOV en documento mencionado.

Es importante tener en cuenta para las implementaciones de soluciones, que dada la naturaleza del SICOV, que los controles van a variar en el tiempo, van a aparecer nuevos, algunos dejarán de ser vigentes y otros se deberán ajustar. Por lo tanto, es absolutamente importante que las soluciones brinden flexibilidad que permitan la adaptación del SICOV en el tiempo en todo lo relativo a gestión de controles.

Ilustración 67 Arquitectura de solución componentes zona de control

Fuente: Elaboración propia Grow Data 2021

6.2.2.1.3.6 Zona de interoperabilidad

Para la implementación de soluciones, se debe tener en cuenta que cada interoperabilidad tendrá su propia estructuración y definición y dependerá en esencia de las implementaciones acordadas y consignadas en los contratos o sus equivalentes que rijan la interacción entre los sistemas interoperables. Más adelante se describen las interoperaciones iniciales que se requieren para el SICOV. Sin embargo, estas evolucionarán en el tiempo de acuerdo con la evolución de los controles del SICOV.

En el catálogo de servicios de intercambio de información que se presenta más adelante, se encuentra información complementaria para establecer los servicios de interoperabilidad a nivel de solución.

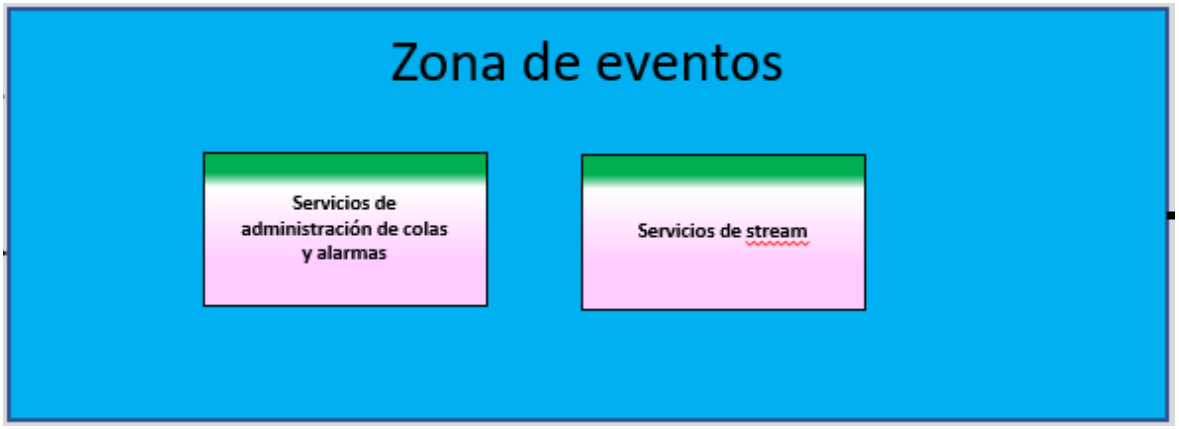
Ilustración 68 Arquitectura de solución componentes zona interoperabilidad con externos

Fuente: Elaboración propia Grow Data 2021

6.2.2.1.3.7 Zona de eventos

La zona de eventos a nivel de solución contiene los servicios específicos que permitirán

Ilustración 69 Arquitectura de solución componentes zona de eventos



Fuente: Elaboración propia Grow Data 2021

implementar de forma adecuada y eficaz mecanismos de interacción entre la zona misional y la zona de control.

6.2.2.1.3.7.1 Administración de colas

- Funcionalidades de administración de colas y alarmas que permite implementar eventos entre publicador y suscriptor para la interoperación entre la zona misional y la zona de controles.

6.2.2.1.3.7.2 Servicio de stream

- Funcionalidades de stream permite procesar alarmas en tiempo real generadas en el procesamiento de las colas

6.2.2.1.3.8 Zona de dispositivos físicos

La zona de dispositivos permite el envío de datos desde dispositivos físicos hacia el SICOV de forma controlada y segura.

6.2.2.1.3.8.1 Integración con equipos biométricos

- La integración con equipos biométricos se dará a través de drivers que el fabricante aporte y que cumplan con los requerimientos funcionales del SICOV.

Ilustración 70 Arquitectura de solución componentes zona de dispositivos físicos

Fuente: Elaboración propia Grow Data 2021

6.2.2.1.3.8.2 Integración con equipos médicos

- La integración con equipos médicos se dará a través de drivers que el fabricante aporte y que cumplan con los requerimientos funcionales y de seguridad del SICOV de tal forma que impidan la alteración de los datos medidos y transmitidos.

6.2.2.1.3.8.3 Integración con equipos RTMEC

- La integración con equipos RTMEC se dará a través de drivers que el fabricante aporte y que cumplan con los requerimientos funcionales y de seguridad del SICOV de tal forma que impidan la alteración de los datos medidos y transmitidos.

6.2.2.1.3.9 Zona de almacenamiento

La zona de almacenamiento contiene servicios que permiten la persistencia de la información.

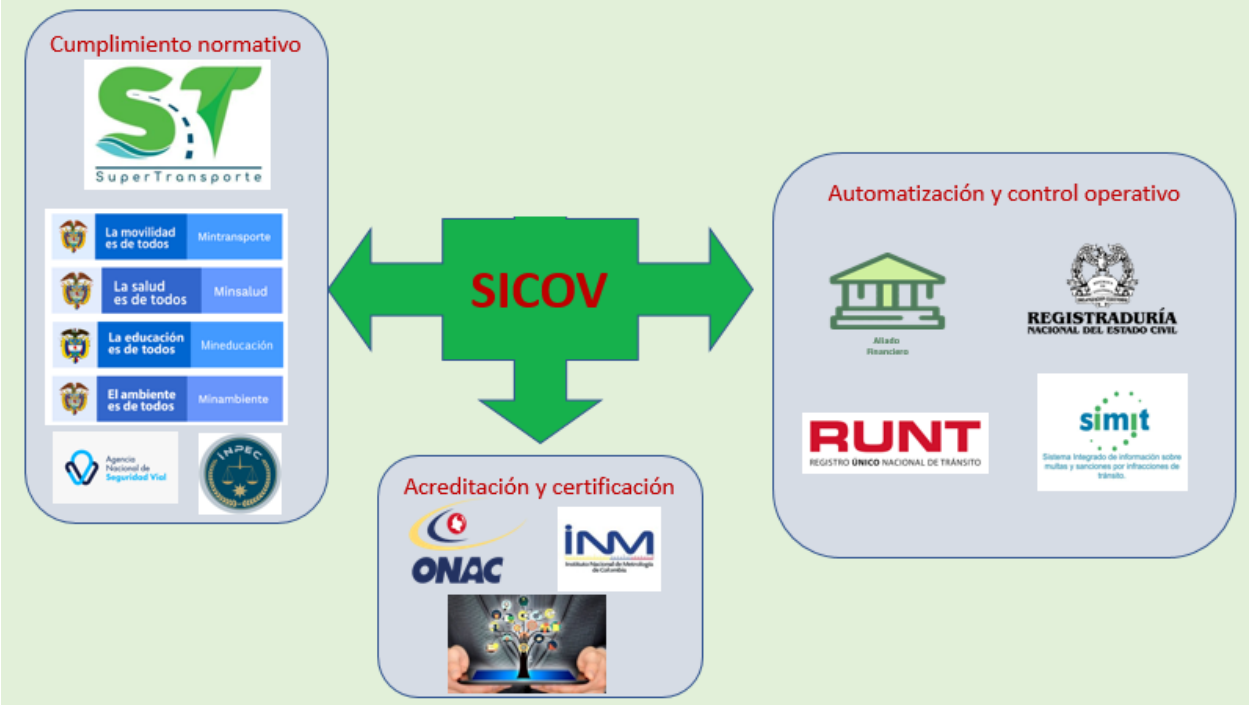
Ilustración 71 Arquitectura de solución componentes zona de almacenamiento

Fuente: Elaboración propia Grow Data 2021

6.2.2.2 Diagrama de interoperabilidad de los sistemas o aplicaciones

La interoperabilidad representa un factor crítico para el SICOV debido a la alta dependencia con los actores del ecosistema. El la Ilustración 73 Diagrama de interoperabilidad SICOV TO BE se presenta de forma gráfica las interoperabilidades que le permitan al SICOV automatizar tanto las actividades operativas de los OAT, como las actividades de control sobre las actividades objeto de vigilancia. La interoperabilidad también le permite al SICOV automatizar las acciones de verificación de cumplimiento normativo por parte de los OAT.

Ilustración 72 Diagrama de interoperabilidad SICOV TO BE



Fuente: Elaboración propia Grow Data 2021

6.2.2.2.1 Interoperabilidad para el cumplimiento normativo

La interoperabilidad sectorial involucra a los interesados del SICOV pertenecientes al sector transporte cuya cabeza en el Ministerio de Transporte. También está en este grupo la SuperTransporte quien es el principal actor debido a su responsabilidad misional de vigilancia y control sobre los OAT. Pertenece a este grupo de interoperabilidad la Agencia Nacional de Seguridad Vial, que es quien da línea en materia de seguridad vial. Le ANSV es quien debe definir y actualizar los aspectos que debe ser enseñados a los conductores de vehículos automotores y a los infractores de las normas de tránsito. Es también función de la ANSV establecer los aspectos que se deben evaluar a los conductores por medio de exámenes teóricos y construir y actualizar el banco de preguntas para habilitar los exámenes en los CEA y los CALE. Se debe tener en cuenta que el fin último de los OAT en aportar en el mejoramiento de la seguridad vial.

La interoperabilidad para verificar el cumplimiento normativo se establece con las entidades cabeza de sector o en su defecto las entidades regionales responsables de evaluar y aprobar que cada OAT en se área de competencia y responsabilidad cumple con los requisitos para operar. En ese orden de ideas los CRC requieren autorización para operar como IPS por parte de la autoridad en salud, los CEA y CIA requieren autorización de la autoridad en educación y los CDA de la autoridad ambiental. Los CIA además requieren autorización del INPEC.

De otra parte, los profesionales de la salud deben tener licencia vigente para poder actuar en los CRC en la evaluación de aptitudes de los aspirantes a conductores.

6.2.2.2.2 Interoperabilidad para verificación de acreditación o certificación de los OAT

Las normativas establecen que para que un OAT pueda iniciar a operar en la prestación del servicio correspondiente, dependiendo del tipo de OAT, deberá someterse a evaluación para acreditación o certificación por parte del ONAC o un OEC. Adicionalmente los OAT mientras se encuentren operando, deben someterse a visitas periódicas por parte de los mismos organismos para verificar que mantienen las condiciones iniciales que permitieron su entrada a operar y que si se han presentado cambios, esos cambios han pasado por la evaluación de los organismos competentes.

Adicionalmente, los OAT que utilicen equipamientos que deban ser verificados y calibrados, estos deberán ser revisados por el INM para garantizar que funcionan correctamente.

Los mecanismos de interoperabilidad de este grupo de actores deben permitir la automatización de la actualización en el SICOV de los resultados de las actuaciones de cada organismo con el propósito de garantizar la calidad de los servicios ofrecidos a los usuarios y que afectan directamente la exactitud de los certificados que expiden los diferentes OAT.

6.2.2.2.3 Interoperabilidad para la automatización y el control operativo

Un factor de alta relevancia para garantizar que las acciones por los OAT con el propósito de otorgar un certificado están siendo realizadas sobre el sujeto motivo de la certificación. En ese orden de ideas es de imperiosa necesidad poder validar y garantizar que las personas que acceden a un OAT son realmente quien dicen ser. La interoperación con la RNEC o con otras instancias oficiales como Migración Nacional y las centrales de riesgo que permitan realizar estas validaciones son indispensables para evitar posibles suplantaciones.

De otra parte, para garantizar el pago que debe realizar el usuario para recibir el servicio que prestan los OAT, y cumplir con los mandatos normativos, se deben establecer acciones de interoperabilidad con los aliados financieros que ofrezcan servicios de recaudo y distribución de los recursos entre los actores destinatarios de dichos recursos.

Un aspecto de máxima prioridad es el relacionado con el cumplimiento de incorporar los resultados de los procesos realizados por los OAT en el RUNT, como requisito para su validez final. Por lo tanto, esta acción de interoperabilidad es la de mayor incidencia en la eficiencia operativa de los OAT para permitir cumplir el requisito y darle validez al certificado generado por los OAT. Igualmente ocurre con el certificado de asistencia a cursos de reeducación en los CIA que habilita el descuento en el valor a pagar por cuenta de la infracción cometida, esto implica que el certificado debe ser ingresado al SIMIT inmediatamente se finalice el curso.

6.2.2.3 Catálogo de servicios de intercambio de información TO BE

Con base en las necesidades de intercambio de información identificadas en los flujos de datos entre las actividades realizadas de los OAT, se establece la necesidad de los servicios de intercambio de información que se presentan en la Tabla 16 Servicios de intercambio de información SICOV TO B.

Tabla 16 Servicios de intercambio de información SICOV TO BE

Organización	Dirección	Métodos	Descripción
Aliado financiero	Bidireccional	• Consultar PIN • Quemar PIN	Este servicio permite consultar con el número de documento de identidad del usuario si tiene disponible algún PIN para el servicio que está solicitando en el OAT. También permite que en caso de existir un PIN adecuado solicite su asignación y uso (quemado) como medio de pago del servicio.
RUNT	Bidireccional	• Validar inscripción usuario • Incorporar certificado personal	Este servicio permite verificar que el objeto de evaluación por parte del OAT (persona o vehículo) está debidamente inscrito en el RUNT. También permite incorporar la información que por norma deba

Organización	Dirección	Métodos	Descripción
		• Consultar vehículo y características • Incorporar FUR • Incorporar certificado RTMYEC	sumarse al registro personal o del vehículo.
RNEC	Unidireccional	• Validar identidad de persona	Este servicio permite mediante un proceso de validación biométrica, determinar que el documento de identidad presentado por el usuario y las minucias tomadas y enviadas coincide con los registros biométricos (dactilares, faciales, otros) registrados en la RNEC bajo ese documento.
SIMIT	Unidireccional	• Incorporar certificado	Este servicio permite reportar al SIMIT que el usuario identificado con el documento presentado realizó el curso que lo hace acreedor al descuento de acuerdo con las reglas propias del SIMIT para descontar al valor a pagar por la infracción cometida.
ONAC	Unidireccional	• Incorporar / actualizar estado de acreditación	Este servicio permite que la ONAC incorpore al SICOV todos los resultados relevantes para determinar el cumplimiento normativo por parte de un OAT al momento de entrar en operación, así como los resultados de las visitas posteriores para verificar la continuidad en el cumplimiento y ajustes por cambios en el OAT
OEC-INM	Unidireccional	• Incorporar / actualizar estado de certificación	Este servicio permite que la ONAC incorpore al SICOV todos los resultados relevantes para determinar el cumplimiento normativo por parte de un OAT al momento de entrar en operación, así como los resultados de las visitas posteriores para verificar la

Organización	Dirección	Métodos	Descripción
			continuidad en el cumplimiento y ajustes por cambios en el OAT
MinTransporte	Unidireccional	• Enviar información sectorial	Este componente deberá permitir el flujo de toda la información del Mintransporte relativa al SICOV para los fines pertinentes al sector
SuperTransporte	Bidireccional	• Enviar información control • Enviar tarifas OAT • Administrar parámetros de control SICOV	Este servicio permite que la SuperTransporte disponga de la información que requiera para cumplir con su responsabilidad misional de ejercer vigilancia y control sobre los OAT. El servicio también deberá permitir que la SuperTransporte a través del canal habilitado para el efecto, realice la gestión de los controles del SICOV en cuanto a activación y manejo de tolerancias
Entidades involucradas en la autorización OAT	Unidireccional	• Incorporación de estados de autorizaciones	Este servicio deberá permitir que todas las entidades que tienen inherencia en la autorización para la operación de los OAT puedan incorporar y actualizar el estado de dicha autorización. Entre otras entidades están inicialmente las siguientes autoridades competentes en: • Salud autorización CRC como IPS • Educación autorice servicio educativo • INPEC para autorizar CIA • Ambiental para CDA
ANSV	Unidireccional	• Liquidación y dispersión de recursos recaudados	Este servicio deberá permitir que periódicamente se envíe a la ANSV las liquidaciones de los recursos recaudados por la prestación de servicios por parte de los OAT

Fuente: Elaboración propia Grow Data 2021

6.3 Arquitectura de Datos

6.3.1 Arquitectura Conceptual

Los artefactos de la Arquitectura de Datos incluyen especificaciones utilizadas para describir el estado deseado, definir requerimientos de datos, guiar la integración de datos y controlar los activos de datos tal como se describe en una estrategia de datos. Para efectos del sistema SICOV y alineados al Marco de referencia de Arquitectura de MinTIC y al DAMA se proponen artefactos como catálogos y diagramas que se abordan en los siguientes apartados:

6.3.1.1 Catálogo de datos

Para el sistema SICOV y como parte de los artefactos que conforman la arquitectura de datos TO BE se aborda el catálogo de entidades de datos:

6.3.1.1.1 Entidades de datos

El catálogo de entidades de datos TO BE lista y contextualiza las entidades de datos de los diferentes Organismos de Apoyo al Transito – OAT; se describe el contenido de cada una de las hojas del catálogo; teniendo en cuenta que las entidades nuevas se encuentran resaltadas por filas con color de relleno, así como aparece en la Ilustración 73. Catálogo entidades de datos ToBe.

