ANEXO TÉCNICO PARA LA IMPLEMENTACIÓN DEL SISTEMA DE CONTROL Y VIGILANCIA PARA CENTROS DE RECONOCIMIENTO DE CONDUCTORES

Este es el Anexo Técnico del Sistema de Control y Vigilancia para Centros de Reconocimiento de Conductores del que trata la Resolución 9699 de 2014 en la versión adoptada a través de la Resolución 2879 de 2026, que sustituyó integralmente la contenida en la Resolución 6246 de 2016 y las normas que la modificaron.

TÍTULO 1

INFORMACIÓN GENERAL DEL SISTEMA DE CONTROL Y VIGILANCIA PARA CENTROS DE RECONOCIMIENTO DE CONDUCTORES

1.1. Introducción

El presente Anexo Técnico establece el conjunto detallado de requerimientos técnicos, funcionales y operativos que deben cumplir los operadores homologados del Sistema de Control y Vigilancia para Centros de Reconocimiento de Conductores (CRC).

Para facilitar su comprensión y aplicación, este documento se estructura en los siguientes títulos principales:

Título 1 – Información general del SICOV: Presenta el objetivo, la definición, el marco normativo y el alcance del Sistema de Control y Vigilancia, contextualizando su importancia y propósito.

Título 2 – Requerimientos para la provisión del SICOV: Detalla los requisitos de carácter jurídico, administrativo, financiero y técnico que deben satisfacer los proveedores tecnológicos homologados.

Título 3 – Auditorías del SICOV: Establece las directrices para las auditorías al Sistema y a sus operadores homologados.

Título 4 – Acuerdos de niveles de servicio y obligaciones de las partes: Define los niveles de servicio esperados del SICOV y sus componentes, la política de tratamiento y conservación de la información, y las obligaciones específicas tanto de los proveedores homologados como de los Centros de Reconocimiento de Conductores frente al funcionamiento del Sistema.

1.2. Objetivo del documento

El presente Anexo Técnico tiene como objetivo principal establecer los requerimientos del conjunto integral de estándares técnicos, infraestructura tecnológica (hardware y software), protocolos de seguridad y servicios de comunicaciones que garantizan la trazabilidad y autenticidad en la prestación del servicio por parte de los CRC.

1.3. Marco normativo

El Sistema de Control y Vigilancia se fundamenta en las facultades constitucionales otorgadas al Presidente de la República, y en las legales otorgadas directamente a la Superintendencia de Transporte. En particular, su creación, implementación y operación se enmarcan en las siguientes normas:

- El artículo 2 de la Constitución Política, que establece el deber de las autoridades de proteger a las personas y asegurar el cumplimiento de los deberes sociales del Estado y los particulares.
- El artículo 24 de la Constitución Política, que consagra el derecho a la libre circulación, sujeto a la reglamentación de las autoridades para garantía de la seguridad.

- El artículo 365 de la Constitución Política y el literal b del artículo 2 de la Ley 105 de 1993, que atribuyen al Estado las funciones de planeación, regulación, control y vigilancia del servicio público de transporte.
- La Ley 769 de 2002 (Código Nacional de Tránsito), que en su parágrafo 3 del artículo 3, modificado por la Ley 1383 de 2010, asigna a la Superintendencia la función de vigilar y controlar a las autoridades, organismos de tránsito y entidades que constituyan organismos de apoyo al tránsito.
- El Decreto 2409 de 2018, que modificó la estructura de la Superintendencia de Transporte y estableció la necesidad de modernizar los sistemas de inspección, vigilancia y control, facultándola para expedir los reglamentos, manuales e instructivos necesarios.
- La Ley 2050 de 2020, artículo 22, que determinó la obligación para la Superintendencia de realizar visitas periódicas a los organismos de apoyo, directamente o a través del SICOV, y le ordenó adjudicar la instalación, implementación, operación y mantenimiento de los sistemas bajo contratación estatal. Así mismo, el artículo 23 de la misma ley, que adicionó un parágrafo al artículo 136 de la Ley 769 de 2002, determinó la posibilidad de cursos virtuales para infractores con autenticación biométrica a través del SICOV.
- Ley 1341 de 2009 (Ley General de Tecnologías de la Información y las Comunicaciones - TIC): Es la ley marco del sector TIC en Colombia y establece principios sobre la sociedad de la información. Su inclusión contextualiza el fomento y desarrollo de TIC como política de Estado, relevante para cualquier sistema tecnológico gubernamental.
- Ley 527 de 1999 (Ley de Comercio Electrónico): Esta ley es fundamental porque otorga validez jurídica a los mensajes de datos, las firmas digitales y, en general, a las transacciones electrónicas. Dado que el SICOV opera con información digital y transacciones electrónicas, esta ley es la base de su fuerza probatoria.
- Ley 1581 de 2012 (Ley de Protección de Datos Personales): El SICOV maneja una gran cantidad de datos personales y sensibles (biométricos, de salud). Aunque se menciona la responsabilidad sobre datos personales en otros artículos de la resolución, su inclusión explícita en el "Marco legal" del Anexo Técnico es esencial por la criticidad de la información tratada.
- Decreto 767 de 2022 (Actualización de la Política de Gobierno Digital): Este decreto es el marco actual de la Política de Gobierno Digital, que impulsa la transformación digital en el sector público, la interoperabilidad y el uso de TIC para la eficiencia estatal. Su inclusión refuerza el sustento de la modernización tecnológica del SICOV. En el marco de esta política, la estandarización de datos y protocolos de intercambio es un principio fundamental para el efectivo intercambio de información entre entidades públicas.
- Decreto 1079 de 2015 (Decreto Único Reglamentario del Sector Transporte) - Específicamente lo relacionado con el SINITT/SIT: Aunque ya se menciona el Decreto 1079 y el SINITT, es importante que en el Marco Legal se haga una referencia explícita a la parte de este decreto que regula los Sistemas Inteligentes de Transporte (SIT) y el Sistema Inteligente Nacional para la Infraestructura, el Tránsito y el Transporte (SINITT), pues el SICOV es un subsistema o se integrará en este marco.
- Resolución 217 de 2014 del Ministerio de Transporte, por la cual reglamenta la expedición de los certificados de aptitud física, mental y de coordinación motriz para la conducción de vehículos y se dictan otras disposiciones.
- Resolución 11355 de 2020 del Ministerio de Transporte, por la cual se reglamenta el registro de los Organismos de Apoyo al Tránsito ante el Sistema del Registro Único Nacional de Tránsito (RUNT) y se dictan otras disposiciones.

Este marco legal confiere a la Superintendencia la atribución pública de mantener el orden y la legalidad en el sector transporte, impulsando el uso de avances tecnológicos para el fortalecimiento de sus capacidades de supervisión.

1.4. Alcance del documento

El presente Anexo Técnico define los requerimientos a nivel técnico y operativo que deben cumplir los proveedores homologados para operar el Sistema de Control y Vigilancia para los Centros de Reconocimiento de Conductores.

TÍTULO 2

REQUERIMIENTOS PARA LA PROVISIÓN DEL SICOV

2.1. Presentación de solicitud de homologación

Los aspirantes a proveedores del Sistema de Control y Vigilancia deben presentar una solicitud formal dirigida a la Superintendencia de Transporte para su homologación, a fin de ser evaluadas y corroboradas sus condiciones jurídicas, administrativas, financieras y técnicas para la implementación y operación del Sistema de Control y Vigilancia para CRC.

Carta de interés y radicación de requerimientos documentales

Los aspirantes a proveedores homologados deberán enviar una carta de interés a la Superintendencia de Transporte, acompañada de la totalidad de documentos descritos en cada uno de los acápites de los diferentes tipos de requerimientos desarrollados en este documento (jurídicos, administrativos, financieros, técnicos y demás).

La radicación de la carta de interés y sus anexos a través del canal virtual y de radicación física dispuesto por la Superintendencia de Transporte dará inicio al proceso de validación del cumplimiento de los requerimientos para obtener la homologación como proveedor del Sistema de Control y Vigilancia para Centros de Reconocimiento de Conductores.

En el *Documento guía con formatos e instrucciones para la presentación de la solicitud* que publicará la entidad, se encuentra un modelo de carta de interés con especificaciones detalladas sobre la forma de presentar el documento.

2.2. REQUERIMIENTOS JURÍDICOS

Los requerimientos jurídicos buscan principalmente garantizar la legalidad de los proveedores homologados que operan y aspiran operar el SICOV y de sus representantes, validar la capacidad jurídica necesaria para actuar como proveedor homologado , a saber: (i) Obligarse a cumplir el objeto que motivó la creación e implementación del SICOV; y (ii) no estar incursa en inhabilidades o incompatibilidades que impidan el ejercicio de las actividades que involucrada ser proveedor del Sistema.

Se presentan a continuación algunas consideraciones que se deben tener en cuenta.

a) **Persona natural.** Las personas naturales mayores de dieciocho (18) años son capaces jurídicamente a menos que estén expresamente inhabilitadas por decisión judicial o administrativa y que no estén incursas en inhabilidades, incompatibilidades o prohibiciones para contratar derivadas de la ley.

b) **Persona jurídica.** La capacidad jurídica de las personas jurídicas está relacionada con: (i) la posibilidad de adelantar actividades en el marco de su objeto social; (ii) las facultades de su representante legal y la autorización del órgano social competente cuando esto es necesario de acuerdo con sus estatutos sociales; y (iii) la ausencia de inhabilidades, incompatibilidades o prohibiciones para contratar, derivadas de la ley.

En el evento de que la solicitud se presente a través de apoderado, éste debe encontrarse debidamente facultado para presentarla.