- CRC, se encuentran 44 entidades de datos identificadas en el CRC.
- CEA, se encuentran 73 entidades de datos identificadas en el CEA.
- CIA, se encuentran 40 entidades de datos identificadas en el CIA.
- CDA, se encuentran 23 entidades de datos identificadas en el CDA.
- CALE, se encuentran 26 entidades de datos identificadas en el CALE.

A continuación, se presenta en la Ilustración 73. Catálogo entidades de datos ToBe, donde se puede observar cada una de las entidades identificadas. Este artefacto se entrega como Anexo Arq.Datos_Catálogo_Entidades_Datos_ToBe.xlsx a este documento. De igual forma el catálogo completo se encuentra en la herramienta ARCHI - Archimate Modelling.

Ilustración 73. Catálogo entidades de datos ToBe

Catálogo Entidades de Datos - CIA

ID	Nombre	Descripción	Nombre Dominio	Fuente	Fecha Identificación	Fecha de Actualización	Fecha de Retiro
EN_CIA_19	Datos Capacitador	Esta entidad, contiene los elementos requeridos para soportar el proceso del flujo de información de los datos de los capacitadores en donde se encuentra su hojas de vida, licencias de conducción y categorías de licencias. En esta entidad también se encuentran los datos del personal administrativo.	Gestión de la Conformidad	Resolución No. 60832 de 2016 / Resolución 20203040011355 de 2020	30/09/2021		
EN_CIA_20	Datos Reportes OAT	Esta entidad, contiene los elementos requeridos para soportar el proceso del flujo de información de los datos de informes estadísticos y de cumplimiento solicitados según los requerimientos que realice la ST y otras autoridades competes que lo requieran.	Reportes	Resolución No. 60832 de 2016 / Resolución 20203040011355 de 2020	30/09/2021		
EN_CIA_21	DATOS_CONNECTA_CERTIFICADOSCALIDAD	Esta entidad, contiene los elementos requeridos para soportar el proceso del flujo de información de los certificados de calidad de los habilitados - Este aplicativo tiene como objetivo brindar un apoyo a las entidades que certifican los CIA's en Colombia.	Gestión de la Conformidad	Resolución No. 60832 de 2016 / Resolución 20203040011355 de 2020	29/11/2021		
EN_CIA_22	DATOS_CONNECTA_ESTABLECIMIENTOS	Esta entidad, contiene los elementos requeridos para soportar el proceso del flujo de información de los establecimientos o habilitados - Este aplicativo tiene como objetivo brindar un apoyo a las entidades que certifican los CIA's en Colombia.	Gestión de la Conformidad	Resolución No. 60832 de 2016 / Resolución 20203040011355 de 2020	29/11/2021		
EN_CIA_23	DATOS_CONNECTA_INSTRUCTOR_CATEGORIA	Esta entidad, contiene los elementos requeridos para soportar el proceso del flujo de información de los datos del instructor de categoría - Este aplicativo tiene como objetivo brindar un apoyo a las entidades que certifican los CIA's en Colombia.	Gestión de la Conformidad	Resolución No. 60832 de 2016 / Resolución 20203040011355 de 2020	29/11/2021		
EN_CIA_24	DATOS_CONNECTA__CERCAL_ESTADO	Esta entidad, contiene los elementos requeridos para soportar el proceso del flujo de información del estado de certificación de los habilitados o establecimientos - Este aplicativo tiene como objetivo brindar un apoyo a las entidades que certifican los CIA's en Colombia.	Gestión de la Conformidad	Resolución No. 60832 de 2016 / Resolución 20203040011355 de 2020	29/11/2021		
EN_CIA_25	DATOS_CONNECTA_CERCAL_INSTRUCTORES	Esta entidad, contiene los elementos requeridos para soportar el proceso del flujo de información de los instructores - Este aplicativo tiene como objetivo brindar un apoyo a las entidades que certifican los CIA's en Colombia.	Gestión de la Conformidad	Resolución No. 60832 de 2016 / Resolución 20203040011355 de 2020	29/11/2021		
EN_CIA_26	DATOS_CONNECTA_ORGCERTIFICADORES	Esta entidad, contiene los elementos requeridos para soportar el proceso del flujo de información de las organizaciones certificadoras - Este aplicativo tiene como objetivo brindar un apoyo a las entidades que certifican los CIA's en Colombia.	Gestión de la Conformidad	Resolución No. 60832 de 2016 / Resolución 20203040011355 de 2020	29/11/2021		
EN_CIA_27	Objeto Social como CIA	Las OAT deben cumplir con todos los requisitos establecidos por MinTransporte para operar	Gestión de la Conformidad	Resolución 20203040011355 de 2020	29/11/2021		

Guía | CRC | CEA | CIA | CDA | CALE

Fuente: Elaboración propia Grow Data 2021

6.3.1.2 Diagramas

Los diagramas, son una forma de representación que sirve para estructurar información y sintetizar conceptos ya sea para explicarlos a los diferentes stakeholders, o para esclarecer ideas que se estén proponiendo o contextualizando. Para efectos de la arquitectura de datos objetivo (To-Be) se abordaron los diagramas de flujos de información, diagrama de despliegue de infraestructura y soluciones y la arquitectura conceptual (Blue print).

A continuación, se detallan cada uno de los diagramas:

6.3.1.2.1 Flujo de información

Estos artefactos presentan los flujos de los datos propuestos en la arquitectura TO-BE entre las entidades internas, entidades externas, procesos y almacenes de datos de los diferentes Organismos de Apoyo al Transito – OAT.

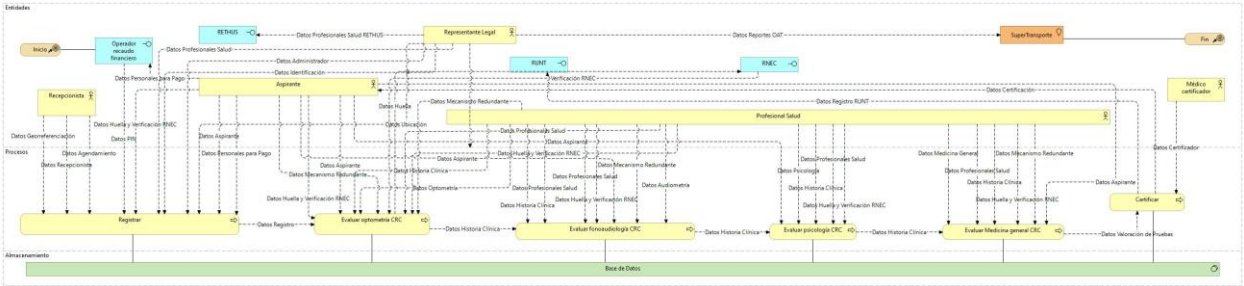
Para la lectura de cada uno de los flujos de información se da con un inicio y un fin, adicional se encuentran organizados por 3 componentes, los cuales son entidades, procesos y almacenamiento; en la parte inicial todo lo relacionado con el primer proceso inscripción de los OAT al SICOV y luego los procesos dentro del OAT para su funcionamiento.

Los flujos de información ilustran las entidades de datos que interactúan con cada uno de los procesos y entidades. Para cada uno de componentes aquí descritos se requiere de cada uno de los catálogos los cuales son los procesos TO BE y las entidades de datos TO BE.

A continuación, se presenta en la Ilustración 74. Flujo de información CRC To Be. En el cual se presentan 5 entidades externas, 5 actores internos, 6 procesos y 1 objeto de almacenamiento.

Este artefacto se entrega como Anexo Arq.Datos_Flujo_Información_CRC_ToBe.pdf a este documento. De igual forma el flujo de información del CRC se encuentra en la herramienta ARCHI - Archimate Modelling.

Ilustración 74. Flujo de información CRC To Be

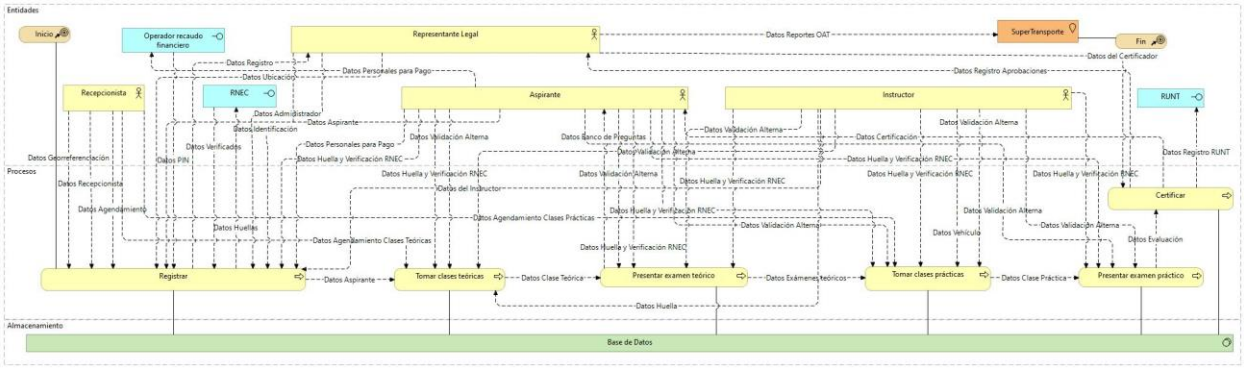


Fuente: Elaboración propia Grow Data 2021

A continuación, se presenta en la Ilustración 75. Flujo de información CEA To Be. En el cual se presentan 4 entidades externas, 4 actores internos, 6 procesos y 1 objetos de almacenamiento.

Este artefacto se entrega como Anexo Arq.Datos_Flujo_Información_CEA_ToBe.pdf a este documento. De igual forma el flujo de información del CEA se encuentra en la herramienta ARCHI - Archimate Modelling.

Ilustración 75. Flujo de información CEA To Be

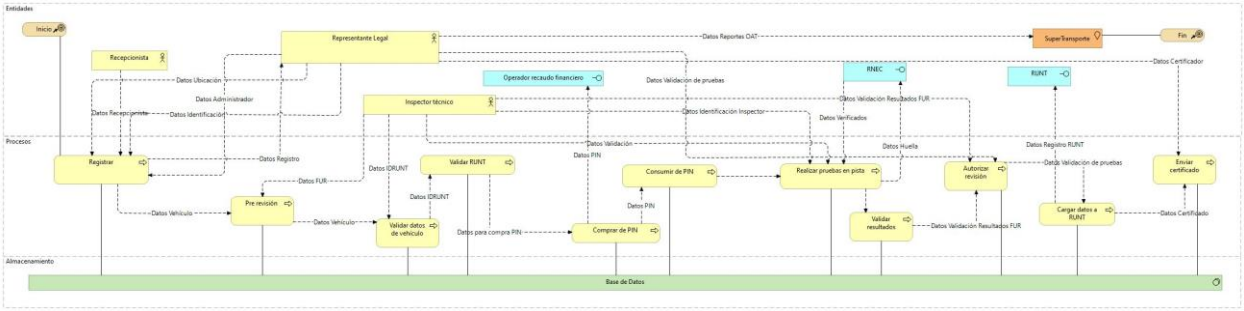


Fuente: Elaboración propia Grow Data 2021

A continuación, se presenta en la Ilustración 76. Flujo de información CDA To Be. En el cual se presentan 4 entidades externas, 3 actores internos, 11 procesos y 1 objeto de almacenamiento.

Este artefacto se entrega como Anexo Arq.Datos_Flujo_Información_CDA_ToBe.pdf a este documento. De igual forma el flujo de información del CDA se encuentra en la herramienta ARCHI - Archimate Modelling.

Ilustración 76. Flujo de información CDA To Be

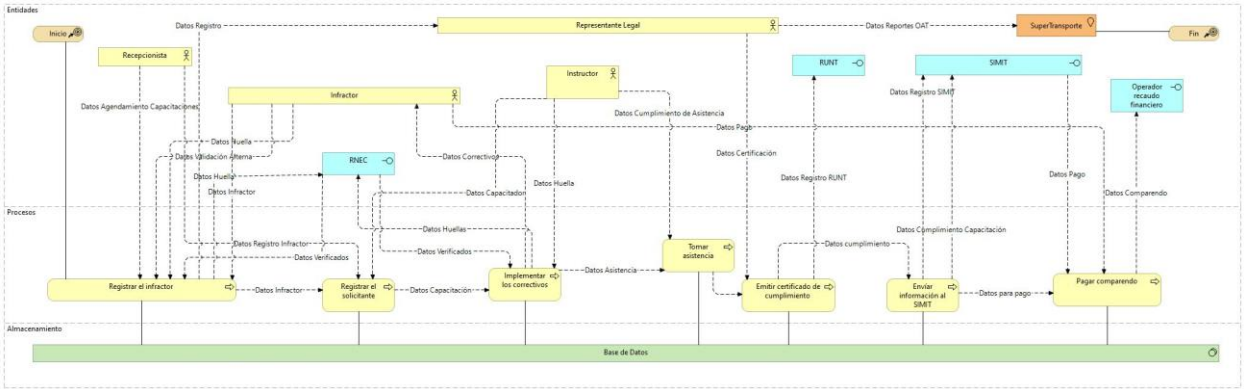


Fuente: Elaboración propia Grow Data 2021

A continuación, se presenta en la Ilustración 77. Flujo de información CIA To Be. En el cual se presentan 5 entidades externas, 4 actores internos, 7 procesos y 1 objeto de almacenamiento.

Este artefacto se entrega como Anexo Arq.Datos_Flujo_Información_CIA_ToBe.pdf a este documento. De igual forma el flujo de información del CIA se encuentra en la herramienta ARCHI - Archimate Modelling.

Ilustración 77. Flujo de información CIA To Be

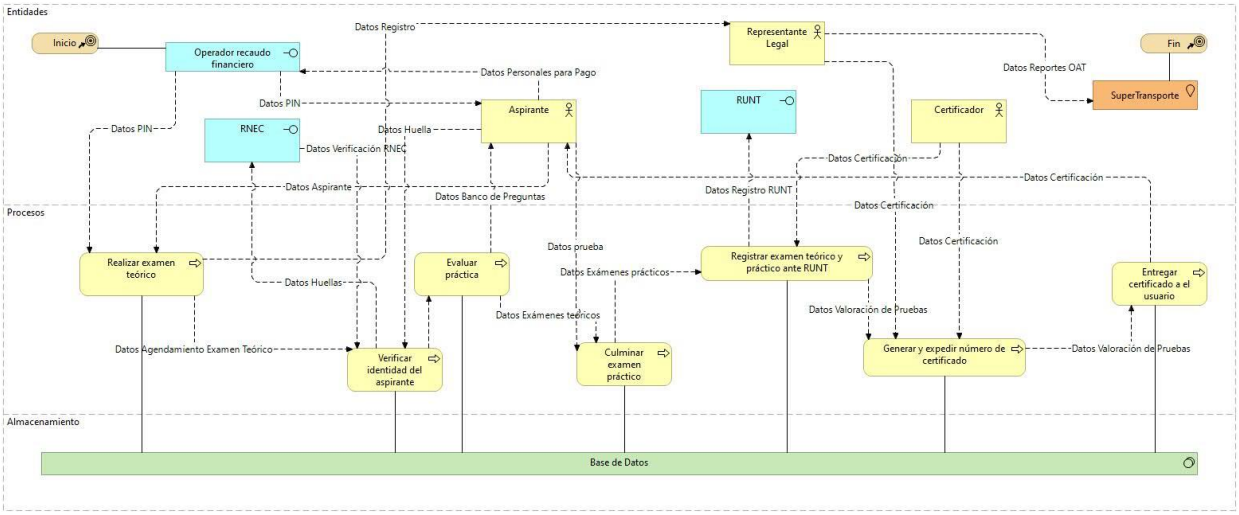


Fuente: Elaboración propia Grow Data 2021

A continuación, se presenta en la Ilustración 78. Flujo de información CALE To Be. En el cual se presentan 4 entidades externas, 3 actores internos, 7 procesos y 1 objeto de almacenamiento.

Este artefacto se entrega como Anexo Arq.Datos_Flujo_Información_CALE_ToBe.pdf a este documento. De igual forma el flujo de información del CALE se encuentra en la herramienta ARCHI - Archimate Modelling.

Ilustración 78. Flujo de información CALE To Be

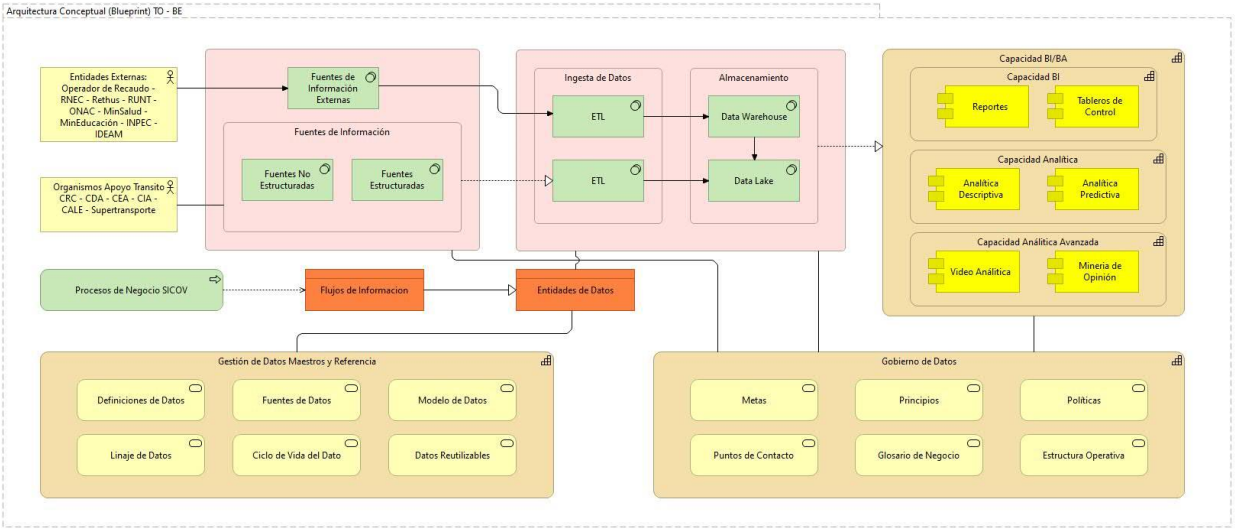


Fuente: Elaboración propia Grow Data 2021

6.3.1.2.2 Arquitectura conceptual TO BE (Blueprint)

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 arquitectura de datos TO BE, con el fin de cerrar las diferentes brechas (ver documento de brechas) y necesidades de capacidades alrededor de la arquitectura de datos:

Ilustración 79. Arquitectura Conceptual To Be



Fuente: Elaboración propia Grow Data 2021

La arquitectura de datos TO BE del sistema SICOV está conformada por los siguientes componentes:

- Entidades: Organizaciones que de forma directa e indirecta deben generan datos hacia el sistema SICOV. Estas se encuentran clasificadas en dos, las entidades externas conformadas por el operador de recaudo, RNEC, Rethus, Runt, ONAC, INPEC, IDEAM, MinSalud y MinEducación y los organismos de apoyo al tránsito: CRC, CDA, CEA, CIA, CALE y la SuperTransporte. Estas entidades dependiendo de la naturaleza de la información generaran datos estructurados y no estructurados dependiendo las necesidades de información (diario, mensual o semestral).

- Fuentes de Información: Conformada por las diferentes estructuras de datos que deben ser generadas por parte de las entidades. Estas se clasifican en fuentes de datos externas, que son datos estructurados en formatos xml o json, según el tipo de tecnología que utilicen las entidades externas para generar la información.

Por otro lado, tenemos las fuentes estructuradas y fuentes no estructuradas; las primeras son generadas por todos los Organismos de Apoyo al Tránsito en formato xml o json y son datos resultantes de la ejecución de los diferentes procesos del sistema, y los datos no estructurados, que son generados por los CDA y son datos conformados en su totalidad por videos de medios de transporte 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.

- Almacenamiento: Este es el componente que tiene un cambio sustancial con relación al AS- IS. Actualmente el sistema SICOV cuenta con diferentes bases datos que dificultan el intercambio y gestión de los datos, por tal motivo, 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 estructurados desde las fuentes externas 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 en una estrategia de colecciones.

  - Almacenamiento: Este componente está conformado por el Data Warehouse y el Data Lake. El primero, en 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.

    El 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.

- Procesos de Negocio, Flujos y Entidades de Datos: Estos componentes tienen como objetivo identificar las diferentes entidades de datos que conforman el sistema SICOV. Inicialmente se identifican y contextualizan los procesos de negocio (descritos y diseñados en el dominio de negocio); estos procesos son insumos para el diagrama de flujos de datos (ver sección de diagramas), donde se puede apreciar cómo deben interactúan con las diferentes entidades de datos y las bases de datos.

- Finalmente, se debe generar las entidades de datos en los catálogos de dominios y 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

alimentado por cambios en los procesos, normativa y necesidades alrededor de los datos.

- 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.

  - 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 o los posibles 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 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 diferentes Organismos de Apoyo al Tránsito y tomar acciones de mejoras.

- Estrategia de gobierno de Datos: La implementación de una estrategia de Gobierno de Datos permite desarrollar políticas y procedimientos para el control y custodia de datos en múltiples niveles dentro del sistema del SICOV. Así como las conductas necesarias para gestionar los datos como un activo de manera exitosa.

- Estrategia de datos maestros y referencia: La implementación de esta estrategia permitirá:

  - Cumplir con los requisitos de datos del sistema SICOV: tener acceso a los mismos conjuntos de datos, con la confianza de que los conjuntos de datos son completos, actuales y consistentes. Los Datos Maestros a menudo forman la base de estos conjuntos de datos.

  - Gestionar la calidad de los datos: Inconsistencias de datos, problemas de calidad y brechas conducen a decisiones incorrectas o a oportunidades

perdidas; la Gestión de Datos Maestros reduce estos riesgos al permitir una representación consistente de las entidades críticas para la organización.

- Gestionar los costos de integración de datos: El costo de integrar nuevas fuentes de datos en un entorno ya complejo es mayor en ausencia de Datos Maestros, lo que reduce la variación en cómo las entidades críticas son definidas e identificadas.

- Reducir el riesgo: Los Datos Maestros pueden permitir la simplificación de la arquitectura de intercambio de datos para reducir costos y riesgos asociados con un entorno complejo.

En términos generales, se puede concluir de la arquitectura de Datos, lo siguiente:

- Debe existir una arquitectura de información documentada y un repositorio que exponga los aspectos asociados con modelamiento, entidades del dato corporativas, modelos conceptuales, lógicos y físicos de manera integral.

- debe existir un catálogo de componentes de información del sistema SICOV de acuerdo con las mejores prácticas del DAMA, el cual incluye la recopilación de la información de atributos de información, atributos de los datos, flujos de información, servicios de información y la matriz de relación entre la información, los servicios de información y los atributos de datos.

- Con respecto al manejo de datos maestros y de referencia, para el sistema SICOV de debe contar con una política, arquitectura, definición y herramienta para su gestión.

- Se debe implementar una estrategia de gobierno de datos, que permita asegurar que los datos se gestionen correctamente, de acuerdo con las políticas y las mejores prácticas. Es importante que el gobierno de Datos este alineado directamente con la estrategia de la organización.

- Debe existir una estrategia de almacenamiento centralizada que permita tener mayor control y gobierno sobre las diferentes fuentes de datos. Se propone una bodega de datos para la información de las entidades externas y un Data Lake para toda la información generada por el sistema SICOV, independientemente si es data estructurada y no estructurada.

- Debe implementarse una estrategia de inteligencia de negocios y analítica que permita a partir de la implementación de tableros de control y modelos de inteligencia artificial poder tomar decisiones que apoyen el control y gestión sobre los procesos del sistema SICOV.

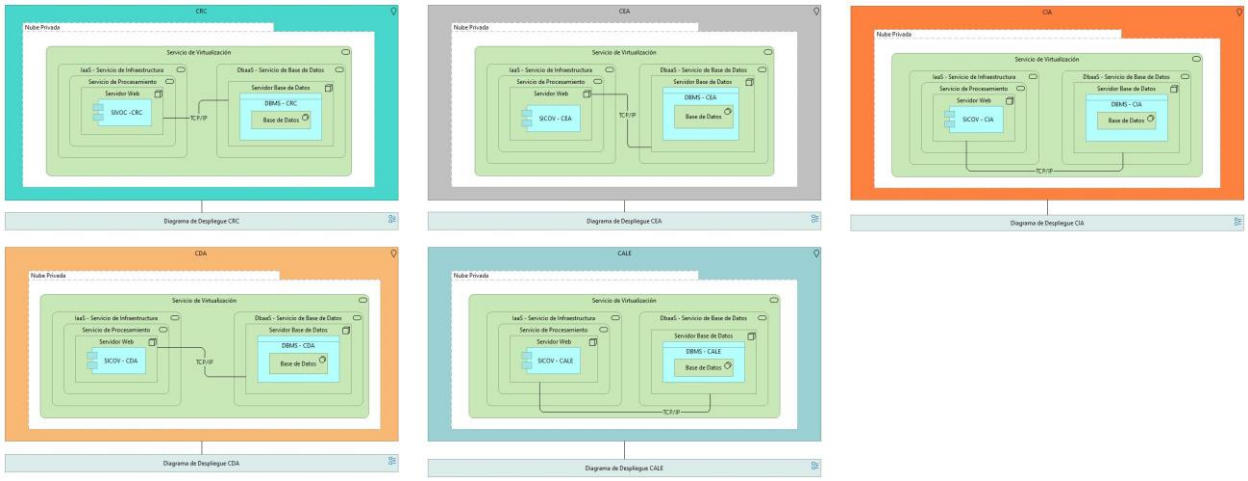
- Debe implementarse una estrategia de interoperabilidad de información basada en X-ROAD y en servicios web, que brinden los componentes necesarios para el intercambio de información (se detallara esta estrategia en el dominio de sistemas de información). Esta estrategia se propone que sea de forma incremental teniendo en cuenta las capacidades de las otras entidades del estado.

Este artefacto se entrega como Anexo Arq.Datos_Arquitectura_Conceptual_ToBe.pdf a este documento. La Arquitectura Conceptual To Be se encuentra en la herramienta ARCHI - Archimate Modelling.

6.3.1.2.3 Diagrama de despliegue de la infraestructura y las soluciones para la gestión de información

El diagrama de despliegue de la ilustración 81 modela el servicio tecnológico de base de datos, enfocado como servicio en la nube.

Ilustración 80. Diagrama de despliegue To Be



Fuente: Elaboración propia Grow Data 2021

- **CRC**

  Servicio de Base de Datos (DBaaS): Dentro de este servicio se despliegan los componentes (bases de datos estructuradas y/o no estructuradas) que buscan proporcionar espacio de almacenamiento para un determinado número de base de datos; permitiendo los correspondientes accesos, estas bases de datos reciben y gestionan la información de la capa de procesamiento donde se encuentran los servidores web (SICOV-CRC), según el modelo de operación definido.

- **CDA**

  Servicio de Base de Datos (DBaaS): Dentro de este servicio se despliegan los componentes (bases de datos estructuradas y/o no estructuradas) que buscan proporcionar espacio de almacenamiento para un determinado número de base de datos permitiendo los correspondientes accesos, estas bases de datos reciben y gestionan la información de la capa de procesamiento donde se encuentran los servidores web (SICOV-CDA), según el modelo de operación definido.

- **CEA**

  Servicio de Base de Datos (DBaaS): Dentro de este servicio se despliegan los componentes (bases de datos estructuradas y/o no estructuradas) que buscan proporcionar espacio de almacenamiento para un determinado número de base de datos permitiendo los correspondientes accesos, estas bases de datos reciben y gestionan la información de la capa de procesamiento donde se encuentran los servidores web (SICOV-CEA), según el modelo de operación definido.

- **CIA**

  Servicio de Base de Datos (DBaaS): Dentro de este servicio se despliegan los componentes (bases de datos estructuradas y/o no estructuradas) que buscan proporcionar espacio de almacenamiento para un determinado número de base de datos permitiendo los correspondientes accesos, estas bases de datos reciben y gestionan la información de la capa de procesamiento donde se encuentran los servidores web (SICOV-CIA), según el modelo de operación definido.

- **CALE**

  Servicio de Base de Datos (DBaaS): Dentro de este servicio se despliegan los componentes (bases de datos estructuradas y/o no estructuradas) que buscan proporcionar espacio de almacenamiento para un determinado

número de base de datos permitiendo los correspondientes accesos, estas bases de datos reciben y gestionan la información de la capa de procesamiento donde se encuentran los servidores web (SICOV-CALE), según el modelo de operación definido.

El diagrama de despliegue se encuentra en la herramienta ARCHI - Archimate Modelling y dentro de cada uno de los OAT descritos se encuentra un link directo al diagrama de despliegue completo de infraestructura tecnológica.

Este artefacto se entrega como Anexo Arq.Datos_Diagrama_despliegue_datos_ToBe.pdf a este documento.

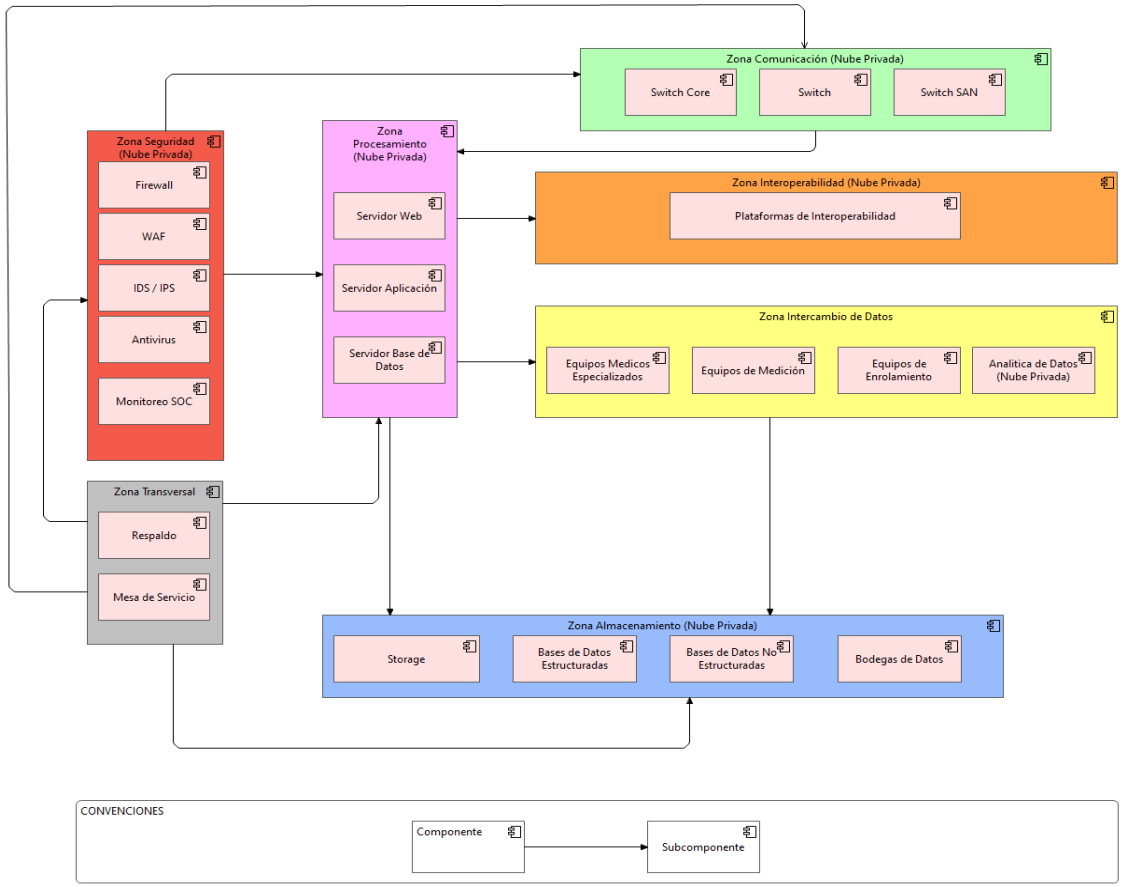
6.4 Arquitectura de infraestructura

La arquitectura deseada del domino de infraestructura inicia desde un ejercicio de diseño conceptual que resulta del análisis de la situación actual As Is y la cual termina con el enfoque de plantear la infraestructura tecnológica como servicio en nube privada, identificando aspectos estratégicos como la visión y la recolección de información realizados desde todos los dominios, junto con el ejercicio propio de arquitectura.

6.4.1 Arquitectura conceptual TO BE (Blueprint)

El diseño conceptual hace parte de las etapas de análisis To-Be como guía de la visión tecnológica que se recomienda seguir al SICOV a partir del ejercicio de Arquitectura.
La siguiente figura presenta el entorno del diseño de zonas y sus relaciones con los componentes.

Ilustración 81. Arquitectura Conceptual Blue Print To Be



Fuente: Elaboración propia Grow Data 2021

- Zona de Seguridad (nube privada): La zona de seguridad (nube privada) agrupa aquellos componentes lógicos necesarios que asegurará la debida protección al sistema de información SICOV contra ataques de ciberseguridad en la capa de aplicación como en la capa de bases de datos, bajo el entorno de la nube privada.