Cuando se trate de personas naturales o jurídicas extranjeras sin domicilio o

sucursal en Colombia, deberán además acreditar un apoderado domiciliado en Colombia, debidamente facultado para presentar la solicitud, participar y comprometer a su representado en las diferentes instancias del proceso de solicitud y hasta la homologación, suscribir los documentos y declaraciones que se requieran, así como notificarse, suministrar la información que le sea solicitada, y demás actos necesarios.

Dicho apoderado podrá ser el mismo apoderado único para el caso de personas extranjeras que participen en consorcio o unión temporal, y en tal caso, bastará para todos los efectos, la presentación del poder común otorgado por todos los integrantes del consorcio, unión temporal, u otra figura asociativa cumpliendo los requisitos relacionados con la autenticación, consularización y traducción; particularmente con lo exigido en el Código de Comercio de Colombia. El poder a que se refiere este párrafo podrá otorgarse en el mismo acto de constitución del consorcio o unión temporal, promesa de sociedad futura u otra figura asociativa.

c) Inhabilidades e incompatibilidades: Las inhabilidades e incompatibilidades están establecidas para asegurar los intereses públicos y proteger la transparencia, objetividad e imparcialidad en las relaciones entre el Estado y los particulares.

El régimen de inhabilidades e incompatibilidades es de aplicación restrictiva, por lo cual cuando existen varias interpretaciones posibles sobre una inhabilidad o incompatibilidad, debe preferirse la que menos limita los derechos de las personas.

Todas las entidades estatales sometidas o no a la Ley 80 de 1993, a la Ley 1150 de 2007 y a la Ley 1474 de 2011 y la normatividad vigente, están obligadas a respetar el régimen de inhabilidades e incompatibilidades para contratar o participar en cualquier proceso con el Estado.

Las inhabilidades son una limitación a la capacidad de contratar o participar con Entidades Estatales y están expresamente señaladas en la Ley 80 de 1993.

El proceso de homologación no constituye una delegación de funciones públicas de inspección, vigilancia o control, sino una certificación de idoneidad tecnológica para la operación del Sistema de Control y Vigilancia que deben utilizar los organismos de apoyo a las autoridades de tránsito.

Condiciones que se deben demostrar a través de los soportes documentales correspondientes:

2.2.1. Certificado de existencia y representación expedido por la Cámara de Comercio

Es aquel mediante el cual se acredita la inscripción del contrato social, las reformas y nombramientos de administradores y representantes legales en la cámara de comercio con jurisdicción en el domicilio de la respectiva sociedad. Este tipo de certificación tiene un valor eminentemente probatorio y está encaminada a demostrar la existencia y representación de las personas jurídicas (art. 117 C. de Co.).

2.2.2. Autorización del órgano social

Si el estatuto social impone algún tipo de restricción al representante legal para la presentación de una solicitud como la de homologación, se debe adjuntar copia del documento de autorización correspondiente, emitido por la junta de socios u órgano superior de gobierno social.

Para el caso de consorcios o uniones temporales, dicho documento es exigible a cada uno de los integrantes, si sus estatutos individuales contienen la misma limitante.

La autorización en comento debe expresar en forma clara que el representante legal está autorizado por la junta de socios u órgano societario competente para comprometer a la Sociedad en la presentación de la solicitud y realizar todos los actos necesarios en el proceso. Adicional a lo anterior, debe autorizarse expresamente la facultad de constituir y hacer parte de un consorcio o unión temporal, si a ello hubiere lugar, documento que deberá cumplir con los requisitos solicitados en el artículo 189 del Código de Comercio.

2.2.3. Registro Único Tributario

Es el mecanismo único para identificar, ubicar y clasificar a las personas y entidades que deban cumplir con obligaciones tributarias administradas por la DIAN, así como a quienes, por disposiciones legales, deban hacerlo o por decisión de la DIAN conforme con las normas legales y reglamentarias vigentes.

El operador homologado debe presentar fotocopia legible del Registro Único Tributario (RUT) expedido por la DIAN.

El Sistema de Control y Vigilancia para los Centros de Reconocimiento de Conductores requiere para su operación de actividades tales como desarrollo de software, seguridad de la información y suministro e implementación de hardware y software, las cuales se encuentran consignadas en las siguientes secciones: Sección J "Información y Comunicaciones", en su división 62 "Desarrollo de sistemas informáticos (planificación, análisis, diseño, programación, pruebas), consultoría informática y actividades relacionadas" en la división 63 "Actividades de servicios de información". Los operadores del Sistema de Control y Vigilancia deberán tener dentro de sus actividades económicas registradas en el RUT las actividades del grupo J que se definen en este numeral en las especificaciones de la entrega del documento.

2.2.4. Copia del documento de identidad del representante legal

Para el caso de los ciudadanos colombianos mayores de edad, el documento de identidad es la Cédula de Ciudadanía. En el caso de los extranjeros, es la Cédula de Extranjería que expide Migración de Colombia a manera de documento de identificación, con los mismos efectos que la Cédula de Ciudadanía.

Toda persona natural colombiana que funja como representante legal del operador homologado, deberá allegar copia legible de su cédula de ciudadanía, o cédula digital de conformidad con el Decreto 620 de 2020. Igualmente, lo deberá hacer el representante legal de la persona jurídica, el representante legal de la unión temporal o consorcio y el representante legal de cada uno de los integrantes del consorcio o unión temporal que se haya constituido para el efecto, cuando así sea, y de cada uno de los integrantes de las figuras asociativas. Cuando las mismas estén conformadas por personas jurídicas y/o personas naturales constituidas en Colombia, deberán presentar en forma individual copia legible de su cédula.

Las personas naturales extranjeras, deben acreditar su existencia mediante la presentación de copia de su pasaporte y si se encuentran residenciadas en Colombia, presentarán copia de la cédula de extranjería expedida por la autoridad colombiana competente.

En el *Documento guía con formatos e instrucciones para la presentación de la solicitud* que publicará la entidad, se encuentra un modelo de presentación del documento de identidad del representante legal con especificaciones detalladas sobre la forma de presentar el documento.

2.2.5. Certificado de pago de aportes parafiscales

Toda empresa o unidad productiva que tenga trabajadores vinculados mediante contrato de trabajo debe hacer los aportes que correspondan por concepto de aportes parafiscales, de conformidad con lo previsto en la normatividad vigente.

De acuerdo con lo señalado en el artículo 50 de la Ley 789 de 2002, modificado por la Ley 828 de 2003, y en el artículo 23 de la Ley 1150 de 2007, el operador homologado que desee extender en el tiempo su autorización, deberá entregar una certificación de cumplimiento de sus obligaciones con los sistemas de salud, riesgos profesionales, pensiones y aportes a las Cajas de Compensación Familiar, Instituto Colombiano de Bienestar Familiar y Servicio Nacional de Aprendizaje, expedida por el revisor fiscal, cuando exista según los requerimientos de ley, o por el representante legal de la sociedad interesada, en la que se acredite que dicha compañía se encuentra al día en el pago de aportes al Sistema de Seguridad Social Integral.

El *Documento guía con formatos e instrucciones para la presentación de la solicitud* que publicará la entidad se incluye un modelo de certificación de pago de aportes parafiscales y las especificaciones para la entrega del documento.

2.2.6. Certificación de composición de socios o accionistas

Certificado firmado por el representante legal o el revisor fiscal dependiendo del tipo de empresa, en el que se relacionan los socios y/o accionistas o asociados que tengan directa o indirectamente el 5% o más del capital social, aporte o participación. La certificación debe haber sido expedida con una antelación de máximo treinta (30) días antes de la fecha de presentación de la solicitud. Si dentro de la composición accionaria de la empresa se encuentra una persona jurídica cuya participación sea igual o superior al 5% del capital, se deberá aportar documento con la información de la composición de participación accionaria de esa empresa, proceso que deberá repetirse hasta que identifique el nombre de los accionistas personas naturales. De cada accionista se debe incluir: Nombre o razón social, identificación y porcentaje de participación, siempre y cuando esta sea igual o superior al 5%.

En el *Documento guía con formatos e instrucciones para la presentación de la solicitud* que publicará la entidad, se encuentra un modelo de presentación de la certificación de composición accionaria con especificaciones detalladas sobre la forma de presentar el documento.

2.3. REQUERIMIENTOS ADMINISTRATIVOS

Los requerimientos administrativos incluyen mecanismos que permitan la validación de aspectos tales como la trayectoria del actual operador homologado, experiencia en proyectos similares de tecnología, experiencia del equipo de trabajo entre otros.

2.3.1. Experiencia del operador homologado

La experiencia se entiende como el conocimiento y la capacidad, adquiridos a través la participación previa en actividades iguales o similares a las previstas para la provisión y soporte de la infraestructura tecnológica integrada a la operación de los OAT. Esta experiencia constituye un criterio fundamental para evaluar su idoneidad para satisfacer las necesidades descritas.

Los aspirantes a operador homologado deben presentar los contratos o actividades que hayan celebrado para prestar servicios que pretenden ofrecer y esta puede ser experiencia adquirida de forma directa o a través de la participación del aspirante en consorcios o uniones temporales. Esta experiencia se obtiene con entidades públicas, privadas, de ámbito nacional o extranjero. En el evento de que el proponente sea una persona jurídica puede acreditar la experiencia de sus accionistas, socios o constituyentes, así como, contratos ejecutados celebrados por consorcios, uniones temporales en que tenga o haya tenido participación.

La experiencia requerida debe ser adecuada y proporcional a la naturaleza, alcance, valor y complejidad de las actividades a ejecutar. Se considerará experiencia adecuada aquella que guarde afinidad con el tipo de actividades previstas y proporcional, aquella cuya magnitud sea coherente con la cuantía, complejidad técnica y operativa del servicio a prestar.

Experiencia del operador plural (Unión Temporal, Consorcio y promesa de Sociedad Futura):

La experiencia acreditable será la suma de la experiencia individual de cada uno de sus integrantes. Cuando la experiencia haya sido adquirida como parte de un contratista plural, se considerará únicamente la proporción correspondiente al porcentaje de participación que dicho integrante haya tenido en el contrato o actividad.

Asimismo, la experiencia acreditada deberá estar compuesta por una combinación de actividades que garantice la cobertura integral de todos los componentes funcionales y operativos requeridos para la implementación del Sistema de Control y Vigilancia para los Centros de Reconocimiento de Conductores.

La Superintendencia considera que el cumplimiento de los requisitos que se exponen a continuación permitirá verificar la idoneidad técnica de los operadores para la provisión y soporte de la infraestructura tecnológica integrada a la operación de los CRC. De este modo, se garantizará que el solicitante cuente con las capacidades mínimas necesarias para soportar la operación del Sistema de Control y Vigilancia.

1. Cuantía total de la experiencia requerida: La cuantía de la sumatoria de las experiencias debe ser igual o superior a 10.000 SMMLV (salarios mínimos mensuales legales vigentes), calculados. El valor total, será aquel contemplado a la fecha de suscripción del informe de recibo final o la del acta de recibo final o la fecha de terminación del contrato, por parte del ente contratante o su representante, y la conversión a salarios mínimos mensuales legales vigentes (SMMLV) se hará conforme al vigente en el año de recibo final o terminación.
2. Cuando el valor del contrato esté dado en dólares americanos (USD) se convertirá a pesos colombianos utilizando para esa conversión la tasa representativa del mercado (TRM) vigente para la fecha en que se suscribió el contrato certificado.
3. En caso de presentar certificaciones globales, deberán desglosar el monto o porcentaje y objeto para el cual aplica dicha certificación.
4. Número de contratos a certificar: Los proveedores deberán acreditar experiencia mediante certificación firmada por los contratantes o entes gubernamentales en máximo cuatro (4) certificaciones.
5. Antigüedad en celebración de contratos: Las certificaciones de experiencia ejecutada deberán tener una antigüedad máxima de seis (6) años a la fecha de radicación de la carta de interés.
6. Acreditación de la experiencia: Acreditar experiencia mediante certificación firmada por los clientes o entidades gubernamentales en por lo menos un proyecto en sistemas que incluyan alguna de las siguientes funcionalidades:
    a. Seguridad Informática y/o Seguridad de la Información: Manejo de Riesgo, Protección de Datos, Cifrado de Información, Auditoría de Bases de Datos, Centro de Operaciones de Seguridad (SOC), Correlación de Eventos, Servicios de confianza y/o de validación de identidad
    b. Software: Instalación, integración, desarrollo, actualización de licenciamiento, mantenimiento, soporte y/o Implantación de Software, solución tecnológica o servicio web.
7. Cumplimiento de contratos: Aquellas certificaciones de experiencia que califiquen el cumplimiento del contrato como "malo", "regular", o expresiones similares que demuestren el cumplimiento no satisfactorio del mismo o que indiquen que durante su ejecución fueron sujetas a multas

o sanciones debidamente impuestas por la administración o que a las mismas se les haya hecho efectiva la cláusula penal estipuladas en los contratos, no se aceptarán por el ente evaluador.

En el *Documento guía con formatos e instrucciones para la presentación de la solicitud* que publicará la entidad, se encuentra un modelo de presentación de la certificación de experiencia del aspirante con especificaciones detalladas sobre la forma de presentar el documento.

2.3.2. Certificaciones exigibles

El operador homologado del Sistema de Control y Vigilancia deberá acreditar, como mínimo, certificación en gestión de la calidad bajo la norma ISO 9001 e ISO 27001 y alguna de las mencionadas en líneas siguientes, correspondientes a la seguridad de la información, gestión de servicios de tecnología, modelos de madurez y capacidad o ciclo de vida de construcción y mantenimiento de software. Estas certificaciones deberán haber sido otorgadas por organismos de certificación reconocidos y debidamente acreditados.

Las certificaciones deberán encontrarse vigentes al momento de la evaluación de las solicitudes y corresponder a normas reconocidas a nivel nacional e internacional, que evidencian la implementación de procesos orientados a la mejora continua, el aseguramiento de la calidad en la prestación de servicios y el cumplimiento de requisitos normativos aplicables.

Cuando se trate de operadores plurales, **cada uno** de los integrantes deberá contar con **cada una** de las certificaciones obligatorias y **al menos uno** de ellos debe contar con alguna de las certificaciones adicionales. Las certificaciones deberán estar vigentes durante la el tiempo en que se mantenga vigente la homologación. El cumplimiento de este requisito se demuestra presentando las certificaciones expedidas por el ente que las otorga.

Certificaciones obligatorias:

ISO 9001: Es la base del sistema de gestión de la calidad ya que es una norma internacional y que se centra en todos los elementos de administración de calidad con los que una empresa debe contar para tener un sistema efectivo que le permita administrar y mejorar la calidad de sus productos o servicios. Los clientes se inclinan por los proveedores que cuentan con esta acreditación porque de este modo se aseguran de que la empresa seleccionada disponga de un buen Sistema de Gestión de Calidad (SGC).

ISO 27001: Es una certificación que define cómo organizar la seguridad de la información en cualquier tipo de organización, con o sin fines de lucro, privada o pública, pequeña o grande. Es posible afirmar que esta norma constituye la base para la gestión de la seguridad de la información. La ISO 27001 es para la seguridad de la información lo mismo que la ISO 9001 es para la calidad: es una norma redactada por los mejores especialistas del mundo en el campo de seguridad de la información y su objetivo es proporcionar una metodología para la implementación de la seguridad de la información en una organización.

También permite que una organización sea certificada, lo cual significa que una entidad de certificación independiente ha confirmado que la seguridad de la información se ha implementado en esa organización de la mejor forma posible.

La operación del SICOV mejorado deberá garantizar la planificación, provisión, implementación y operación integral de los servicios de ciberseguridad, cubriendo de manera continua y eficiente la gestión de los centros de operación SOC y NOC, así como las operaciones de mesa de servicio orientadas al soporte técnico, atención de incidentes, gestión de eventos, monitoreo de infraestructura y mantenimiento operativo.

El alcance contempla la definición y despliegue de capacidades técnicas,

procesos, herramientas y recursos necesarios para asegurar la confidencialidad, integridad y disponibilidad de los activos tecnológicos y de información, incluyendo modelos de monitoreo 7x24, respuesta a incidentes, administración de plataformas de seguridad, gestión de vulnerabilidades, correlación de eventos, escalamiento oportuno y la operación coordinada entre NOC, SOC y Mesa de Servicio. Asimismo, se deberán establecer indicadores, acuerdos de nivel de servicio (ANS), roles, responsabilidades y mecanismos de seguimiento que garanticen la continuidad, eficacia y mejora continua del servicio.

Certificaciones adicionales:

El operador homologado del Sistema de Control y Vigilancia deberá contar por lo menos con una de las siguientes certificaciones: CMMI nivel 3 o superior en cualquier de sus áreas, ISO 20000, ISO 15504 y/o SOC 2.

1. **CMMI:** Es un modelo para la mejora y evaluación de procesos para el desarrollo, mantenimiento y operación de sistemas de software. Es un modelo de evaluación de los procesos de una organización y se ha convertido en un estándar para promocionar la capacidad de desarrollar software de alta criticidad, una ventaja para las empresas que participan de proyectos complejos, riesgosos y de alto costo. De acuerdo con la Dirección de Políticas y Desarrollo TI del Ministerio TIC, las organizaciones que implementan el CMMI tienen costos predecibles y cumplen sus actividades dentro de los cronogramas indicados, lo que sin duda redunda en resultados de calidad en sus negocios, contribuyendo al mejoramiento de la competitividad de la empresa, un factor que lo hace diferenciador entre sus competidores.
   Las mejores prácticas CMMI se publican en los documentos llamados modelos. En la actualidad hay tres áreas de interés cubiertas por los modelos de CMMI: Desarrollo, Adquisición y Servicios.

   El Modelo presenta 5 niveles de Madurez. Para ser evaluado en determinado nivel, se debe implementar un conjunto determinado de Prácticas (requeridas).

2. **ISO 20000:** Es el estándar reconocido internacionalmente en gestión de servicios de TI (Tecnologías de la Información). La ISO/IEC 20000 es aplicable a cualquier organización, pequeña o grande, en cualquier sector o parte del mundo donde confían en los servicios de TI. La norma es particularmente aplicable para proveedores de servicios internos de TI, tales como Departamentos de Información Tecnológica, proveedores externos de TI o incluso organizaciones subcontratadas. La norma está impactando positivamente en algunos de los sectores que necesitan TI tales como subcontratación de negocios, Telecomunicaciones, Finanzas y el Sector Público.

   La ISO/IEC 20000 es totalmente compatible con la ITIL (IT Infraestructure Library), o guía de mejores prácticas para el proceso de GSTI. La diferencia es que el ITIL no es medible y puede ser implementado de muchas maneras, mientras que en la ISO/IEC 20000, las organizaciones deben ser auditadas y medidas frente a un conjunto establecido de requerimientos.

3. **ISO 15504:** Es un estándar internacional de evaluación y determinación de la capacidad y mejora continua de procesos de ingeniería del software, con la filosofía de desarrollar un conjunto de medidas de capacidad estructuradas para todos los procesos del ciclo de vida y para todos los participantes. Es el resultado de un esfuerzo internacional de trabajo y colaboración y tiene la innovación, en comparación con otros modelos, del proceso paralelo de evaluación empírica del resultado.