- Zona de Comunicación (nube privada): La zona de comunicación (nube privada) agrupa aquellos componentes lógicos necesarios que garantizan la debida comunicación entre los equipos de procesamiento y almacenamiento que apalancan al SICOV, bajo el entorno de la nube privada.

- Zona de Procesamiento (nube privada): La zona de procesamiento (nube privada) agrupa aquellos componentes lógicos que son necesarios para poder procesar el sistema de información del SICOV y la información generada dentro de su funcionalidad, bajo el entorno de la nube privada.

- Zona de Almacenamiento (nube privada): La zona de almacenamiento (nube privada) agrupa aquellos componentes lógicos necesarios para poder almacenar y respaldar la información generada dentro de la operación del sistema SICOV, bajo el entorno de la nube privada.

- Zona de Interoperabilidad (nube privada): La zona de interoperabilidad (nube privada) agrupa aquellos componentes lógicos necesarios para el intercambio de información entre el SICOV y los diferentes interesados externos, bajo el entorno de la nube privada.

- Zona Intercambio de Datos: La zona de intercambio de datos agrupa aquellos componentes lógicos necesarios para garantizar la recopilación y la captura de los datos capturados por los diferentes organismos de apoyo al tránsito de cara al ciudadano.

- Zona Transversal: La zona transversal agrupa aquellos componentes lógicos que son necesarios para brindar el apoyo a la operación del SICOV ya sea de manera preventiva y/o reactiva.

6.4.2 Arquitectura de solución

En esta arquitectura se puede contar con todos los recursos tecnológicos en modalidad por servicios. De esta forma, aloja y provee servicios tecnológicos desde una nube de servicios para las capas de infraestructura (IaaS), plataforma (PaaS), Base de Datos

(DbaaS) y Analítica (AaaS). El acceso a estos servicios obliga a contar con un portafolio soportado por la infraestructura por demanda permitiendo el crecimiento o decrecimiento dinámico de sus capacidades desde un fuerte elemento de gestión. Este concepto lo implementan los grandes fabricantes como capacidad elástica o arquitectura tecnológica flexible.

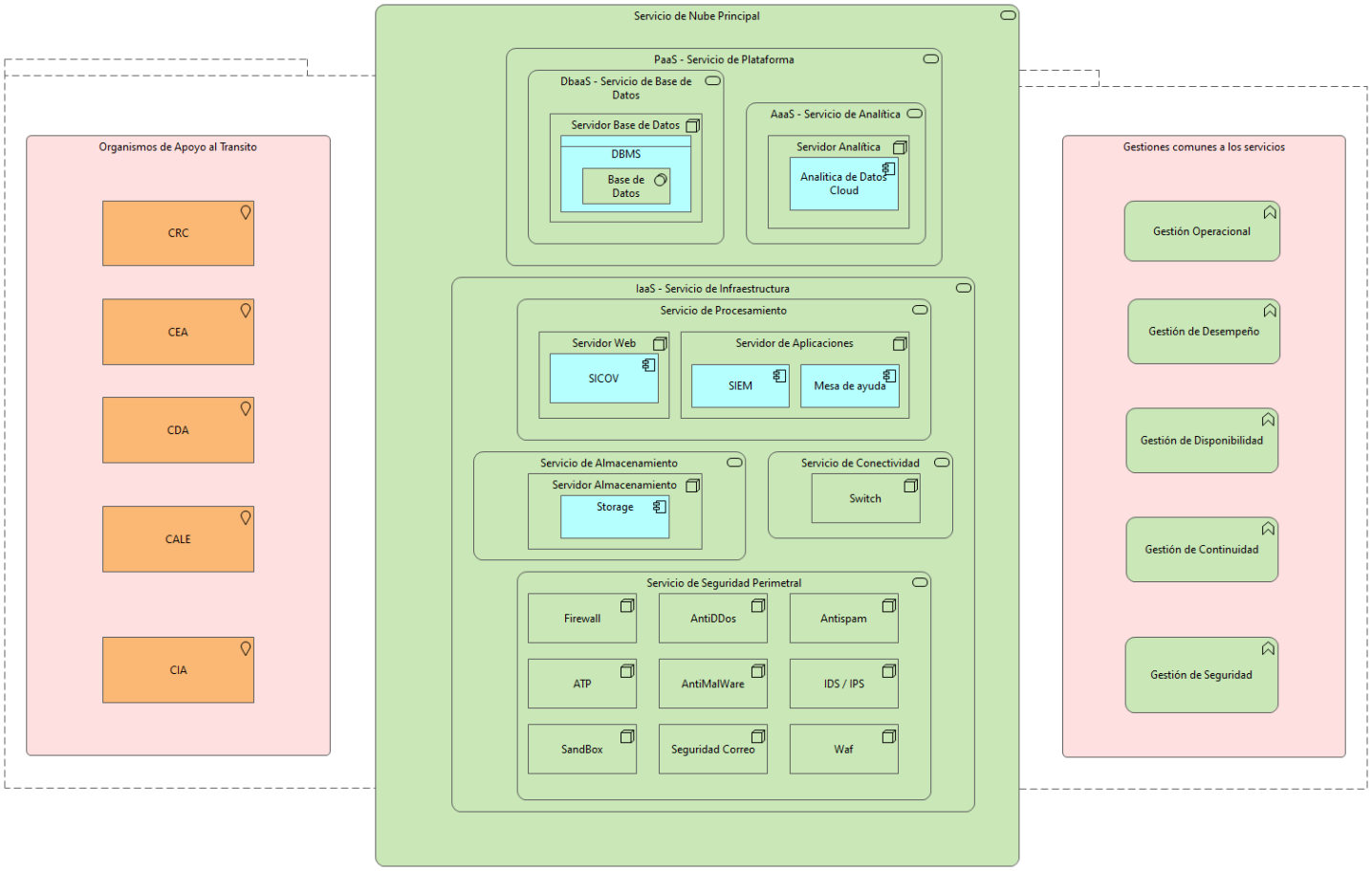
La Arquitectura de Infraestructura propuesta, se define a través del concepto de XaaS – Componentes de Infraestructura como servicio. De esta forma la arquitectura propuesta podrá ser implementada a través de infraestructura física (elementos de hardware on - premise), a través de servicios de infraestructura en nube o una combinación de los dos.

Todos los componentes de las soluciones instaladas en esta arquitectura de solución deben poder funcionar en esquemas asociados a la demanda y a la capacidad dinámica en todas sus capas.

Desde el punto de vista de arquitectura, esta arquitectura de solución puede crecer y decrecer los servicios tecnológicos y componentes lógicos de infraestructura de acuerdo con los requerimientos.

Los anteriores conceptos podrán ser implementados a través de la creación de una nube privada ya bien sea con infraestructura física propia del operador de SICOV, un proveedor de servicios de CPD (Centro de Procesamiento de Datos), proveedores de VDC (Virtual Data Center) o en general, proveedores de servicios de infraestructura tecnológica que habiliten la creación de los compontes propuestos dentro de la presente arquitectura. Lo que finalmente se busca con esta estrategia es brindar flexibilidad en el diseño e implementación de la Arquitectura de Infraestructura propuesta mitigando la dependencia del hardware de los servicios de infraestructura definidos.

Ilustración 82. Arquitectura de Solución To Be



Fuente: Elaboración propia Grow Data 2021

En este diagrama se muestra la arquitectura de solución para los diferentes organismos de apoyo al tránsito (CRC, CEA, CDA, CALE y CIA), la cual se encuentra enmarcada en los diferentes servicios mencionados anteriormente y los cuales buscan fortalecer la gestión operacional, la gestión de desempeño, la gestión de disponibilidad, gestión de continuidad y la gestión de seguridad de estos servicios, descritos a continuación:

- Infraestructura como servicio (IaaS)
  Posibilita que los servicios tradicionales de infraestructura como data center, comunicación, seguridad perimetral, almacenamiento o servidores (físicos o virtuales) puedan crecer de manera dinámica y de forma casi instantánea teniendo como apoyo la nube.

  Contar con un esquema de infraestructura como servicio implica necesariamente que los servicios locales también hagan parte del servicio desde el componente local incluyendo lógicas de conexión (Convergencia) informática de "alto rendimiento" mediante la conformación de mallas o clústeres de infraestructura o la agregación de demanda según la necesidad.

- Plataforma como servicio (PaaS)

  Permite que servicios básicos considerados de plataforma tales como herramientas de desarrollo, plataformas de monitoreo, etc., se ofrezcan como un paquete que puede crecer o decrecer según la demanda. Para el caso de la arquitectura propuesta, las plataformas como servicio serían apropiada para la implementación de los controles de seguridad como los Firewall, WAF o IDS/IPS. Estos elementos se recomiendan inicialmente ser implementados como infraestructura como servicio, pero podrían ser usuarios a través de la modalidad de PaaS o SaaS.

- Base de Datos como servicio (DBaaS)

  Permite organizar, filtrar y almacenar los datos generados en la operación del SICOV en un software fácilmente accesible y recuperable.
  Al utilizar el software DBaaS no se tendría que diseñar y construir las bases de datos partiendo desde cero, en su lugar, se pueden personalizar y crear una base de datos personalizada en la nube utilizando una solución DBaaS enfocando el esfuerzo de diseño en los objetos y componentes de la base de datos y dejando de lado el diseño e implementación de la infraestructura asociada a soporte y operación del motor de base de datos, dado que estas son labores inmersas dentro del servicio asumidas por el proveedor.

- Analítica como servicio (AaaS)

  Se contempla una plataforma para gestionar información estratégica para el apoyo a la toma de decisiones, a partir de realizar el análisis de grandes volúmenes de datos, actuando como puntos centralizados de múltiples fuentes de información, brindando de esta forma la posibilidad de tener un único punto de procesamiento de información sin que esto genere cargas adicionales de procesamiento a la base de datos transaccional de SICOV.

  La definición de la Arquitectura de Infraestructura soportada a través del concepto de XaaS (Componentes de Infraestructura como servicio) busca aprovechar las capacidades a nivel de:

- **Dimensionamiento**: uno de los grandes retos a nivel de implementación de infraestructura física de hardware está asociado a que es obligatorio tener un dimensionamiento de cada uno de los elementos que harán parte de la arquitectura de infraestructura. Bajo el concepto de XaaS se podrá hacer una implementación de la Arquitectura propuesta aprovechando el concepto de flexibilidad o elasticidad en la infraestructura.

- **Crecimiento horizontal**: La implementación de todos los componentes de una infraestructura tecnológica implica grandes retos asociados a la compatibilidad de componentes, instalación, configuración y puesta en marcha de dichos elementos. Bajo el concepto de Xaas se pueden encontrar diversos proveedores de servicios de infraestructura con múltiples componentes que pueden ser activados o desactivados bajo demanda. Este es uno de los grandes beneficios que se plantea aprovechar dado que esto reduce los tiempos de implementación y los riesgos asociados a la integración de componentes de infraestructura.

- **Disponibilidad**: uno de los grandes conceptos que debe implementar la arquitectura propuesta es la disponibilidad entre los servicios y la resiliencia entendida como la capacidad de recuperar el servicio lo más pronto posible. bajo el concepto de XaaS se busca obtener todos los beneficios asociados a la alta disponibilidad de los componentes que soportan el servicio tecnológico, la capacidad de recuperación y el soporte en todos los niveles de estos componentes provistos por el proveedor, transfiriendo el riesgo de la continuidad de los componentes a este y obteniendo los beneficios materializados a través de altos niveles de disponibilidad de los servicios de infraestructura tecnológica.

- **Costos**: una de las grandes promesas de generación de valor del concepto de XaaS es la optimización de costos a través de una reducción del Opex y el Capex. los servicios básicos bajo esta modalidad en su gran mayoría no requieren inversiones iniciales son costos únicamente asociados al Opex y estos son optimizados a través de la transferencia de responsabilidades a nivel de administración, operación y soporte, los cuales son costos manejados de una forma optimizada a través de economías de escala por parte del proveedor de estos.

- **Despliegue**: uno de los grandes beneficios de la modalidad XaaS y la cual se busca explotar es la reducción de los tiempos de despliegue y la puesta en marcha de los elementos que soportan la infraestructura tecnológica. Dado que los proveedores de este tipo de servicios cuentan con los elementos ya en producción, estabilizados y configurados, la implementación de estos servicios para SICOV tendrían una optimización a nivel de tiempos de puesta en producción.

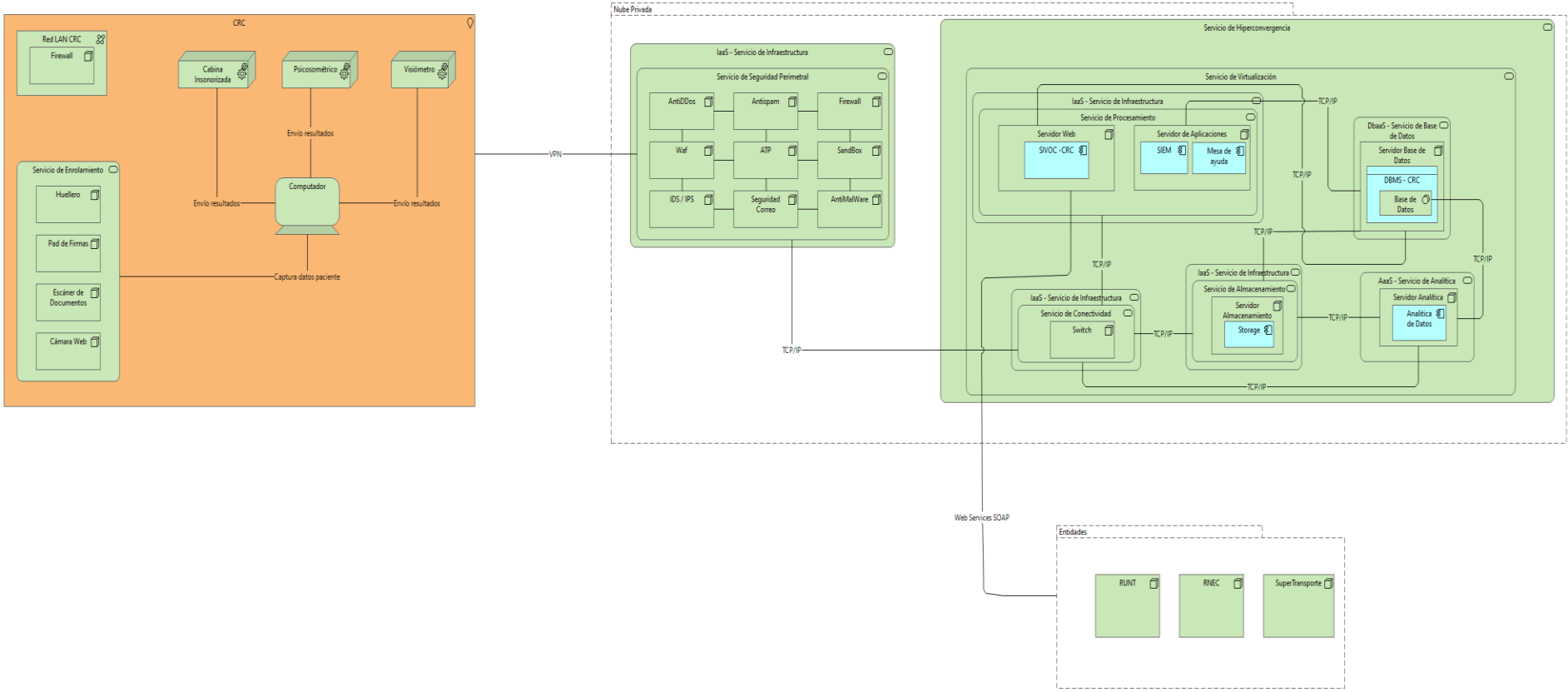
6.4.3 Diagramas de despliegue

En este capítulo se muestran los diagramas de despliegue para los diferentes organismos de apoyo al tránsito (CRC, CEA, CDA, CALE y CIA) de acuerdo con la arquitectura de solución propuesta en el capítulo anterior, detallando la relación entre los diferentes componentes que se encontrarán desplegados para apalancar la operación del SICOV.

6.4.3.1 Diagrama de despliegue para los CRC

En este diagrama se pueden visualizar los diferentes componentes que hacen parte de los diferentes servicios tecnológicos desplegados y enfocados como servicios en la nube de la infraestructura centralizada y su relación con la infraestructura de la operación de los CRC.