   Norma que trata los procesos de ingeniería, gestión, relación cliente-proveedor, de la organización y del soporte. Se creó por la alta competencia del mercado de desarrollo de software, a la difícil tarea de identificar los riesgos, cumplir con el calendario, controlar los costos y mejorar la eficiencia y calidad. Este engloba un modelo de referencia para los procesos y sus

potencialidades sobre la base de la experiencia de compañías grandes, medianas y pequeñas.

4. **Certificación SOC 2:** Es una certificación que constituye un estándar de control emitido por el AICPA, mediante el cual se verifica que la organización dispone de políticas, procedimientos y controles efectivos orientados a garantizar la seguridad, disponibilidad, integridad, confidencialidad y privacidad de la información bajo su administración. Esta certificación deberá evidenciar el cumplimiento de los principios de seguridad, disponibilidad, integridad del procesamiento, confidencialidad y privacidad, de acuerdo con los criterios establecidos en el marco de los Trust Services Criteria.

   Para garantizar la confiabilidad, integridad operativa y seguridad de todos los procesos asociados a la prestación del servicio, el proveedor deberá cumplir de manera obligatoria con los criterios del marco SOC 2 (Service Organization Control 2), alineándose con los Principios de Confianza: Seguridad, Disponibilidad, Integridad de Procesamiento, Confidencialidad y Privacidad. Este cumplimiento es un requisito indispensable dado que la operación implica el tratamiento de información sensible, la continuidad de servicios críticos y la ejecución de actividades que requieren controles estrictos en materia de accesos, monitoreo continuo, trazabilidad, gestión de incidentes, segregación de ambientes, auditoría verificable y protección de datos. De forma obligatoria, el proveedor deberá demostrar que cuenta con controles implementados, auditados y vigentes bajo SOC 2, garantizando así evidencia independiente, verificabilidad objetiva y un nivel adecuado de gobernanza y seguridad. Este requisito reduce riesgos tecnológicos, operativos, contractuales y regulatorios, y asegura que la prestación del servicio se realice bajo estándares internacionales de seguridad, resiliencia y cumplimiento.

En el *Documento guía con formatos e instrucciones para la presentación de la solicitud* que publicará la entidad, se encuentra un modelo de presentación de las certificaciones exigibles con especificaciones detalladas sobre la forma de presentar el documento.

Adicionalmente, el homologado acreditará el cumplimiento de este requisito presentando las certificaciones expedidas por el ente que las otorga.

2.3.3. Equipo de trabajo exigible a la compañía

El equipo de trabajo es el personal mínimo idóneo con que debe contar el operador homologado para la ejecución del proyecto, para garantizar atención suficiente y oportuna a todos los frentes operacionales involucrados en el funcionamiento del Sistema de Control y Vigilancia.

Con el fin de asegurar la idoneidad y estabilidad del equipo de trabajo se deberá adjuntar copia de título profesional, matrícula profesional vigente (en los casos que aplique) y las certificaciones correspondientes que permitan demostrar que el personal tiene algún tipo de contrato con el operador homologado.

En el *Documento guía con formatos e instrucciones para la presentación de la solicitud* que publicará la entidad, se encuentra un modelo de certificado de cumplimiento de las exigencias mínimas de personal, con especificaciones detalladas sobre la forma de presentar el documento.

2.3.3.1. Equipo de Dirección

2.3.3.1.1. Gerente de proyectos

El Gerente de Proyectos tiene a su cargo la planificación, dirección y coordinación del proyecto en todos sus aspectos, definiendo y concretando los objetivos, identificando las actividades a realizar, los recursos técnicos y de personal, los plazos y los costos requeridos para la ejecución del mismo. Se encargará de

mantener permanente contacto con el personal que se requiera durante la ejecución del proyecto y tomará las medidas preventivas y correctivas pertinentes para contrarrestar los riesgos que se detecten.

Se requerirá un (1) profesional en ingeniería de sistemas, industrial, electrónica, derecho, administración de empresas, economía o carreras afines, con especialización o maestría en gerencia de proyectos, con certificación de PMP o certificado SCRUM y experiencia certificada en dirección de proyectos en los últimos tres (3) años.

2.3.3.2. Equipo de trabajo de seguridad

Los operadores homologados deberán contar con los perfiles solicitados en los numerales subsiguientes y, en caso de subcontratar el servicio de SOC, se deberá anexar el contrato suscrito con la empresa que presta el servicio y las hojas de vida del personal solicitado, las cuales deberán cumplir con lo que aquí se establece o su equivalente.

2.3.3.2.1. Gerente de SOC

El Gerente de SOC tiene a su cargo el diseño, la planificación, dirección y coordinación de la seguridad de la información, de su monitoreo y tratamiento de las incidencias o novedades que se puedan presentar.

Un (1) profesional en ingeniería de sistemas, industrial, electrónica o carreras afines, con especialización o maestría en seguridad informática o certificación como auditor Interno de ISO-27001.

2.3.3.2.2. Oficial de seguridad

Es el encargado de monitorear y evidenciar los diferentes casos de novedades y darles el respectivo tratamiento a los eventos presentados. Debe establecer los controles respectivos para la defensa de los mismos.

Un (1) profesional en Ingeniería de Sistemas, Industrial, Electrónica o carreras afines, con especialización o Maestría en Seguridad Informática o certificado como CISSP o CISM.

2.3.3.2.3. Especialista DBA

Es el encargado de establecer las políticas de acceso a las bases de datos y monitorear los eventos presentados en tiempo real; esta tarea la podrá realizar a través de herramientas de monitoreo activo de bases de datos o través de la activación y monitoreo de los logs de las bases de datos.

Se requerirá un (1) profesional en Ingeniería de Sistemas, Industrial, Electrónica o carreras afines, con certificaciones en la base de datos de la solución implementada o certificación técnica o experiencia certificada como DBA en los últimos dos (2) años.

2.3.3.2.4. Especialista en ethical hacking

Tiene a su cargo adelantar las actividades tendientes a detectar las debilidades y vulnerabilidades en los sistemas, utilizando para ello, el mismo conocimiento y herramientas de un hacker malicioso, con el fin de generar las herramientas de prevención que requiere el sistema.

Se requerirá un (1) profesional en Ingeniería de Sistemas, Industrial, Electrónica o carreras afines, certificado como CEH, seguridad informática, Ethical Hacker y/o CISSP o experiencia certificada de siete (7) años, por parte de entidades públicas o privadas, en Ethical Hacking; o tener contrato vigente con una compañía para la prestación de Servicios de Ethical Hacking que tenga personal certificado como CEH y/o CISSP.

En caso de que este servicio sea provisto por un tercero, el operador homologado deberá aportar la hoja de vida del personal que será asignado de forma efectiva al SICOV, demostrando que dicho personal cumple con las el perfil individual aquí exigido.

2.3.3.2.5. Analista de inteligencia y fraude

El analista de inteligencia de datos y fraude tendrá a su cargo el diseño y la implementación de los modelos analíticos y la aplicación de tecnologías como la inteligencia artificial para el análisis de patrones, la detección de anomalías y la identificación de riesgos de fraude, incluyendo aquellos relacionados con la rotación de personal, el uso indebido de recursos y la expedición irregular de certificados. Se requerirá un (1) profesional en ingeniería de sistemas, estadística, matemáticas o carreras afines, con postgrado o especialización en análisis de datos, inteligencia de negocio o ciencia de datos y con experiencia certificada en proyectos de analítica y/o modelos de detección de fraude en los últimos tres (3) años.

2.3.3.3. Equipo de trabajo de desarrollo

2.3.3.3.1. Gerente de producto

El Gerente de producto tiene a su cargo el diseño, la planificación, dirección y coordinación del desarrollo, pruebas, integraciones y la operación del Software de gestión y control.

Se requerirá un (1) profesional en ingeniería de sistemas, industrial, electrónica, de redes o afines, con posgrado en diseño o desarrollo de producto, o experiencia laboral como gerente, líder o coordinador de producto en los últimos cinco (5) años.

2.3.3.3.2. Gerente o líder de desarrollo

El Gerente o líder de desarrollo tiene a su cargo garantizar que la solución a nivel técnico sea la más adecuada dependiendo de las necesidades actuales y previendo evolución a futuro. Valida previamente cada entrega.

Se requerirá un (1) profesional en ingeniería de sistemas, electrónica, de redes o afines, con posgrado en arquitectura, construcción o ingeniería de software y experiencia laboral certificada como arquitecto, líder, coordinador o gerente de desarrollo en los últimos dos (2) años.

2.3.3.3.3. Ingenieros o tecnólogos de desarrollo

Es el equipo de profesionales o tecnólogos necesario para el desarrollo e integración de las diferentes funcionalidades del software del Sistema de Control y Vigilancia y la aplicación móvil.

Se requerirá que los operadores homologados del Sistema de Control y Vigilancia cuenten con:

Cinco (5) profesionales en ingeniería de sistemas, electrónica, industrial o afines o tecnólogo en sistemas con certificación en lenguajes de programación en los que se encuentra construida el software o aplicación móvil, o experiencia laboral certificada en los últimos tres (3) años en dichos lenguajes.

En caso de que el desarrollo de software se contrate con una fábrica de software, el aspirante o actual homologado deberá tener contrato vigente suscrito con dicha fábrica, así como las licencias de uso vigentes en los casos que aplique.

2.3.3.4. Mesa de ayuda/ Equipo de soporte

Entendida como un conjunto de recursos tecnológicos y personal técnico, para prestar servicios con la posibilidad de gestionar y solucionar todas las posibles

incidencias de manera integral, junto con la atención de requerimientos relacionados a las Tecnologías de la Información y la Comunicación (TIC). El personal técnico encargado de Mesa de Ayuda (MDA) debe proporcionar respuestas y soluciones a los usuarios finales, clientes o beneficiarios (destinatarios del servicio), y también puede otorgar asesoramiento en relación con una organización o institución, productos y servicios.

Generalmente, el propósito de MDA es solucionar problemas de la operación y atención de usuarios relacionado con los servicios tecnológicos, equipos de cómputo, electrónicos o software. El homologado deberá contar con un Ingeniero certificado en ITIL (Information Technology lnfrastructure Library), en español Biblioteca de Infraestructura de Tecnologías de Información) intermedio superior, quien deberá definir, implementar, entregar, avalar y mantener actualizado el esquema de atención de la mesa de ayuda, así como la impementación de buenas prácticas para la gestión de servicios de tecnologías de la información (TI).

El servicio de Mesa de Ayuda debe estar disponible durante los horarios operativos de los centros, y horas adicionales, así: de lunes a sábados, de 5:00 am a 10:00 pm; y los domingos y festivos de 7:00 am a 4:00 pm. Al entrar en operación, el equipo de la Mesa de ayuda será el necesario para el cumplimiento de los ANS (Acuerdo de Niveles de Servicio) atendiendo la demanda de los CRC con los que exista contrato vigente.

2.3.3.4.1. Líder de Mesa de Ayuda

Se requerirá contar con un al menos un (1) profesional en ingeniería de sistemas, industrial, electrónica o carreras afines con posgrado o certificación en ITIL o experiencia en soporte al momento de presentarse al proceso de evaluación de homologación.

2.3.3.4.2. Analistas de soporte/Mesa de Ayuda

Se requerirá contar un equipo de analistas de soporte o mesa de ayuda que permita cumplir con los Acuerdos de Niveles de Servicio establecidos en el presente Anexo Técnico.

El equipo deberá estar integrado por al menos dos (2) profesionales en ingeniería de sistemas, electrónica o redes y ocho (8) técnicos de soporte, técnicos, tecnólogos o ingenieros de sistemas, electrónica, redes, telecomunicaciones o afines. El volumen adicional del personal de analistas obedecerá a la demanda.

2.3.4. Aliado u operador de recaudo

El operador homologado del Sistema de Control y Vigilancia deberá ser o contar con contrato vigente con uno o más aliados u operadores de recaudo que deberán cumplir con los siguientes requerimientos:

1. Acreditar experiencia mediante certificación firmada por los clientes en por lo menos dos (2) proyectos donde se haya efectuado integración con los sistemas transaccionales de cualquier sector productivo en los últimos tres (3) años.
2. Ser un miembro del Sistema Financiero Colombiano (en el caso de los bancos deberá ser calificado como de bajo riesgo), u operador postal de pago habilitado o autorizado en Colombia y que tenga convenio para este proyecto por lo menos con una entidad financiera vigilada por la Superintendencia Financiera de Colombia
3. El aliado de recaudo deberá generar un número de identificación único de pago (PIN) a través de un proceso seguro, que se realiza a través de un algoritmo que concatena diferentes campos de información de una transacción, que finalmente se construye con un consecutivo secuencial, único e irrepetible de forma segura

El PIN de pago estará obligatoriamente asociado al número de documento de identidad del usuario. Para realizar el pago, se requerirá a quien lo realiza que exhiba su documento si es que es la misma persona que va a tomar el servicio, o y/o en todo caso deberá confirmar los datos de quien lo va a tomar. Lo anterior, a fin de verificar, por parte del recaudador, que el tipo y número de documento de identidad, para la generación del PIN, son precisos.

Además, el operador de recaudo debe cumplir con las siguientes obligaciones:

4. Encriptación de los datos que viajan a través de la red.
5. Actualización en línea de lo recaudado.
6. Debe estar constituido un esquema de replicación en línea de los datos.
7. Deberá emitir o generar comprobantes de recaudo, con posibilidades de emitir las copias necesarias.
8. Contar con redundancia de un CPD principal y un CAPD, que garantice la continuidad del servicio.
9. Deberá contar con dispositivos de seguridad perimetral en la red.
10. Disponer de un canal de atención inmediata para los usuarios y/o clientes.
11. Deberá tener restricción en la manipulación técnica de los equipos de cómputo o terminales en los puntos de recaudo.
12. Debe registrar y llevar trazabilidad de datos de cada operación de recaudo tales como fecha, hora, nombres e identificación de la persona que realiza el pago con tipo y número de identidad, valor del servicio. Con estos últimos datos deberá generar un algoritmo hash cuyo resultado debe ser un número que permita realizar verificaciones de información y prevenir cualquier intento de violación o cambio de información.
13. Debe registrar, controlar, validar y llevar trazabilidad de los datos de pago tales como: número único de registro o número único de identificación de pago o compra, el valor del pago, el estado (pago o utilizado), fecha del uso del servicio, hora del uso del servicio, número único de uso, entre otros.
14. Deberá presentar procedimiento que evite que traten de falsificar comprobantes de recaudo.
15. Deberá suministrar al operador del SICOV, la información requerida de la trazabilidad de cada operación de recaudo.
16. Deberá efectuar la conciliación bancaria por parte de terceros, respecto al uso y manejo de recursos del Estado de los valores ordenados por el artículo 20 de la Ley 1702 de 2013.
17. Los aliados de recaudo deberán garantizar atención para resolver cualquier novedad, atender cualquier petición, reclamo o denuncia, por parte de cualquiera de los organismos de apoyo a los que el proveedor SICOV preste el servicio, independientemente del municipio del país en el que se encuentren.
18. La atención debe ser garantizada a través de los siguientes canales o medios de atención: línea telefónica, WhatsApp y correo electrónico.
19. El aliado de recaudo deberá brindar la opción de pago a través de diferentes medios, tales como: pagos a través de internet, datáfonos o dispositivos satélites.
20. El aliado de recaudo deberá estar integrado con el Sistema de Control y Vigilancia, permitiendo que el SICOV realice en línea y tiempo real la consulta, validación y control del consumo de los Pines y toda la información de quienes los adquieren y del servicio.
21. El aliado de recaudo deberá efectuar la conciliación bancaria por parte de terceros, respecto al uso y manejo de recursos del Estado, entre estos, de los valores ordenados por el articulo 20 de Ley 1702 de 2013, modificado por el artículo 30 de la Ley 1753 de 2015 y conforme a lo previsto en la Resolución 993 de 2017 y las demás, que la sustituyan, modifiquen o deroguen.
22. El operador de recaudo deberá reportar al SICOV la información de cada operación realizada, con toda la trazabilidad de datos indicada, y la demás que determine la Superintendencia, en línea y tiempo real.
23. Constituir una póliza de cumplimiento a favor de cada CRC a los que preste el servicio y del homologado, por el buen manejo del dinero recaudado.

El recaudo del PIN de pago responde a la gestión financiera de un componente del costo del servicio.

2.3.5. Operador tecnológico del servicio para la autenticación biométrica de la Registraduría Nacional del Estado Civil

El operador homologado del Sistema de Control y Vigilancia deberá ser o tener contrato vigente suscrito con un operador del servicio para autenticación biométrica en el nivel 1. Para tal efecto, deberá cumplir con todos los requerimientos y evaluaciones exigidos por la Registraduría Nacional del Estado Civil y estar habilitado de conformidad con la normatividad vigente aplicable.

En cuanto la Registraduría habilite operadores en el nivel 2, de biometría facial, los operadores homologados del SICOV deben cumplir con tales requerimientos.

El operador debe cumplir con los siguientes requerimientos:

1. Acreditar cumplimiento de requisitos con la RNEC según la resolución y anexos vigentes.
2. Tener infraestructura tecnológica aprobada, desplegada, auditada por la RNEC y en producción realizando consultas permanentes para por lo menos una entidad pública o con funciones públicas del servicio de validación de identidad contra las bases de datos de identificación ciudadana (Biometría), manejando el estándar ISO 19794-2, conforme a lo dispuesto en la Resolución 27145 del 2023 de la RNEC, sus anexos y la normatividad vigente.
3. La validación de identidad biométrica deberá tener características de firma electrónica con validez jurídica y probatoria según el Decreto 2364 de 2012, asegurando la autenticidad, integridad y no repudio de la transacción usando los mecanismos previstos por la ley 527 de 1999.

2.4. REQUERIMIENTOS FINANCIEROS

Los requerimientos financieros buscan establecer unas mínimas condiciones económicas que reflejan solidez y capacidad económica suficiente de los operadores homologados del SICOV para garantizar la implementación, operación y mantenimiento continuo del Sistema, bajo las exigencias aquí descritas. Estas condiciones se miden a través del análisis de indicadores clave como la liquidez y el nivel de endeudamiento. Tales parámetros permiten verificar la capacidad del proveedor para asegurar la operación, disponibilidad y mantenimiento de la infraestructura tecnológica del SICOV.

La capacidad financiera exigida deberá ser adecuada y proporcional en relación con la naturaleza, el valor, el plazo y la forma de ejecución del Sistema a implementar y operar.

En función de las particularidades del servicio, se deberán utilizar los indicadores financieros que resulten más pertinentes para evaluar la viabilidad económica del proveedor frente al alcance del proyecto. Algunos ejemplos comunes pueden incluir: razón corriente, índice de endeudamiento, prueba ácida, entre otros.

Es importante resaltar que la evaluación financiera no debe aplicarse de forma mecánica ni limitarse al uso de fórmulas estándar. Las entidades responsables de la verificación deben tener un conocimiento claro sobre el significado, la interpretación y la aplicabilidad de cada indicador, de modo que el análisis financiero refleje con precisión la aptitud del proveedor para asumir los compromisos requeridos.