Ilustración 83. Diagrama de despliegue To-Be CRC



Fuente: Elaboración propia Grow Data 2021

Desde la operación realizada desde los OAT (CRC), se realiza la conexión segura mediante una VPN a los siguientes servicios:

- Servicio de Seguridad Perimetral (IaaS Servicio de Infraestructura): Dentro de este servicio se despliegan los diferentes componentes que buscan asegurar la defensa de las redes informáticas mediante la implementación de controles especializados (WAF/ firewall, antiDDoS, ATP, Sandbox, IDS/IPS, seguridad al correo y antimalware)en los que se establecen políticas de seguridad necesarias para la protección perimetral ante potenciales ataques internos y externos que afecten la confidencialidad, integridad y disponibilidad de los activos de información que controlan SICOV.

- Servicio de Conectividad (IaaS Servicio de Infraestructura): Dentro de este servicio se despliegan los componentes que buscan brindar la capacidad de establecer la conexión y la comunicación entre los demás componentes de infraestructura que apalancan la operación del SICOV. Se deben tener en cuenta los estándares y protocolos que ayudan a que el hardware y el software necesarios para la operación del SICOV trabajen de manera conjunta permitiendo que estos se comuniquen a través de la red informática.

- Servicio de Procesamiento (IaaS Servicio de Infraestructura): Dentro de este servicio se despliegan los componentes (servidores físicos y/o virtuales) que buscan brindar la capacidad de procesar, gestionar y difundir datos y aplicaciones relevantes para la operación del SICOV, como son el SICOV-CRC, correlacionador de eventos, software para mesa de ayuda.

- Servicio de Base de Datos (DBaaS): Dentro de este servicio se despliegan los componentes (bases de datos estructuradas y/o no estructuradas) que buscan proporcionar espacio de almacenamiento para un determinado número de base de datos permitiendo los correspondientes accesos, estas bases de datos reciben y gestionan la información de la capa de procesamiento donde se encuentran los servidores web (SICOV-CRC) y los servidores de aplicaciones (SIEM y mesa de ayuda).

- Servicio de Almacenamiento (IaaS Servicio de Infraestructura): Dentro de este servicio se despliegan los componentes (storage) que buscan almacenar los datos generados por el SICOV a través de servidores especializados donde estos datos quedan alojados en espacios de almacenamiento físico y/o virtual. Estos componentes reciben y almacenan la información de la capa de base de datos.

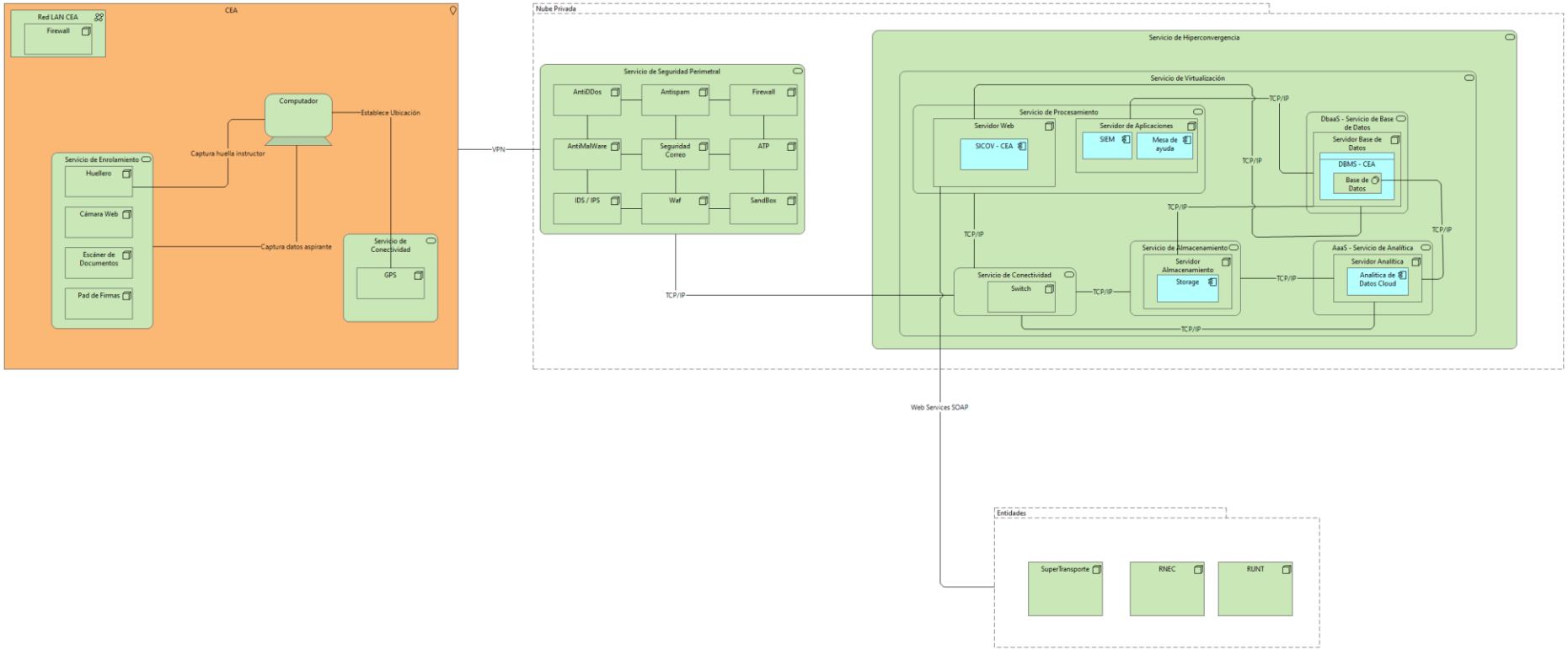
- Servicio de Analítica (AaaS): Dentro de este servicio se despliegan los componentes (analítica de datos) que permiten la gestión y el análisis de un gran volumen de datos generados dentro de la operación del SICOV y que ayudan a la toma de decisiones y al proceso de control y vigilancia. Estos componentes reciben y procesan la información procesada en las bases de datos del SICOV.

- Servicio de virtualización: Dentro de este servicio se despliegan los componentes que facilitan la creación de una forma virtual los diferentes elementos de cómputo requeridos para proveer los recursos necesarios para la operación del SICOV.

6.4.3.2 Diagrama de despliegue para los CEA

En este diagrama se pueden visualizar los diferentes componentes que hacen parte de los diferentes servicios tecnológicos desplegados y enfocados como servicios en la nube de la infraestructura centralizada y su relación con la infraestructura de la operación de los CEA.

Ilustración 84. Diagrama de despliegue To Be CEA



Fuente: Elaboración propia Grow Data 2021

Desde la operación realizada desde los CEA, se realiza la conexión segura mediante una VPN a los siguientes servicios:

- Servicio de Seguridad Perimetral (IaaS Servicio de Infraestructura): Dentro de este servicio se despliegan los diferentes componentes que buscan asegurar la defensa de las redes informáticas mediante la implementación de controles especializados (WAF/ firewall, antiDDoS, ATP, Sandbox, IDS/IPS, seguridad al correo y antimalware)en los que se establecen políticas de seguridad necesarias para la protección perimetral ante potenciales ataques internos y externos que afecten la confidencialidad, integridad y disponibilidad de los activos de información que controlan SICOV.

- Servicio de Conectividad (IaaS Servicio de Infraestructura): Dentro de este servicio se despliegan los componentes que buscan brindar la capacidad de establecer la conexión y la comunicación entre los demás componentes de infraestructura que apalancan la operación del SICOV. Se deben tener en cuenta los estándares y protocolos que ayudan a que el hardware y el software necesarios para la operación del SICOV trabajen de manera conjunta permitiendo que estos se comuniquen a través de la red informática.

- Servicio de Procesamiento (IaaS Servicio de Infraestructura): Dentro de este servicio se despliegan los componentes (servidores físicos y/o virtuales) que buscan brindar la capacidad de procesar, gestionar y difundir datos y aplicaciones relevantes para la operación del SICOV, como son el SICOV-CEA, correlacionador de eventos, software para mesa de ayuda.

- Servicio de Base de Datos (DBaaS): Dentro de este servicio se despliegan los componentes (bases de datos estructuradas y/o no estructuradas) que buscan proporcionar espacio de almacenamiento para un determinado número de base de datos permitiendo los correspondientes accesos, estas bases de datos reciben y gestionan la información de la capa de procesamiento donde se encuentran los servidores web (SICOV-CEA) y los servidores de aplicaciones (SIEM y mesa de ayuda).

- Servicio de Almacenamiento (IaaS Servicio de Infraestructura): Dentro de este servicio se despliegan los componentes (storage) que buscan almacenar los datos generados por el SICOV a través de servidores especializados donde estos datos quedan alojados en espacios de almacenamiento físico y/o virtual. Estos componentes reciben y almacenan la información de la capa de base de datos.

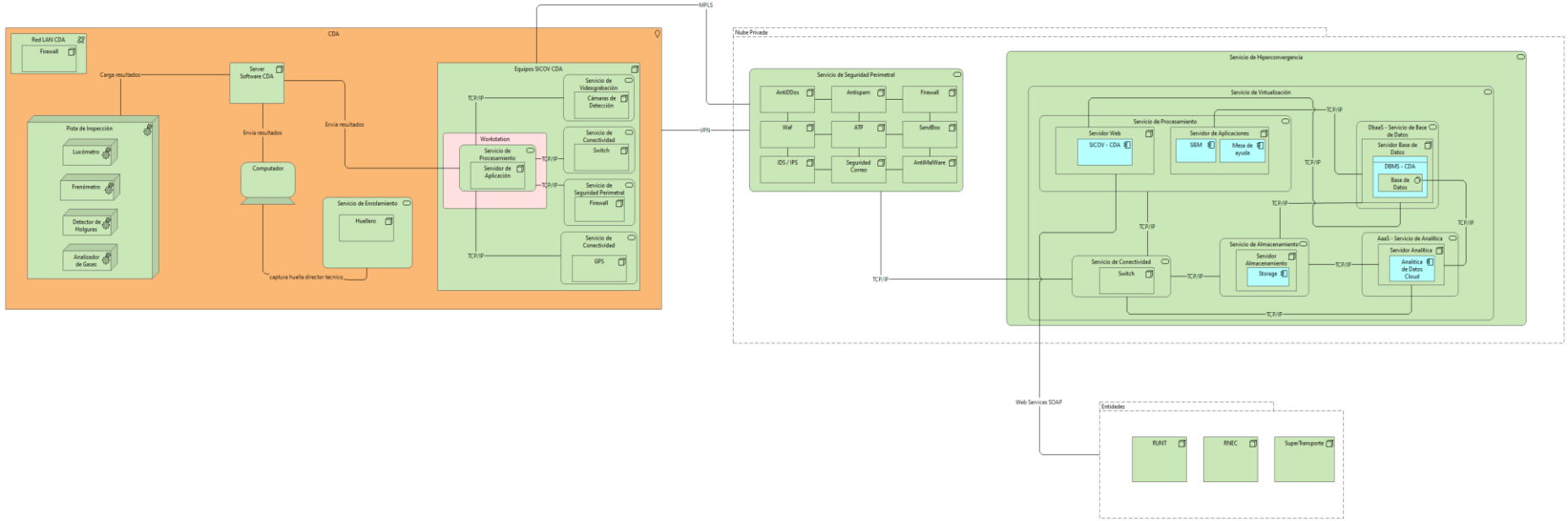
- Servicio de Analítica (AaaS): Dentro de este servicio se despliegan los componentes (analítica de datos) que permiten la gestión y el análisis de un gran volumen de datos generados dentro de la operación del SICOV y que ayudan a la toma de decisiones y al proceso de control y vigilancia. Estos componentes reciben y procesan la información procesada en las bases de datos del SICOV.

- Servicio de virtualización: Dentro de este servicio se despliegan los componentes que facilitan la creación de una forma virtual los diferentes elementos de cómputo requeridos para proveer los recursos necesarios para la operación del SICOV.

6.4.3.3 Diagrama de despliegue para los CDA

En este diagrama se pueden visualizar los diferentes componentes que hacen parte de los diferentes servicios tecnológicos enfocados como servicios en la nube de la infraestructura centralizada y su relación con la infraestructura de la operación de los CDA.

Ilustración 85. Diagrama de despliegue To Be CDA



Fuente: Elaboración propia Grow Data 2021

Desde la operación realizada desde los CDA, se realiza la conexión segura mediante una VPN a los siguientes servicios:

- Servicio de Seguridad Perimetral (IaaS Servicio de Infraestructura): Dentro de este servicio se despliegan los diferentes componentes que buscan asegurar la defensa de las redes informáticas mediante la implementación de controles especializados (WAF/ Firewall, antiDDoS, ATP, Sandbox, IDS/IPS, seguridad al correo y antimalware)en los que se establecen políticas de seguridad necesarias para la protección perimetral ante potenciales ataques internos y externos que afecten la confidencialidad, integridad y disponibilidad de los activos de información que controlan SICOV.

- Servicio de Conectividad (IaaS Servicio de Infraestructura): Dentro de este servicio se despliegan los componentes que buscan brindar la capacidad de establecer la conexión y la comunicación entre los demás componentes de infraestructura que apalancan la operación del SICOV. Se deben tener en cuenta los estándares y protocolos que ayudan a que el hardware y el software necesarios para la operación del SICOV trabajen de manera conjunta permitiendo que estos se comuniquen a través de la red informática.

- Servicio de Procesamiento (IaaS Servicio de Infraestructura): Dentro de este servicio se despliegan los componentes (servidores físicos y/o virtuales) que buscan brindar la capacidad de procesar, gestionar y difundir datos y aplicaciones relevantes para la operación del SICOV, como son el SICOV-CDA, correlacionador de eventos, software para mesa de ayuda.

- Servicio de Base de Datos (DBaaS): Dentro de este servicio se despliegan los componentes (bases de datos estructuradas y/o no estructuradas) que buscan proporcionar espacio de almacenamiento para un determinado número de base de datos permitiendo los correspondientes accesos, estas bases de datos reciben y gestionan la información de la capa de procesamiento donde se encuentran los servidores web (SICOV-CDA) y los servidores de aplicaciones (SIEM y mesa de ayuda).

- Servicio de Almacenamiento (IaaS Servicio de Infraestructura): Dentro de este servicio se despliegan los componentes (storage) que buscan almacenar los datos generados por el SICOV a través de servidores especializados donde estos datos quedan alojados en espacios de almacenamiento físico y/o virtual. Estos componentes reciben y almacenan la información de la capa de base de datos.

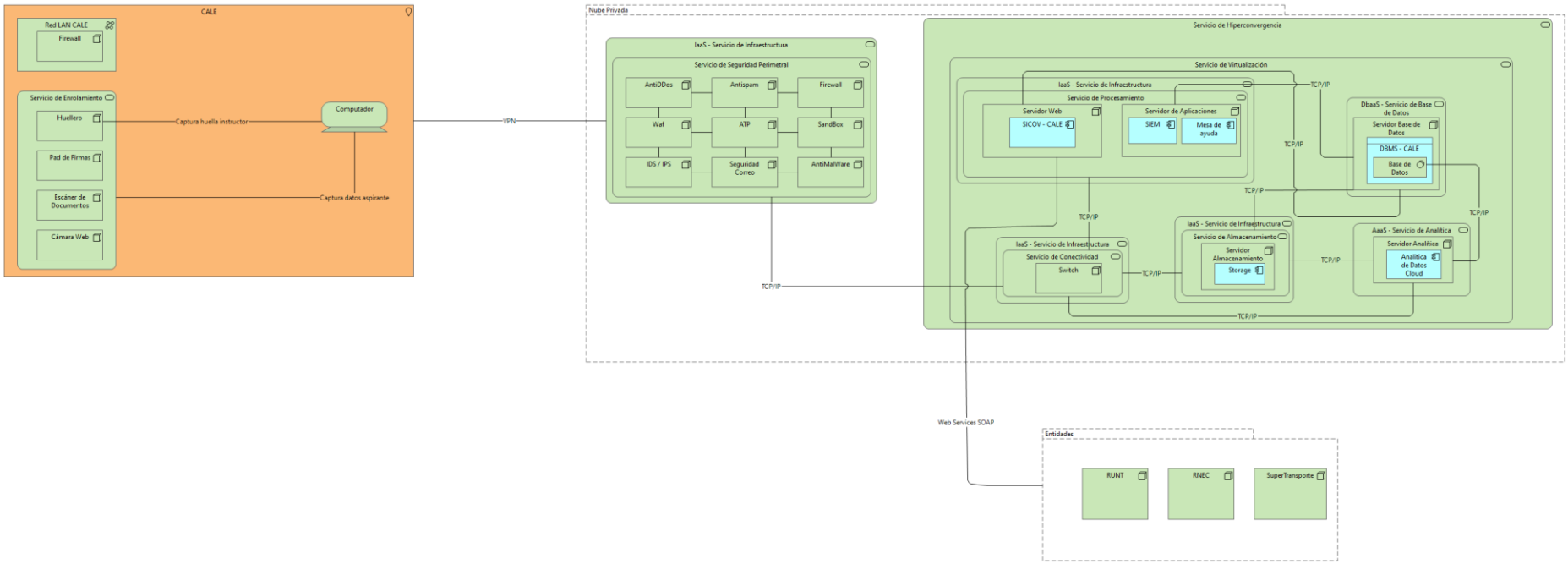
- Servicio de Analítica (AaaS): Dentro de este servicio se despliegan los componentes (analítica de datos) que permiten la gestión y el análisis de un gran volumen de datos generados dentro de la operación del SICOV y que ayudan a la toma de decisiones y al proceso de control y vigilancia. Estos componentes reciben y procesan la información procesada en las bases de datos del SICOV.

- Servicio de virtualización: Dentro de este servicio se despliegan los componentes que facilitan la creación de una forma virtual los diferentes elementos de cómputo requeridos para proveer los recursos necesarios para la operación del SICOV.

6.4.3.4 Diagrama de despliegue para los CALE

En este diagrama se pueden visualizar los diferentes componentes que hacen parte de los diferentes servicios tecnológicos desplegados y enfocados como servicios en la nube de la infraestructura centralizada y su relación con la infraestructura de la operación de los CALE.

Ilustración 86. Diagrama de despliegue To Be CALE



Fuente: Elaboración propia Grow Data 2021

Desde la operación realizada desde los CALE, se realiza la conexión segura mediante una VPN a los siguientes servicios:

- Servicio de Seguridad Perimetral (IaaS Servicio de Infraestructura): Dentro de este servicio se despliegan los diferentes Componentes que buscan asegurar la defensa de las redes informáticas mediante la implementación de controles especializados (WAF/ Firewall, antiDDoS, ATP, Sandbox, IDS/IPS, seguridad al correo y antimalware)en los que se establecen políticas de seguridad necesarias para la protección perimetral ante potenciales ataques internos y externos que afecten la confidencialidad, integridad y disponibilidad de los activos de información que controlan SICOV.

- Servicio de Conectividad (IaaS Servicio de Infraestructura): Dentro de este servicio se despliegan los componentes que buscan brindar la capacidad de establecer la conexión y la comunicación entre los demás componentes de infraestructura que apalancan la operación del SICOV. Se deben tener en cuenta los estándares y protocolos que ayudan a que el hardware y el software necesarios para la operación del SICOV trabajen de manera conjunta permitiendo que estos se comuniquen a través de la red informática.

- Servicio de Procesamiento (IaaS Servicio de Infraestructura): Dentro de este servicio se despliegan los componentes (servidores físicos y/o virtuales) que buscan brindar la capacidad de procesar, gestionar y difundir datos y aplicaciones relevantes para la operación del SICOV, como son el SICOV-CALE, correlacionador de eventos, software para mesa de ayuda.

- Servicio de Base de Datos (DBaaS): Dentro de este servicio se despliegan los componentes (bases de datos estructuradas y/o no estructuradas) que buscan proporcionar espacio de almacenamiento para un determinado número de base de datos permitiendo los correspondientes accesos, estas bases de datos reciben y gestionan la información de la capa de procesamiento donde se encuentran los servidores web (SICOV-CALE) y los servidores de aplicaciones (SIEM y mesa de ayuda).

- Servicio de Almacenamiento (IaaS Servicio de Infraestructura): Dentro de este servicio se despliegan los componentes (storage) que buscan almacenar los datos generados por el SICOV a través de servidores especializados donde estos datos quedan alojados en espacios de almacenamiento físico y/o virtual. Estos componentes reciben y almacenan la información de la capa de base de datos.

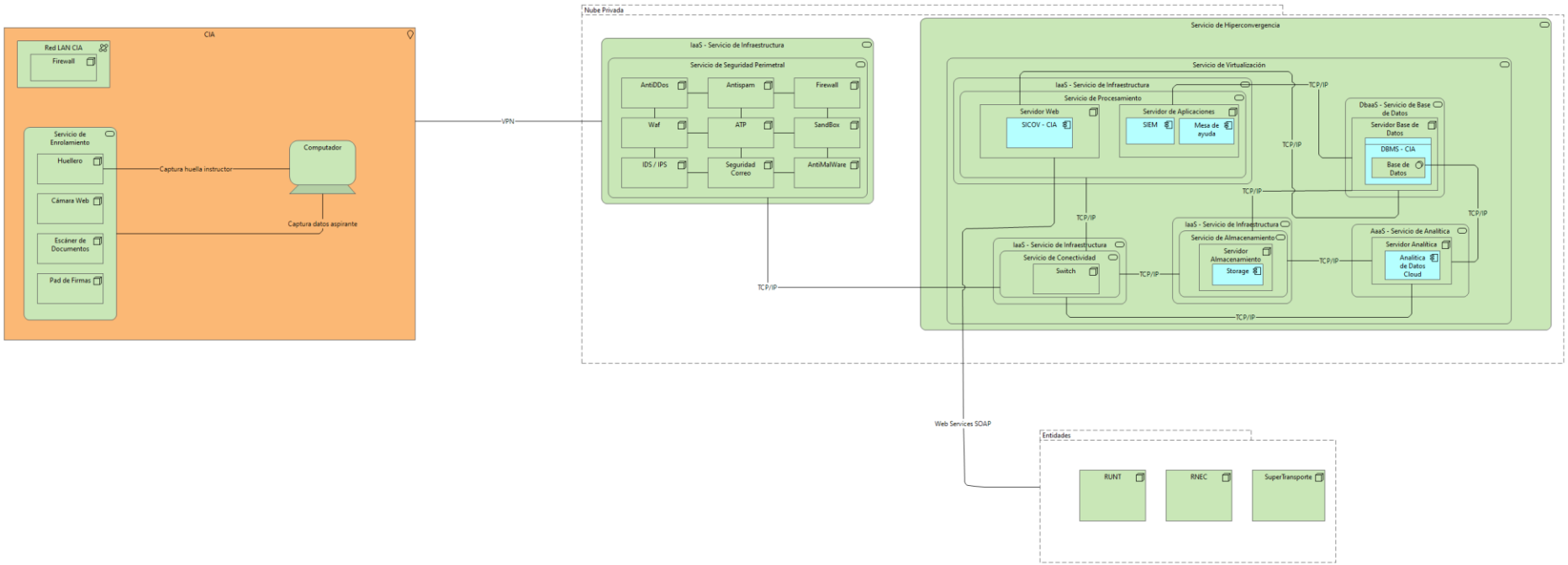
- Servicio de Analítica (AaaS): Dentro de este servicio se despliegan los componentes (analítica de datos) que permiten la gestión y el análisis de un gran volumen de datos generados dentro de la operación del SICOV y que ayudan a la toma de decisiones y al proceso de control y vigilancia. Estos componentes reciben y procesan la información procesada en las bases de datos del SICOV.

- Servicio de virtualización: Dentro de este servicio se despliegan los componentes que facilitan la creación de una forma virtual los diferentes elementos de cómputo requeridos para proveer los recursos necesarios para la operación del SICOV.

6.4.3.5 Diagrama de despliegue para los CIA

En este diagrama se pueden visualizar los diferentes componentes que hacen parte de los diferentes servicios tecnológicos enfocados y desplegados como servicios en la nube de la infraestructura centralizada y su relación con la infraestructura de la operación de los CIA.

Ilustración 87. Diagrama de despliegue To Be CIA



Fuente: Elaboración propia Grow Data 2021

Desde la operación realizada desde los CIA, se realiza la conexión segura mediante una VPN a los siguientes servicios:

- Servicio de Seguridad Perimetral (IaaS Servicio de Infraestructura): Dentro de este servicio se despliegan los diferentes componentes que buscan asegurar la defensa de las redes informáticas mediante la implementación de controles especializados (WAF/ firewall, antiDDoS, ATP, Sandbox, IDS/IPS, seguridad al correo y antimalware)en los que se establecen políticas de seguridad necesarias para la protección perimetral ante potenciales ataques internos y externos que afecten la confidencialidad, integridad y disponibilidad de los activos de información que controlan SICOV.

- Servicio de Conectividad (IaaS Servicio de Infraestructura): Dentro de este servicio se despliegan los componentes que buscan brindar la capacidad de establecer la conexión y la comunicación entre los demás componentes de infraestructura que apalancan la operación del SICOV. Se deben tener en cuenta los estándares y protocolos de comunicación TCP/IP y HTTPS que ayudan a que el hardware y el software necesarios para la operación del SICOV trabajen de manera conjunta permitiendo que estos se comuniquen a través de la red informática.

- Servicio de Procesamiento (IaaS Servicio de Infraestructura): Dentro de este servicio se despliegan los componentes (servidores físicos y/o virtuales) que buscan brindar la capacidad de procesar, gestionar y difundir datos y aplicaciones relevantes para la operación del SICOV, como son el SICOV-CIA, correlacionador de eventos, software para mesa de ayuda.

- Servicio de Base de Datos (DBaaS): Dentro de este servicio se despliegan los componentes (bases de datos estructuradas y/o no estructuradas) que buscan proporcionar espacio de almacenamiento para un determinado número de base de datos permitiendo los correspondientes accesos, estas bases de datos reciben y gestionan la información de la capa de procesamiento donde se encuentran los servidores web (SICOV-CIA) y los servidores de aplicaciones (SIEM y mesa de ayuda).

- Servicio de Almacenamiento (IaaS Servicio de Infraestructura): Dentro de este servicio se despliegan los componentes (storage) que buscan almacenar los datos generados por el SICOV a través de servidores especializados donde estos datos quedan alojados en espacios de almacenamiento físico y/o virtual. Estos componentes reciben y almacenan la información de la capa de base de datos.

- Servicio de Analítica (AaaS): Dentro de este servicio se despliegan los componentes (analítica de datos) que permiten la gestión y el análisis de un gran volumen de datos generados dentro de la operación del SICOV y que ayudan a la toma de decisiones y al proceso de control y vigilancia. Estos componentes reciben y procesan la información procesada en las bases de datos del SICOV.

- Servicio de virtualización: Dentro de este servicio se despliegan los componentes que facilitan la creación de una forma virtual los diferentes elementos de cómputo requeridos para proveer los recursos necesarios para la operación del SICOV.

6.4.4 Protocolos y Estándares

En este capítulo se relacionan los diferentes protocolos y estándares que se deben tener en consideración para gestionar de una manera más técnica y estructurada cada uno de los servicios tecnológicos propuestos en la arquitectura de solución.

6.4.4.1 Protocolos

En la actualidad existen diferentes tipos de protocolos de internet, los cuales establecen condiciones distintas al momento de asegurar la información que se desea transmitir. A continuación, se enlistan estos protocolos.

- TCP/IP: El principal conjunto de protocolos de red que se utilizan para este propósito es el protocolo de control de transmisión (TCP/IP). Este protocolo está orientado a la conexión en la capa de transporte, el cual asegura la conexión entre el nodo origen y el nodo destino antes de transferir la información.

- HTTPS: Este es un protocolo que protege la integridad y la confidencialidad de la información de los usuarios entre los computadores de los OAT y el sitio web del SICOV.

- SSH: Este protocolo proporciona una manera segura de autenticación y encriptación entre dos computadoras que se conectan a internet, por medio de un canal seguro en el que toda la información se encuentra cifrada.

- VPN: Este protocolo permite establecer conexiones seguras con alto desempeño interconectando redes y dispositivos de manera segura a través de internet, encriptando el tráfico para ocultar los datos que se están transmitiendo.

- SOAP: Este protocolo estándar define la comunicación entre dos nodos que se encuentran en diferentes procesos por medio de intercambio de datos XML.

6.4.4.2 Estándares y mejores prácticas

Existen un conjunto de reglas establecidas y aprobadas por organismos reconocidos que buscan unificar los procesos, procedimientos y/o políticas que se deben tener en cuenta en la operación del nuevo SICOV. A continuación, se enlistan estos estándares y mejores prácticas que debe ser aplicadas e implementadas en el nuevo SICOV.

- ISO 22301 / 2019: Versión de la norma internacional para sistemas de gestión de continuidad de negocio, el cual proporciona un marco de referencia de buenas prácticas que ayuda a las organizaciones a gestionar de una manera más eficiente los posibles impactos de una interrupción sobre la operación.

- ISO 27001 / 2013: Versión de la norma internacional la cual proporciona un marco de trabajo para los sistemas de gestión de seguridad de la información con el fin de proporcionar confidencialidad, integridad y disponibilidad continuada de la información, incluyendo el cumplimiento legal.

- ISO 31000 / 2018: Versión de la norma internacional la cual proporciona las directrices para gestionar los diferentes riesgos que pueden afectar la infraestructura tecnológica que apalanca al SICOV.

- ISO 9001 / 2015: Versión de la norma internacional la cual proporciona los requisitos y objetivos para mejorar la eficiencia de los procesos enfocados en la gestión de la infraestructura tecnológica, mejorando las medidas de seguridad y control para reducir los riesgos asociados a la pérdida o robo de información generada en la operación del SICOV.

- ISO 38500 / 2015: Versión de la norma internacional la cual proporciona las directrices sobre el uso eficaz, eficiente y aceptable de la tecnología de la información (TI), incluyendo los procesos de gestión y las decisiones relacionadas con el uso actual y futuro de TI.

- ISO 20000-1: Versión de la norma internacional la cual proporciona las directrices para la gestión de servicios TI de forma metódica a través de la implementación del PHVA (planear, hacer, verificar, actuar), demostrando la capacidad de gestionar los servicios de TI de forma eficiente y efectiva.

- COBIT 2019: Conjunto de herramientas orientadas a garantizar el control y seguimiento de gobernabilidad de Sistemas de Información a largo plazo a través de auditorías, agrupados en cuatro dominios (planificación y organización – adquisición e implementación – entrega y soporte – monitoreo).

- ITIL V4: Marco de trabajo enfocado en la administración de servicios de TI, buscando garantizar un sistema flexible, coordinado e integrado para el gobierno y la gestión efectiva de los servicios habilitados para TI.

- Lenguaje Común de Intercambio (X-Road): Estándar nacional definido y administrado por el Ministerio de Tecnologías de la Información y las Comunicaciones que facilita el intercambio de información entre las entidades públicas con el propósito de mejorar los servicios digitales dirigidos a los ciudadanos y empresas, fortaleciendo los procesos de interoperabilidad y la eficiencia del Estado.

6.5 Arquitectura de seguridad

Las siguientes son las vistas de arquitectura donde se consolida el estado propuesto de la arquitectura de seguridad de SICOV. La presentación de las vistas se realiza de tal forma que se inicie de lo más general a lo más específico. Es importante aclarar que la arquitectura puede requerir cambios a futuro, por lo tanto, se recomienda que se adopte para SICOV y se actualice constantemente según se requiera.

Estado Objetivo (TO-BE)
La arquitectura de seguridad y Privacidad de la información en la Entidad se centra en el cumplimiento de estándares internacionales que se adapten a las necesidades y requerimiento de los procesos. Estos estándares son: ISO/IEC 27001:2013, ISO/IEC 27002:2013, ISO 27017, ISO 27033 e ISO 27035 las cuales contiene requisitos y controles de seguridad y privacidad de la información, bajo un enfoque de mejora continua, buscando el establecimiento, implementación, mantenimiento y mejora de un Sistema de Gestión de Seguridad de la Información – SGSI. Igualmente, se realiza la equivalencia de los controles respecto a lo planteado en el Marco de Arquitectura Empresarial de MinTIC, desde los 6 lineamientos establecidos para la Arquitectura en Seguridad.

A continuación, se describe Los diagramas o vistas enmarcadas en lograr un nivel de madurez óptimo a nivel de arquitectura de seguridad.

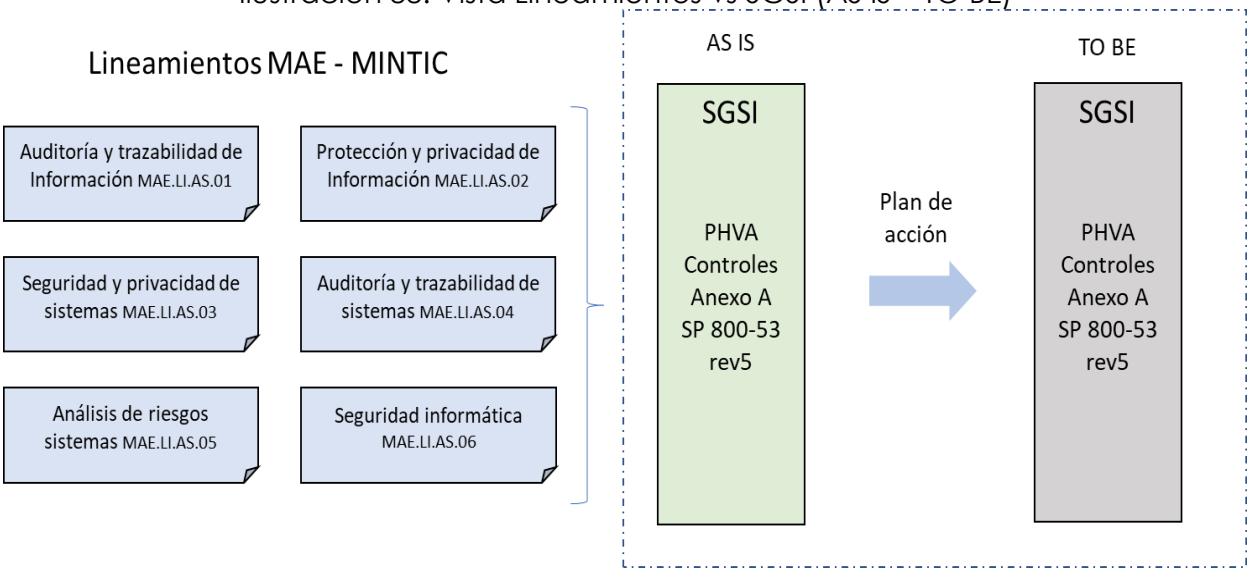
6.5.1 Protocolos, estándares y mejores prácticas

6.5.1.1 Lineamientos de Seguridad de la Información

El primer enfoque, se define de acuerdo con los lineamientos de seguridad de la información del Marco de Arquitectura Empresarial de MinTIC, que contienen la auditoría y trazabilidad de los sistemas e información, seguridad y privacidad de los sistemas e información, la gestión de riesgos y finalmente los controles de seguridad informática.