Los indicadores de capacidad financiera que se encuentran descritos en el artículo 10 del Decreto 1510 de 2013 son:

Índice de Liquidez = Activo Corriente / Pasivo Corriente, el cual determina la capacidad que tiene el operador homologado para cumplir con sus obligaciones

de corto plazo. A mayor índice de liquidez, menor es la probabilidad de que el aspirante incumpla sus obligaciones de corto plazo.

Índice de Endeudamiento = Pasivo Total / Activo Total, el cual determina el grado de endeudamiento en la estructura de financiación (pasivos y patrimonio) del homologado. A mayor índice de endeudamiento, mayor es la probabilidad del homologado de no poder cumplir con sus pasivos.

Capital de Trabajo = Activo corriente - Pasivo Corriente, el cual muestra la liquidez operativa que tiene un homologado, es decir, el remanente del homologado luego de liquidar sus activos corrientes (convertirlos en efectivo) y pagar el pasivo de corto plazo. Un capital de trabajo positivo contribuye al desarrollo eficiente de la actividad económica del proponente. Es recomendable su uso cuando la Entidad Estatal requiere analizar el nivel de liquidez en términos absolutos.

La siguiente tabla muestra la interpretación de cada uno de los indicadores de capacidad financiera y su relación con la probabilidad de Riesgo:

Indicador	Si el indicador es mayor, la probabilidad de riesgo es	Límite
Índice de liquidez	Menor	Mínimo
Índice del endeudamiento	Mayor	Máximo

Las entidades estatales pueden establecer indicadores adicionales a los establecidos en el numeral 3 del artículo 10 del Decreto 1510, solo en aquellos casos en que sea necesario por las características, la naturaleza o complejidad del servicio a implementar. Es importante tener en cuenta que los indicadores pueden ser índices como en el caso del índice de liquidez (activo corriente dividido por el pasivo corriente) o valores absolutos como el capital de trabajo y el patrimonio.

Los indicadores solicitados serán los siguientes:

INDICADORES	CONCEPTO	REQUISITO
Capital real (Entendido como el respaldo y solvencia)	Utilidades del ejercicio	> $ 3.500.000.000
Liquidez	Activo corriente/pasivo corriente	>1.2
Nivel de endeudamiento	Pasivo total/activo total	< 65%
Capital de trabajo	Activo corriente-pasivo corriente	>$10.000.000.000
De riesgo	Activo fijo/patrimonio neto	<0.6

El operador homologado deberá presentar los siguientes documentos mínimos con la presentación de la carta de intención:

2.4.1. Balance general, estado de resultados y notas a los estados financieros

Con corte al 31 de diciembre del año inmediatamente anterior a la presentación de la propuesta ante la Superintendencia de Transporte, aprobados por el órgano competente, debidamente certificados y dictaminados.

La Superintendencia de Transporte, al hacer la verificación financiera, podrá requerir información adicional del aspirante o actual homologado para el esclarecimiento de la información, tales como: estados financieros de años anteriores, anexos específicos o cualquier otro soporte. Asimismo, podrá pedir las aclaraciones que considere necesarias, sin que las aclaraciones o documentos

que el homologado allegue a la solicitud de la Superintendencia puedan modificar, adicionar o complementar la propuesta. Para efectos del dictamen de los estados financieros, se tendrá en cuenta lo dispuesto en el artículo 38 de la Ley 222 de 1995 que indica: Son dictaminados aquellos estados financieros certificados que se acompañen de la opinión profesional del revisor fiscal o, a falta de este, del contador público independiente que los hubiere examinado de conformidad con las normas de auditoría generalmente aceptadas. Estos estados deben ser suscritos por dicho profesional, anteponiendo la expresión "ver la opinión adjunta" u otra similar. El sentido y alcance de su firma será el que se indique en el dictamen correspondiente.

Cuando los estados financieros se presenten conjuntamente con el informe de gestión de los administradores, el revisor fiscal o contador público independiente deberá incluir en su informe su opinión sobre si entre aquellos y estos existe la debida concordancia. En consecuencia, entiéndase que quien certifica los estados financieros no puede dictaminar los mismos. Solo se aceptará "dictamen limpio", entendiéndose por este, aquel en el que se declara que los estados financieros presentan razonablemente en todos los aspectos significativos, la situación financiera, los cambios en el patrimonio, los resultados de operaciones y los cambios en la situación financiera de la entidad, de conformidad con los principios de contabilidad generalmente aceptados.

Los operadores homologados deberán presentar los estados financieros dictaminados a corte 31 de diciembre del año inmediatamente anterior durante los años en que presten el servicio en caso de resultar homologados.

En caso de que el operador homologado sea evaluado antes del 31 de marzo de la vigencia en que se presente, y no cuente con los estados financieros a corte de 31 de diciembre de la vigencia inmediatamente anterior, podrá presentar los estados financieros del año fiscal anterior.

2.4.2. **Fotocopia de la tarjeta profesional del contador**, revisor fiscal o contador independiente, según corresponda;

2.4.3. **Certificación expedida por la Junta Central de Contadores**, la cual no será anterior a tres (3) meses de la fecha de presentación de la solicitud, del contador, revisor fiscal o contador independiente, según corresponda.

2.4.4. **Indicadores de las uniones temporales o consorcios.** En caso de que el homologado participe como una Unión Temporal o Consorcio, para los efectos de este Anexo, deberá cumplir con los indicadores financieros que se proponen. Los indicadores se calcularán mediante la sumatoria simple del resultado de cada uno de sus integrantes.

2.5. REQUERIMIENTOS TÉCNICOS

Este capítulo establece los requerimientos técnicos mínimos que demostrar la infraestructura tecnológica provista por los operadores homologados del Sistema de Control y Vigilancia para Centros de Reconocimiento de Conductores, con el fin de cumplir con el objeto para el cual fue creado y garantizar su funcionamiento óptimo y disponibilidad.

A través de los distintos componentes mínimos que se desarrollan en este documento, se deberá garantizar la operación del Sistema, el óptimo desempeño de la totalidad de sus funciones mínimas previstas en la Resolución 9699 de 2014, así como el procesamiento y la transmisión segura de la información.

Los requerimientos y condiciones del Sistema y los requisitos exigidos al proveedor, en razón de su naturaleza tecnológica, están sujetos a modificaciones como consecuencia del desarrollo y avances de la ciencia y la tecnología. Para la elaboración de este documento, se ha tenido en cuenta la información en materia de normas, estándares y reglamentaciones técnicas internacionales.

En razón de lo anterior, los dispositivos que se describen en detalle, por lo tanto, corresponden a referentes mínimos esperados por la Superintendencia de

Transporte. En consecuencia, los operadores podrán proponer e implementar tecnologías, dispositivos o servicios que superen estos estándares, siempre que dicha mejora esté técnica y funcionalmente justificada ante la Superintendencia de Transporte y no comprometa la integridad de la cadena de custodia de la información.

Son componentes del SICOV:

1. **Centro de Procesamiento de Datos (CPD).** Es el lugar o instalación física donde se concentran un conjunto de recursos tecnológicos (servidores, sistemas de almacenamiento, equipos de red, *hardware*, *software*) y humanos necesarios para la organización, realización y control del procesamiento de la información. También se le conoce como centro de datos o datacenter. Con el fin de garantizar la seguridad de la información, la infraestructura deberá ser desplegada dentro del territorio nacional.

   Sirve para alojar y operar las aplicaciones y datos críticos de un sistema, garantizando la continuidad y disponibilidad del servicio. Su propósito principal es asegurar la accesibilidad y confianza de la información 24 horas al día, 7 días a la semana, 365 días al año. Provee la infraestructura fundamental para el almacenamiento seguro y el procesamiento de la información, permitiendo la fiabilidad, seguridad, redundancia y diversificación de los datos y servicios. En el contexto del SICOV, es donde residen el software de gestión y control, las bases de datos y la información de control y monitoreo.

2. **Centro de Operaciones de Seguridad (NOC-SOC)**. Es un grupo de personas, procesos, infraestructura y tecnología dedicados a gestionar, tanto de forma reactiva como proactiva, amenazas, vulnerabilidades y, en general, incidentes de seguridad de la información.

   Su objetivo es minimizar y controlar el impacto de los eventos de seguridad en el sistema. Sirve para monitorear, detectar, analizar y responder a incidentes de ciberseguridad, aplicando controles para la defensa y manteniendo la integridad, confidencialidad y disponibilidad de la información. En el SICOV, el SOC es fundamental para prevenir fraudes, proteger datos sensibles y asegurar la continuidad operativa frente a ataques o vulnerabilidades.

3. **Mesa de Ayuda.** Es un conjunto de recursos tecnológicos y humanos, diseñado para prestar servicios con la posibilidad de gestionar y solucionar todas las posibles incidencias de manera integral, junto con la atención de requerimientos relacionados con las Tecnologías de la Información y la Comunicación (TIC).

4. **Red de Comunicaciones.** Se refiere a la infraestructura necesaria para interconectar todos los elementos del Sistema de Control y Vigilancia, incluyendo los Centros de Reconocimiento de Conductores y la Superintendencia de Transporte (mediante una interfaz).

   Sirve para garantizar la transmisión segura, eficiente y confiable de la información entre todos los componentes y actores del sistema. Es la base para que la información (como validaciones biométricas, registros de exámenes, gestión de recursos, certificaciones, etc.) pueda fluir en tiempo real desde los organismos de apoyo hacia los servidores centrales del SICOV y hacia la Superintendencia, así como para la comunicación con sistemas externos como y el acceso a las redes de área extensa (WAN) e internet.