Lo anterior, puede ser cubierto desde un enfoque de un Sistema de Gestión de Seguridad de la Información – SGSI, que contiene una serie de requisitos (numeral 4 al 10 norma ISO 27001:2013) y controles de seguridad de la información (Anexo A norma ISO 27001:2013). Por lo tanto, se realiza la equivalencia a nivel de controles y requisitos entre los lineamientos de seguridad de MAE de MinTIC y el SGSI. Finalmente, desde la arquitectura de seguridad, se realiza la revisión del estado actual (AS IS), se define un estado futuro (TO BE) y las brechas (Plan de acción) que permitirán lograr ese estado ideal.

Ilustración 88. Vista Lineamientos vs SGSI (AS IS – TO BE)



Fuente: Elaboración propia Grow Data 2021

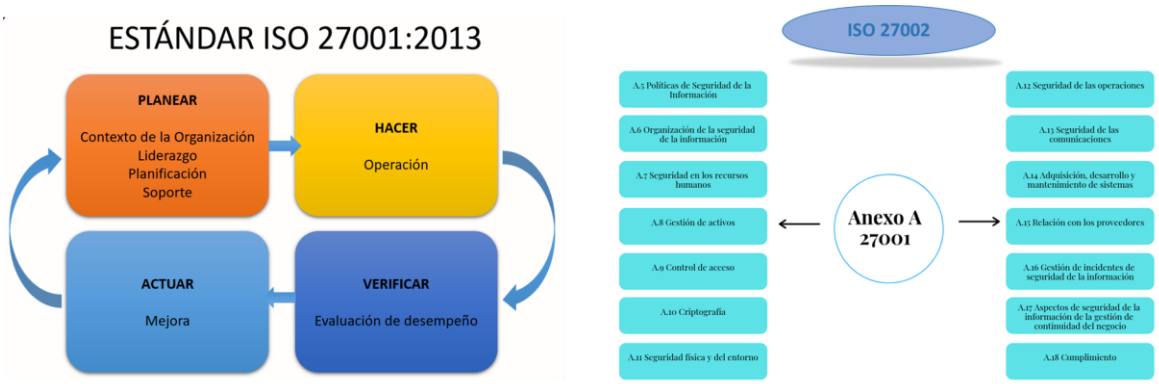
6.5.1.2 Estándares aplicables

En lo referente a estándares, la arquitectura de seguridad se soporta en un conjunto de buenas prácticas establecidas y aprobadas por organismos reconocidos (internacionales) que buscan es establecimiento de sistemas de gestión de seguridad y controles técnicos para la protección de la confidencialidad, integridad y disponibilidad de los activos de información que son parte fundamental en la operación del nuevo SICOV. A continuación, se enlistan estos estándares.

- ISO/IEC 27001:2013 Norma técnica colombiana - tecnología de la información. Técnicas de seguridad. Sistemas de gestión de la seguridad de la información (SGSI). Versión de la norma internacional la cual proporciona las definiciones y requisitos para los sistemas de gestión de seguridad de la información con el fin de proporcionar confidencialidad, integridad y disponibilidad continuada de la información, incluyendo el cumplimiento legal.

- ISO/IEC 27002:2013 Código de buenas prácticas para controles de seguridad de la información. Versión de la norma internacional que proporciona un código de buenas prácticas para los controles de seguridad de la información relacionados en el Anexo A de la norma ISO/IEC 27001:2013.

Ilustración 89. Estándares aplicables en seguridad de la información



Fuente: Elaboración propia Grow Data 2021

- ISO/IEC 27017:2015 Controles de seguridad para servicios Cloud. Versión de la norma internacional que proporciona controles para proveedores y clientes de servicios en la nube. Aclara las funciones y responsabilidades de ambas partes (Cliente-Proveedor) para ayudar a que los servicios en la nube sean tan seguros como el resto de los datos incluidos en un SGSI.

- ISO/IEC 27033:2014 Guía detallada de seguridad de la administración, operación y uso de las redes. Corresponde a una serie de normas internacionales que proporcionan una guía detallada sobre la implementación de los controles de seguridad de red que se describen de manera general en la norma ISO/IEC 27002. Contiene de manera general la descripción de directrices sobre la seguridad entre redes (pasarelas, cortafuegos, sistemas de protección contra intrusos). Así mismo, incluye la identificación y análisis de las amenazas a la seguridad de la red, definición de requisitos de control de la seguridad y el diseño, aplicación, funcionamiento y supervisión de los controles

- ISO/IEC 27035-1:2016 Gestión de incidentes de seguridad de la información. Versión de la norma que contiene los conceptos básicos y fases de la gestión de incidentes de seguridad de la información y combina estos conceptos con principios en un enfoque estructurado para detectar, informar, evaluar y responder a incidentes de seguridad de la información y aplicar las lecciones aprendidas.

6.5.1.3 Protocolos:

En la actualidad existen diferentes tipos de protocolos de seguridad, los cuales aseguran un nivel de protección mayor en confidencialidad, integridad y disponibilidad de la información. A continuación, se enlistan estos protocolos.

- SSH: Este protocolo proporciona una manera segura de autenticación y encriptación entre dos computadoras que se comunican a internet, por medio de un canal seguro en el que toda la información se encuentra cifrada.

- VPN: Este protocolo establece una conexión segura permite establecer conexiones seguras con alto desempeño interconectando redes y dispositivos de manera segura a través de internet, encriptando el tráfico para proteger los datos que se están transmitiendo a través de estas redes.

- HTTPS: Este protocolo establece una conexión segura protegiendo la integridad y la confidencialidad de la información de los usuarios entre los equipos de cómputo de los OAT y el sitio web del SICOV. Los servidores Web deben únicamente permite el uso de TLS 1.2 y TLS 1.3 (Transport Layer Security). Adicional, SSL 3 y SSL 2 deberán estar deshabilitados.

- Certificados digitales: Corresponde a un formato estándar con una estructura de datos que contiene información sobre un sitio web, individuo u organización (por ejemplo, una clave pública, una identidad o un conjunto de privilegios), firmada por otra entidad, considerada por un grupo de otras entidades como una autoridad para este tipo de contenido. Entre los formatos de mayor relevancia se encuentran: X.509, SPKI, PGP, SAML.

- Cifrado simétrico AES 192/256 bits: Corresponde a un esquema de cifrado en bloques con una alta seguridad en la actualidad. Se debe implementar AES 192 o AES 256 bits para ofrecer una seguridad optima y poco probable de ataque para el cifrado de la información en reposo.

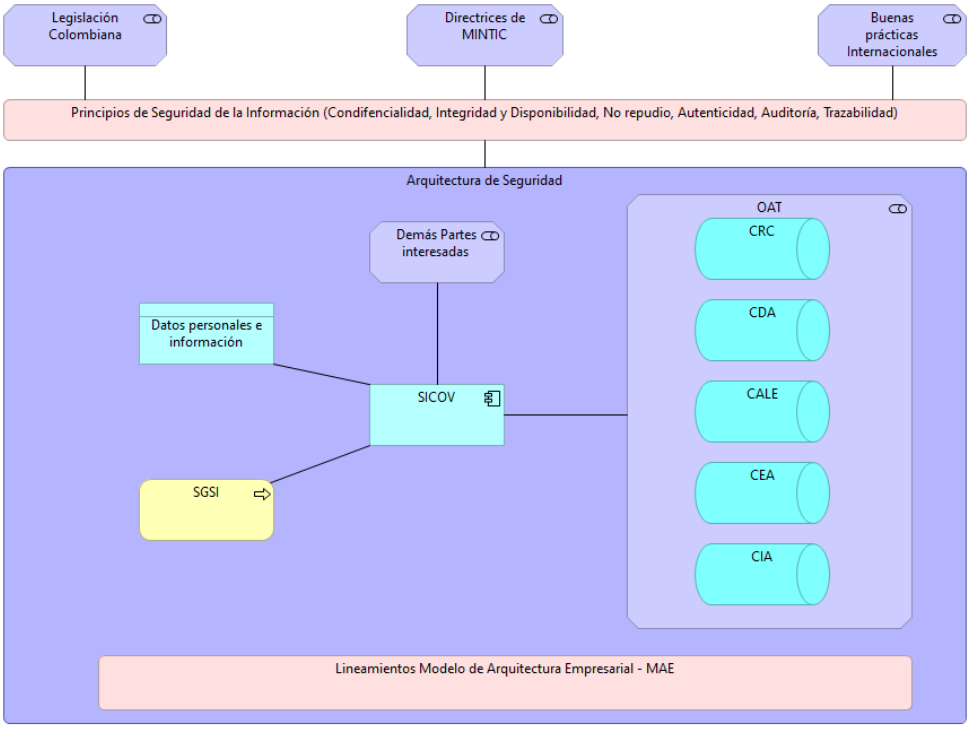
- Cifrado asimétrico RSA 2048 bits o superior: Corresponde a un sistema criptográfico de clave pública, que utiliza factorización de números enteros. Por ser uno de los más utilizados se recomienda su implementación en 2048 bits, siendo válido tanto para cifrar como para firmar digitalmente.

6.5.2 Arquitectura Conceptual

Esta vista permite identificar las entradas de la arquitectura, dentro de las cuales contempla: La legislación colombiana en materia de seguridad de la información, las directrices de MinTIC, quien regula la seguridad y privacidad en materia de sector Gobierno y los principios de la arquitectura, que se enmarcan en los principios de seguridad de la información que han sido adoptados como buenas prácticas internacionales.

Así mismo, la siguiente ilustración presenta alto nivel la arquitectura de seguridad desde un enfoque de protección a los datos personales e información en general de SICOV, enmarcados en un proceso de mejora continua (SGSI), esto para SICOV, que prestará los servicios a los diferentes OATs y demás partes interesadas. Igualmente, se tiene como base los lineamientos del Modelo de Arquitectura Empresarial (MAE), en lo que respecta a los lineamientos del dominio de Arquitectura de Seguridad, esto alineado con los controles de seguridad de la información del SGSI.

Ilustración 90. Vista Arquitectura General Seguridad – SICOV



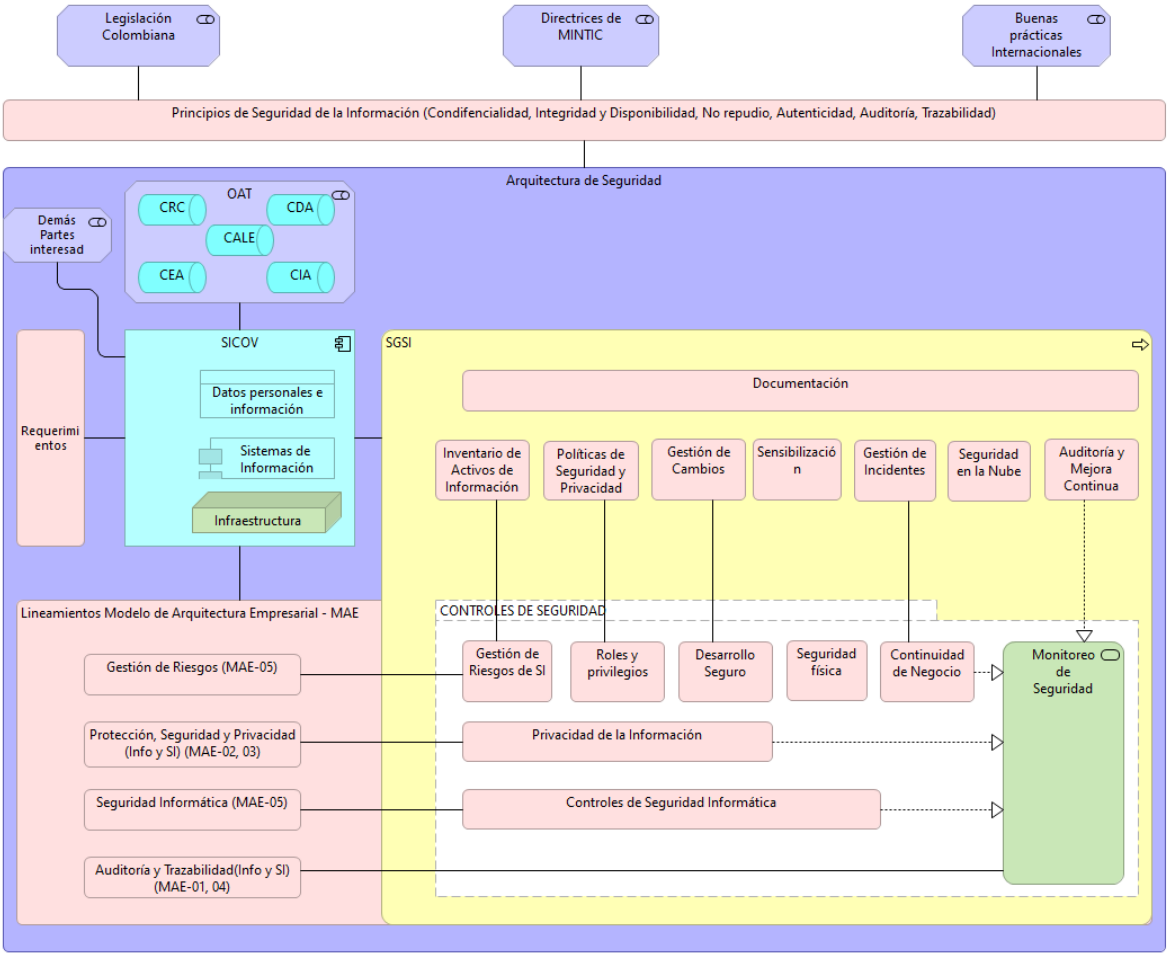
Fuente: Elaboración propia Grow Data 2021

6.5.3 Controles de Seguridad

En esta vista se tiene un acercamiento a tres (3) puntos específicos: los aspectos del SGSI, los lineamientos del MAE y la intersección que tienen estos dos bloques, el cual resulta en un bloque (de color amarillo) con los controles de seguridad que se aplican sobre SICOV. Estos controles de la intersección se encuentran alineados tanto con el bloque de lineamientos del MAE como con los aspectos de seguridad del SGSI y los demás estándares de seguridad (Cloud, Privacidad, Incidentes).

A continuación, se presenta la vista de arquitectura de controles.

Ilustración 91. Vista Arquitectura Seguridad – Controles - SICOV



Fuente: Elaboración propia Grow Data 2021

En la parte superior izquierda, encontramos las entradas y requerimientos de SICOV, así como las partes interesadas del SGSI, con el elemento adicional de que el sistema contiene información, aplicaciones y una infraestructura que lo soporta.

En la parte superior derecha, se encuentra la documentación, como eje principal que se lidera desde la Alta Dirección para una correcta planeación del sistema y en general de los controles que contiene (Políticas, procedimientos, metodologías, matrices, manuales, entre otros). Así mismo, se cuenta con las bases fundamentales del SGSI, entre ellos lo que permiten brindar la protección y mantenimiento de la confidencialidad, Integridad y Disponibilidad de los activos de información.

Finalmente, se establece los requisitos de un SGSI y los lineamientos de arquitectura de seguridad del MAE de MinTIC. La gestión de riesgos de los activos de información como columna vertebral de una SGSI, y en este caso de la seguridad del SICOV. De otra parte, se establece controles para la gestión de roles, desarrollo seguro, seguridad a nivel físico, nube (Cloud) y continuidad de negocio sobre los activos de información, buscando avanzar a un enfoque de privacidad de los datos; todo enmarcado en un monitoreo de la gestión de seguridad para lograr una protección y la mejora continua.

Se anexa catálogo de controles de seguridad TO-BE que consolida las salvaguardas alienadas con las normas ISO 27001, ISO 27002, ISO 27017 entre otras.

6.5.4 Arquitectura Objetivo

La arquitectura objetivo del dominio de seguridad recopila los conceptos aquí desarrollados. A un alto nivel se parte de la arquitectura conceptual TO-BE como estructura base para el desarrollo de la arquitectura objetivo

Esta vista permite visualizar contenido detallado que aborda cada uno de los aspectos de seguridad del SGSI y de su intersección (controles) con los lineamientos del MAE para el SICOV. Permite identificar claramente los aspectos de seguridad desde un enfoque de los diferentes niveles de seguridad. Con la claridad del enfoque de la arquitectura de seguridad planteada para SICOV de la vista general y la vista global de controles, se tiene establecido en la parte superior la gestión de activos de información (datos e información, aplicaciones, software, seguridad perimetral, infraestructura, recurso humano, infraestructura física), seguidamente todo el soporte documental desde el proceso estratégico o la Alta Dirección. Esto comprende:

- Planeación estratégica de seguridad de la información PESI
- Plan de tratamiento de riesgos en seguridad
- Plan de capacitación y sensibilización en seguridad
- Plan de Continuidad de Negocio
- Plan de recuperación de desastres

Un nivel más abajo, se define los pilares o bases fundamentales para la gestión de seguridad de la información, entre ellos se tiene:

- Políticas de seguridad de la información, como máxima directriz gerencial.
- Gestión de cambios: Este proceso permite mantener la seguridad de la información ante actualizaciones, mejoras o modificaciones en SICOV.
- Seguridad en la Nube: controles de seguridad que se requieren para proteger la confidencialidad, integridad y disponibilidad en una infraestructura Cloud de SICOV, entre los cuales se debe definir: Acuerdos de niveles de servicios con los proveedores, gestión de accesos, acuerdos contractuales, cumplimiento de normatividad nacional e internacional, controles de seguridad a nivel de aplicaciones e infraestructura, entre otros.
- Gestión de incidentes: para mantener un permanente monitoreo y control de la seguridad se sugiere integraciones con herramientas SIEM, procesos de monitoreo y atención mediante un SOC, integración con la gestión de continuidad de negocio, para saber en qué momento se debe activar o

no un plan de contingencia tecnológica y en caso de investigación interna o con entes de control, tener un proceso de análisis forense

- Sensibilizaciones de la seguridad (gestión de activos, gestión de incidentes, gestión de riesgos, entre otros) de SICOV a las partes interesadas, para generar confianza y así mejorar el uso y apropiación del sistema de una manera segura.
- Finalmente, un proceso de auditoría y mejora continua mediante la planeación y ejecución de revisión internas y externas para evidenciar la conformidad y mejora de los controles.

En el eje central donde se cruzan los controles del SGSI con los lineamientos MAE de MinTIC, se encuentra el detalle de controles y documentos finales o productos que se derivan de la seguridad de la información aplicada. En la parte superior derecha de los controles de seguridad, se evidencia la gestión de riesgos de seguridad aplicado a los activos de información de acuerdo con su criticidad, la cual contiene la matriz de riesgos y los indicadores a nivel de riesgos y de implementación de plan de tratamiento de riesgos. Seguidamente, la gestión de roles, donde se encuentra las matrices de roles y responsabilidades (control A.6.1.1 y A.6.1.2), adicionalmente, se puede establecer controles más avanzados y centralizados como los es la gestión de identidades y de usuarios privilegiados, siendo un componente fundamental es la gestión de usuarios seguros. En el lado derecho, se encuentra la seguridad a nivel de desarrollo, donde se plantea la definición y aplicación de metodologías de desarrollo seguro para SICOV, junto con una adecuada separación de ambientes (Desarrollo, pruebas, QA y producción). Finalmente, una revisión constante de código seguro, para proteger una de las ultimas fronteras que permiten el acceso a la información o datos de SICOV desde la aplicación.

Seguidamente, se tiene la gestión de continuidad de negocio, que viene como componente clave para mantener la operatividad tecnológica y de negocio de SICOV, por ello comprende el establecimiento de estrategias para la alta disponibilidad de los activos de información de SICOV, análisis de impacto para el entendimiento y definición de al menos los tiempos objetivos de respuesta y punto objetivos de restauración; y finalmente la definición, implementación y prueba de estrategias de recuperación de desastres y continuidad de negocio para lograr la mejora continua.

En un nivel inferior, se presentan los diferentes tipos de seguridad para la alineación con las arquitecturas de información y datos, aplicaciones e infraestructura. Por ello, desde la arquitectura de seguridad se plantea los siguientes niveles en seguridad:

- Seguridad física
- Seguridad de redes y comunicaciones

- Seguridad de las aplicaciones
- Seguridad de la información - datos

6.5.4.1 Seguridad física:

En la protección física, la arquitectura de seguridad contiene los controles que cubren el Dominio A.11 de la norma ISO 27001:2013, entre ellos se encuentra la seguridad del perímetro, controles de acceso físico mediante biometría, seguridad en los recintos mediante controles de CCTV, seguridad física en el cableado estructurado, amenazas ambientales y la definición y protección de áreas seguras.

6.5.4.2 Seguridad de redes y comunicaciones:

Para la seguridad a nivel de infraestructura tecnológica de SICOV se plantea controles que brinden la protección de la confidencialidad, integridad y disponibilidad de la aplicación e información. La arquitectura propuesta, a nivel de seguridad en redes y equipos finales busca el aseguramiento a través de:

- Fortalecimiento en el monitoreo del tráfico de red para un seguimiento y atención a eventos e incidentes de seguridad.
- Implementación de ATP (Protección avanzada contra amenazas) en la arquitectura para la detección y contención de ATP, ZeroDay, entre otros.
    - Detección temprana
    - Protección adecuada
    - Respuesta eficaz
- Control 360 Endpoint
- Perfil de protección de equipos finales. (Hardening al equipo final)
- Comunicaciones seguras con la infraestructura Cloud.

Entre los controles que conforman la seguridad de redes y comunicaciones se tienen:

- **VPN**: Mediante la aplicación de tecnología de conectividad se establece la conexión segura entre los administradores y la infraestructura tecnológica de SICOV en la Nube o la del proveedor que la contenga.
- **AntiDDoS**: Ante los inminentes ataques de Denegación de servicio distribuidos, se requiere tener salvaguardas que revisen y filtren el tráfico legítimo del tráfico atacante, es decir que solo se procese el flujo de trabajo habitual mientras que las peticiones basura del ciberdelincuente no alcancen al sistema.
- **WAF:** Permite la protección de múltiples ataques a nivel de aplicaciones web en el backend. Este tipo de control busca reducir las amenazas y potenciales

incidentes de seguridad a nivel Web, mediante el análisis de paquetes de petición HTTP / HTTPS y modelos de tráfico.

- **SandBox:** En caso de tener potencial código malicioso se requiere controles que permitan disponer de un entorno aislado del resto del sistema operativo. Un SanBox comprende la ejecución de programas de manera controlada mediante asignación de espacio en disco y memoria, ejecución en un sistema de archivos temporal, entre otras características para evaluar y definir el potencial de daño que puede generar un programa o archivo al momento de su ejecución.
- **Control 360 EndPoint:** Protección en el equipo final de usuario, para controlar la gestión de manera remota de los equipos de cómputo y en general de los dispositivos que estarán conectados al SICOV. Permite una protección adicional de entrada de malware a través de dispositivos externos, a la vez que permite aumentar la productividad evitando el uso ineficiente de los mismos.
- **Seguridad del correo**: Establecer las reglas y configuración de seguridad en el servicio de correo electrónico que estará integrado con SICOV. Mediante una adecuada configuración y parametrización, se establece un nivel de seguridad óptimo para brindar protección a nivel de SPAM, revisión de malware, suplantación de dominio y cuentas, entre otros controles a nivel de correo.
- **AntiMalware**: Con la implementación de un antimalware en los servidores y equipos que hacen parte de SICOV se previene, detecta y controla y remedia programas maliciosos.
- **IDS/IPS**: Implementación y mejora de sistemas de detección y prevención de intrusos sobre la infraestructura que soporta SICOV. Se establecen reglas y mediante un aprendizaje automatizad, se brinda un nivel de seguridad en la red.
- **Protección Avanzada de Amenazas – ATP:** Implementación de un ATP para la identificación, detección e investigación de amenazas avanzadas a nivel informático, accesos peligrosos y acciones malintencionadas dirigidas hacia el SICOV, realizadas por usuarios internos o externos.

6.5.4.3 Seguridad de las aplicaciones:

A nivel de aplicaciones, se plantea controles enfocados a la criptografía para una gestión de llaves segura, dando cumplimiento al control A.10.1.2 de la norma ISO 27001:2013. Así mismo, el uso seguro de certificados digitales en el sistema y la aplicación de controles parala ofuscación de código, cuando se considere necesaria, protegiendo la lógica del sistema ante ataques avanzados a nivel de código.

6.5.4.4 Seguridad de la información – Datos:

La seguridad de los datos corresponde al último anillo de seguridad planteado en la arquitectura de seguridad. Para ello, se sugiere desde la arquitectura, controles

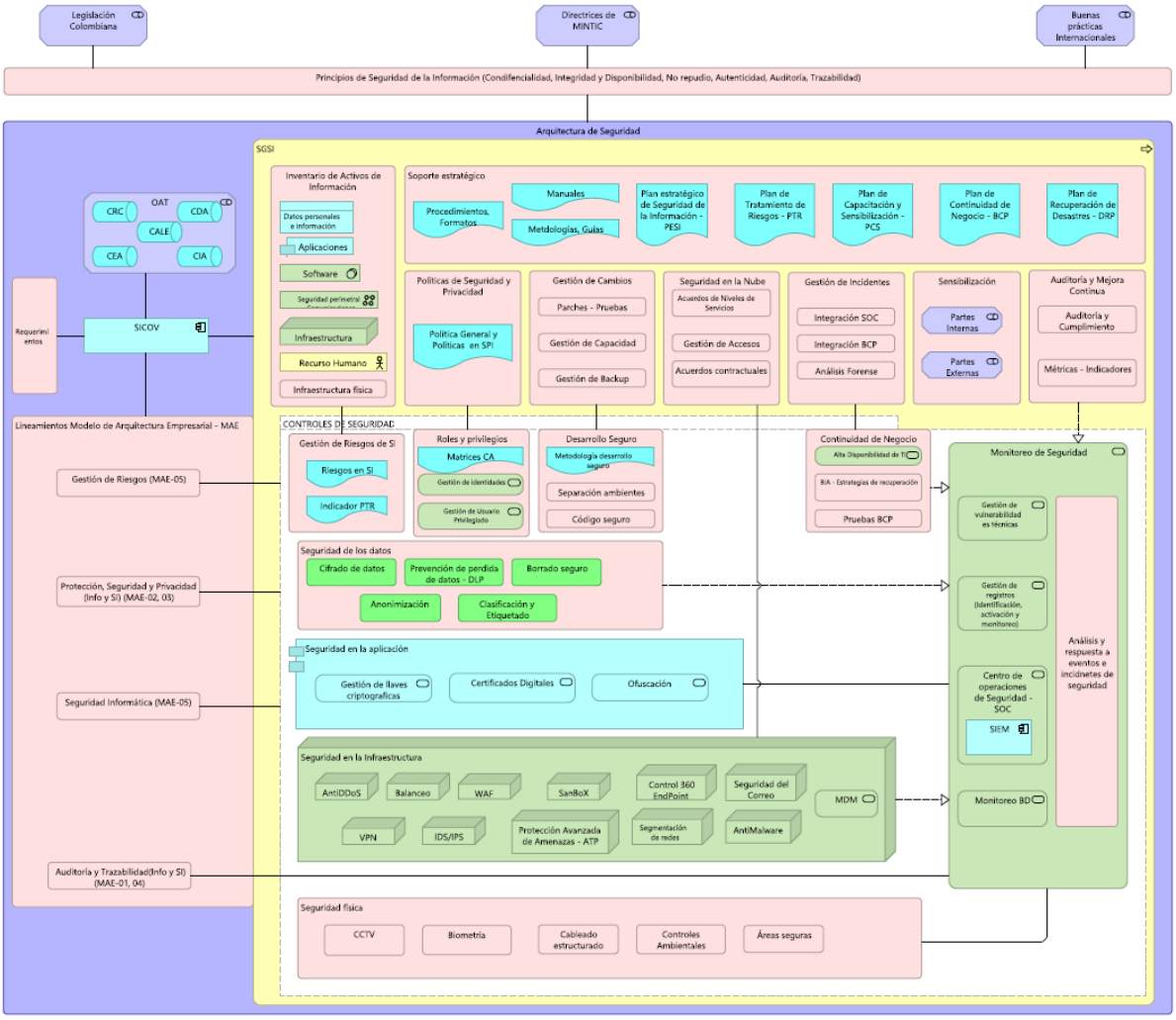
enfocados a la proteger la confidencialidad e integridad de estos. Entre los controles propuestos se tiene:

- Clasificación y etiquetado de la información, esto para conocer el nivel de criticidad o sensibilidad de la información que se tiene.
- Cifrado de los datos, esto a nivel de datos en reposo, de acuerdo con los niveles de clasificación de la información.
- Aplicación de controles de borrado seguro, para datos que no se encuentren en uso o requerían ser eliminados de forma segura por estar en un ambiente diferente al productivo.
- A nivel de controles con un enfoque más a la privacidad se plantea la anonimización de datos, evitando la identificación de los usuarios y reducir su probabilidad de reidentificación sin afectar la veracidad de los resultados y la utilidad de los datos que han sido tratados.

Finalmente, y para lograr la evaluación y mejora continua en seguridad de la información, la arquitectura planeta un proceso transversal de monitoreo que comprende:

- Gestión de vulnerabilidades, de modo que se tenga un constante proceso en la identificación, análisis y cierre de vulnerabilidades técnicas, aplicando procedimientos de gestión de parches, pruebas de seguridad informática, gestión de cambios, logrando una mejora en la seguridad de manera permanente.
- Gestión de registros, para identificar lo que se requiere generar y capturar a nivel de logs. Así mismo, realizar el monitoreo mediante herramientas como un SIEM (Security Incident Events Managment).
- Centro de Operación de Seguridad – SOC, para brindar supervisión y administración de la seguridad del SICOV a través de herramientas de captura, envío, correlación y presentación de eventos e intervención remota.
- Monitore de Base de Datos.

Ilustración 92. Vista Arquitectura Seguridad – Detallada - SICOV



Fuente: Elaboración propia Grow Data 2021

Finalmente, la arquitectura objetivo cubre los controles actualmente implementados y gestionados en los homologados, como controles nuevos; todos enmarcados en la búsqueda de lograr un enfoque integral de la seguridad de la información para SICOV. Se plantean aspectos de seguridad para dar cumplimiento con los requisitos gubernamentales (MinTIC, SIC, entre otros), así como el cumplimiento de estándares internacionales en materia de seguridad de la información (ISO 270001, ISO 27002, ISO 27017, ISO 27035, entre otras).

7 Anexos

- **Arquitectura de Negocio**
  - Controles_Dominios
  - Controles_Listado de Chequeo Requerimientos y Verificación -SICOV-CDA
  - Controles_Listado de Chequeo Requerimientos y Verificación SICOV-CEAS-CIAS
  - Controles_Listado de Chequeo Requerimientos y Verificación SICOV-CRCs
- **Arquitectura de Sistemas de Información**
  - Arq.Sist.Inf Catálogo de aplicativos SICOV
  - Arq.Sist.Inf Catálogo de servicios de intercambio de información
- **Arquitectura de Datos**
  - Arq.Datos_Catálogo_Dominios_AsIs
  - Arq.Datos_Catálogo_Entidades_Datos_AsIs
  - Arq.Datos_Matriz_Entidades_Datos-Proceso_AsIs
  - Arq.Datos_Matriz_Entidades_Datos-Aplicaciones_AsIs
  - Arq.Datos_Flujo_Información_CRC_AsIs
  - Arq.Datos_Flujo_Información_CEA_AsIs
  - Arq.Datos_Flujo_Información_CDA_AsIs
  - Arq.Datos_Diagrama_despliegue_datos_AsIs
  - Arq.Datos_Arquitectura_Conceptual_AsIs
  - Arq.Datos_Catálogo_Entidades_Datos_ToBe
  - Arq.Datos_Flujo_Información_CRC_ToBe
  - Arq.Datos_Flujo_Información_CEA_ToBe
  - Arq.Datos_Flujo_Información_CDA_ToBe
  - Arq.Datos_Flujo_Información_CIA_ToBe
  - Arq.Datos_Flujo_Información_CALE_ToBe
  - Arq.Datos_Diagrama_despliegue_datos_ToBe
  - Arq.Datos_Arquitectura_Conceptual_ToBe

- **Arquitectura de Infraestructura**
  - Catálogo de Servicios T.I.
  - Catálogo de Componentes
- **Arquitectura de Seguridad**
  - Catálogo de controles