5. **Software de gestión y control.** El Sistema de Control y Vigilancia contará con una solución de software ejecutable en la sede de los Centros de Reconocimiento de Conductores que permita capturar información y llevar trazabilidad integral de su operación, en cada una de las etapas de la prestación del servicio, bajo los parámetros definidos por la Superintendencia de Transporte. La parametrización precisa y segura de

este Sistema permitirá vigilar y controlar el cumplimiento de las obligaciones de este grupo de vigilados.

6. **Hardware y software de uso descentralizado.** La operación del SICOV requerirá de la adquisición, disposición e implementación de dispositivos hardware (a nivel centralizado y descentralizado) y software propios o provistos por terceros que faciliten y permitan el funcionamiento de la herramienta del software de gestión y control del SICOV de acuerdo con las funcionalidades desarrolladas.

7. **Centro de analítica de datos y monitoreo central de operación.** El Sistema de Control y Vigilancia debe garantizar el conjunto de recursos tecnológicos (servidores, sistemas de almacenamiento, equipos de red, hardware, software) que sean necesarios para el funcionamiento de un Módulo de Consulta, IVC e Inteligencia de Negocio (MOCVI) que sirva para la consulta, visualización, procesamiento y descarga de información sobre la operación del SICOV operado por todos los operadores homologados en los diferentes tipos de organismos de apoyo a las autoridades de tránsito.

   A efectos de garantizar dichas capacidades, los operadores homologados deberán implementar y mantener un Centro de Procesamiento de Datos Analítico y de Identificación, conformado por un Centro de Procesamiento de Datos y un Centro Alterno de Procesamiento de Datos, los cuales consolidarán en un único repositorio nacional los datos generados por los organismos de apoyo (CDA, CEA, CIA, OTT, CRC) a través del SICOV.

   Este centro no sustituye los CPD ni CAPD operativos de cada operador, sino que actúa como una infraestructura especializada en integración, transformación, análisis, inteligencia de negocio e inteligencia artificial, permitiendo a la Superintendencia de Transporte acceder, en tiempo casi real, a tableros analíticos, reportes consolidados, indicadores estratégicos, flujos de inspección y mecanismos de seguimiento y control basados en datos. El CPD Analítico y de Identificación proveerá la plataforma tecnológica requerida para soportar el Módulo de Consulta, Vigilancia, Control e Inteligencia de Negocio (MOCVI), centralizando la información nacional del SICOV bajo condiciones de alta disponibilidad, integridad, seguridad y continuidad operativa.

   El CDP Analítico y de Identificación es la fuente oficial y centralizada de información analítica del SICOV, lo que permite a la Superintendencia ejercer sus funciones de inspección, vigilancia y control mediante herramientas avanzadas de visualización, analítica descriptiva, analítica predictiva, conciliación de datos y seguimiento transversal de la operación de los organismos de apoyo. Su diseño y operación garantizarán que la información consolidada sea íntegra, confiable y oportuna, respaldando las decisiones regulatorias, los procesos de auditoría y los mecanismos de prevención, detección y mitigación de conductas irregulares en el sistema.

2.5.1. Documentación técnica

Los operadores homologados deberán presentar la siguiente documentación técnica:

- **Copia del certificado de registro de soporte lógico de la Dirección Nacional de Derechos de Autor** respecto del software de gestión y control del SICOV. En el caso de que el aspirante utilice una licencia de software de una solución fabricada por otra compañia, deberá adjuntar copia de la licencia de uso o cesión de derechos de autor por parte de la compañía fabricante.
- **Relación de equipos del CPD y CPAD**, teniendo en cuenta los requisitos mínimos que se desarrollan más adelante, identificando marca, modelo, el datasheet y soporte de Gartner o Forester Wave de las soluciones de servidores, SAN, licencia de sistemas operativos y licencias de bases de datos. En caso de que el CPD se encuentre subcontratado se debe

adjuntar **copia de contrato**. Los contratos deberán tener una duración mínima de veinticuatro (24) meses.

- **Relación de equipos del Centro de Operaciones de Seguridad,** teniendo en cuenta los requisitos mínimos que se desarrollan más adelante, identificando marca, modelo, IPS, Herramienta DAM. Firewall, Herramienta, SIEM, SAN, Escáner de Vulnerabilidades, Application Delivery Controller. En el caso en el que el Centro de operaciones SOC se encuentre subcontratado, la relación presentada deberá ser del proveedor contratado. En caso de que la operación del NOC-SOC se encuentre subcontratado, se debe adjuntar copia de contrato.

  El SIEM debe ubicarse en la última versión del cuadrante mágico de Gartner.

- **Plan de recuperación de desastres** del Operador, indicando los objetivos de recuperación, conforme se detalla en el presente Anexo.

2.5.2. Aspectos técnicos generales del SICOV

El Sistema de Control y Vigilancia deberá concebirse, diseñarse e implementarse bajo los siguientes principios y requisitos técnicos generales, que regirán la totalidad de sus componentes y operaciones:

1. **Ubicación segura de la infraestructura centralizada:** Las instalaciones físicas principales y las de respaldo (sistema espejo) de la infraestructura centralizada del SICOV (CPD, SOC) deberán estar ubicadas en la República de Colombia, en un sitio seguro, con controles de acceso físico y vigilancia permanente, que permitan procesos de auditoría sobre la información y su administración. Se buscará la diversificación geográfica para garantizar la continuidad del servicio ante eventos de impacto regional.
2. **Operación continua y planes de contingencia:** Todos los componentes del Sistema deberán contar con la capacidad para garantizar la operación continua (*24/7/365*), con sus respectivos planes de contingencia y protocolos de actuación definidos para la atención de incidentes y la recuperación ante fallas. La disponibilidad operativa deberá reflejar los niveles de servicio establecidos para cada componente.
3. **Escalabilidad y rendimiento robusto:** Los componentes del sistema deberán responder a los niveles de escalabilidad requeridos, tanto vertical como horizontal, que permitan atender picos de demanda y expansiones futuras de la prestación del servicio a la totalidad de los organismos de apoyo a nivel nacional. En consecuencia, la infraestructura tecnológica deberá estar soportada por equipos de cómputo robustos, con alto poder de procesamiento y capacidad para ejecutar cargas operativas intensivas.
4. **Almacenamiento y conectividad resilientes:** Se requerirán sistemas de almacenamiento de alto rendimiento, capaces de soportar tanto las operaciones activas como los periodos de reposo de datos, incorporando esquemas de redundancia y tolerancia a fallos para asegurar la continuidad e integridad del servicio. La solución deberá incluir también equipos de comunicación como switches, routers y balanceadores de carga que garanticen la conectividad eficiente, segura y de alta disponibilidad entre todos los componentes del sistema y con los sistemas externos de la Superintendencia de Transporte y otras entidades.
5. **Seguridad integral (perimetral y lógica):** La infraestructura deberá contemplar la implementación de soluciones de seguridad perimetral y lógica de última generación, mediante el uso de firewalls de próxima generación, WAF (Web Application Firewall), sistemas de prevención de intrusiones (IPS/IDS) y otros dispositivos de inspección profunda de tráfico (DPI). Estas soluciones permitirán el monitoreo continuo, la detección proactiva de amenazas, la generación automatizada de alertas y la gestión integral de incidentes de seguridad, protegiendo la confidencialidad, integridad y disponibilidad de la información.
6. **Software de monitoreo centralizado:** Será necesario contar con sistemas operativos estables y seguros, así como software especializado para el monitoreo y administración centralizada del sistema. Dicho software deberá

permitir observar el estado de la infraestructura en tiempo real, generar reportes de desempeño, administrar recursos, controlar eventos críticos, facilitar el análisis predictivo del comportamiento del sistema y apoyar la toma de decisiones basada en datos.

7. **Respaldo, recuperación de desastres y continuidad del negocio:** Deberá garantizarse la disponibilidad de mecanismos de respaldo (*backup*) y recuperación de datos robustos, además de herramientas de continuidad operativa que aseguren la integridad, disponibilidad y trazabilidad de la información crítica durante toda la operación del SICOV. Para ello, el proveedor del Sistema deberá contar con un Plan de Recuperación de Desastres (DRP) debidamente documentado y probado periódicamente, y un Plan de Continuidad del Negocio (BCP) que asegure la resiliencia de los servicios esenciales.
8. **Provisión de hardware:** El *hardware* necesario para el funcionamiento del Sistema de Control y Vigilancia en las sedes de los CRC, será provisto, instalado, configurado y mantenido por los proveedores homologados del SICOV.

   La Superintendencia de Transporte definirá en el presente Anexo Técnico los estándares funcionales, de rendimiento y de seguridad mínimos que deberá cumplir todo el hardware necesario para la operación del SICOV en las sedes de los CRC.

2.5.3. Arquitectura de alta disponibilidad y resiliencia

La arquitectura del SICOV deberá ser diseñada bajo un esquema de alta disponibilidad en todas sus capas, que asegure el cumplimiento de los Objetivos de Tiempo de Recuperación (RTO) y de Punto de Recuperación (RPO) ante la indisponibilidad de cualquier componente. Esta arquitectura abarcará, como mínimo:

1. **Capa de infraestructura (CPD/CAPD):** Garantizar la redundancia N+1 o superior en hardware, energía y comunicaciones, conforme a los requisitos de certificación TIER III.
2. **Capa de base de datos:** Implementación de clústeres de bases de datos con replicación asincrónica entre el CPD y el CAPD, con monitoreo activo y recuperación automática.
3. **Capa de aplicación (Software SICOV):** Despliegue de las aplicaciones permitiendo la escalabilidad horizontal y la reactivación instantánea del servicio ante la caída de un nodo.
4. **Monitoreo proactivo (NOC/SOC):** Operación 24/7/365 de un sistema de monitoreo que alerte y registre cualquier degradación del servicio o latencia que pueda comprometer el cumplimiento de los Acuerdos de Niveles de Servicio (ANS).

2.5.4. Planes y objetivos de recuperación

2.5.4.1. Plan de Recuperación de Desastres (DRP)

Todo operador del SICOV debe contar con un Plan de Recuperación de Desastres (DRP) que garantice la continuidad del negocio en cualquier circunstancia que pueda afectar la disponibilidad y estabilidad de la operación y los niveles de servicio del SICOV.

El DRP deberá remitido a la Superintendencia de Transporte. Dicho Plan deberá estar suscrito por el líder del proceso de gestión de sistemas de información y tecnología y haber sido aprobado por la Gerencia.

2.5.4.2. Objetivos de recuperación (RTO y RPO) del SICOV

Dada la naturaleza crítica del Sistema de Control y Vigilancia y su impacto directo en la operación continua y diaria de los organismos de apoyo al tránsito a nivel nacional, se establecen los siguientes objetivos de recuperación:

2.5.4.2.1. Objetivo de Tiempo de Recuperación (RTO - Recovery Time Objective)

El Objetivo de Tiempo de Recuperación para el Sistema de Control y Vigilancia será de treinta (30) minutos. Esto significa que, ante cualquier interrupción o desastre que afecte la operación del SICOV a nivel de CPD/CAPD, el tiempo máximo permitido para restaurar completamente la funcionalidad del sistema y sus servicios críticos, de manera que los organismos de apoyo puedan retomar su operación, no deberá exceder de este tiempo, sin pérdida significativa de datos. Este RTO aplica a todas las funcionalidades esenciales que soportan la prestación de servicios a los usuarios y las actividades de vigilancia de la Superintendencia.

El parámetro de treinta (30) minutos aplicará al CPD, mientras que para sus componentes distribuidos que hagan parte de la infraestructura descentralizada será de cuatro (4) horas.

El RTO (30 minutos) se refiere al tiempo máximo de indisponibilidad y recuperación del sistema transaccional principal. El parámetro de recuperación de análisis de datos (1 hora) se refiere al tiempo máximo para la reanudación total del procesamiento de las herramientas de Business Intelligence y analítica que dan soporte a la IVC.

2.5.4.2.2. Objetivo de Punto de Recuperación (RPO - Recovery Point Objective)

El Objetivo de Punto de Recuperación para el Sistema de Control y Vigilancia será de diez (10) minutos. Esto implica que, en caso de cualquier incidente o desastre, la cantidad máxima de datos que se permite perder es muy baja. Todas las transacciones y la información generada y procesada por el SICOV deberán ser replicadas y sincronizadas en tiempo real, garantizando que no haya pérdida de información crítica entre el momento del incidente y el punto de recuperación. Este RPO de diez (10) minutos es fundamental para la integridad y trazabilidad de los procesos de control y vigilancia.

2.5.4.3. Plataforma de Disaster Recovery

El homologado deberá incorporar dentro de su solución tecnológica una herramienta de recuperación critica con niveles de igual forma, herramientas que permitan generar políticas de Backup a los servidores, almacenamiento y ambientes virtualizados.

2.5.4.4. Parámetro objetivo de recuperación de análisis de datos

Se deberá garantizar reanudación completa del procesamiento de datos en menos de una (1) hora.

2.5.5. Centro de Procesamiento de Datos (CPD) y Centro Alterno de Procesamiento de Datos (CAPD)

2.5.5.1. Objetivo y estructura

El proveedor del SICOV deberá implementar y operar un Centro de Procesamiento de Datos (CPD) principal y un Centro Alterno de Procesamiento de Datos (CAPD), que constituyan la infraestructura centralizada para el alojamiento, procesamiento y resguardo de la información del SICOV. El CPD y CAPD se componen de servidores, bases de datos, canales de comunicación, dispositivos de red y de seguridad, y el personal encargado de la gestión de estos recursos.

2.5.5.2. Requisitos generales y certificación

El CPD y CAPD del SICOV (principal y alterno) deben cumplir como mínimo con lo establecido para la certificación como **TIER III**. La condición de operación de

estos centros deberá ser **activo-pasivo**. La infraestructura tecnológica de los dos CPD debe estar instalada en dos sitios geográficamente diferentes. Los recursos del CPD y CAPD destinados a la operación del Sistema de Control y Vigilancia de CRC, cuyas características se detallan a continuación, deben ser de uso exclusivo.

2.5.5.3. Recursos de cómputo y procesamiento

El CPD/CAPD deberá tener como mínimo las siguientes capacidades de cómputo para la operación:

- **Servidores:** Equipos tipo servidor de rack, de tipo empresarial y de alta disponibilidad, organizados en granjas de servidores físicos y/o virtuales. Deberán contar con procesadores multinúcleo de alto rendimiento de última generación (CPU) y aceleradores gráficos (GPU) para cómputo de propósito general (GPGPU) con soporte a tecnologías como CUDA o Tensor Cores, para ejecutar cargas de inteligencia artificial, inferencias y análisis en tiempo real de datos.
- **Arquitectura de software:** La infraestructura deberá ser compatible con plataformas de virtualización y deberá permitir la implementación de entornos de contenedorización y orquestación basados en Kubernetes para garantizar escalabilidad, despliegue automatizado, balanceo de cargas y una gestión eficiente de los recursos computacionales. Los servidores también deberán ser compatibles con entornos de ejecución que soporten arquitecturas basadas en microservicios, facilitando la implementación de pipelines de procesamiento distribuido y la integración con herramientas de DevOps, CI/CD y gestión de clústeres. El sistema de virtualización se debe comportar como una nube privada.
- **Resiliencia y tolerancia a fallos:** El sistema debe garantizar tolerancia a fallos, auto-recuperación de servicios y escalabilidad horizontal dinámica, permitiendo el aprovisionamiento y redistribución automática de cargas en función de la demanda de procesamiento analítico o de inferencia.
- **Soporte:** Todos los componentes de hardware y software instalados en el CPD, CAPD y SOC deben contar con contratos de soporte vigentes con los fabricantes o proveedores autorizados y contar con los mantenimientos correspondientes al día.

Los ciclos de obsolescencia y renovación tecnológica de la infraestructura del CPD y CAPD serán de cinco (5) años, o por el tiempo que el fabricante brinde soporte para dicha tecnología. Estos procesos de actualización estarán bajo supervisión de la Superintendencia de Transporte.

2.5.5.4. Requerimientos de almacenamiento

El sistema de almacenamiento del CPD/CAPD deberá garantizar el acceso de alta velocidad y baja latencia para operaciones críticas en tiempo real.

- **Almacenamiento de datos en tiempo real (SAN):** Se debe garantizar una arquitectura de almacenamiento tipo SAN (Storage Area Network) de nivel empresarial. Sus principales características serán:

    - Arquitectura redundante 2N o superior, con controladoras duales activo-activo o activo-pasivo.
    - Conectividad de alta velocidad mediante canales de fibra.
    - Soporte para volúmenes compartidos multi-host con compatibilidad con hipervisores.
    - Utilización de unidades NVMe y/o SSD SAS de alto rendimiento.
    - Capacidad de escalar horizontal y verticalmente.
    - Integración con sistemas de respaldo en línea y replicación síncrona/asincrónica entre sitios para garantizar la continuidad operativa.

- **Almacenamiento de Información en Reposo (NAS):** El subsistema NAS (Network Attached Storage) será destinado al almacenamiento de

grandes volúmenes de información en reposo, incluyendo registros históricos, datos procesados y respaldos de largo plazo. Sus características clave incluirán:

- Arquitectura escalable basada en clúster, con soporte de protocolos de red estándar como NFS v4, SMB 3.1.1 y FTP/SFTP.
- Discos de tipo SATA III de alta capacidad.
- Mecanismos de protección de la información como RAID 6 o Erasure Coding, snapshots y replicación diferencial a otras ubicaciones o a nube privada.
- Interfaz de administración unificada que permita monitoreo en tiempo real, asignación de cuotas y control de accesos.
- Soporte para auditoría y trazabilidad conforme a esquemas de seguridad y cumplimiento normativo.

2.5.5.5. Requerimientos de bases de datos

El sistema deberá contar como mínimo con un modelo de base de datos diseñado para soportar operaciones intensivas de consulta, almacenamiento estructurado y no estructurado, y procesamiento analítico en tiempo real.

- **Arquitectura:** Deberá estar basado en una arquitectura distribuida, desplegable sobre entornos virtualizados y/o contenedorizados (Kubernetes), permitiendo su escalado automático.
- **Tipos de bases de datos:** La plataforma debe soportar bases de datos relacionales (SQL) para garantizar integridad referencial y consistencia ACID, y bases de datos NoSQL para soportar grandes volúmenes de datos semiestructurados y consultas de alta velocidad.
- **Alta disponibilidad y tolerancia a fallos:** Deberá garantizar la disponibilidad continua de los datos mediante mecanismos como replicación síncrona y/o asíncrona entre nodos, con soporte para recuperación automática ante fallos (failover automático).
- **Despliegue y Respaldo:** Debe permitir el despliegue sobre volúmenes persistentes gestionados por Kubernetes.

2.5.5.6. Seguridad y gobernanza de datos

La solución deberá contemplar medidas de protección de la información, tanto física como lógica.

- **Seguridad Física y Lógica:** Deberá contar con dispositivos de seguridad de red actualizados, incluyendo Firewall de Nueva Generación (NGFW), WAF (Web Application Firewall), IDS/IPS, Protección de endpoint para servidores, protección contra ataques de denegación de servicio distribuido (DDoS) y VPN Segura. La protección contra ataques DDoS deberá garantizarse mediante los módulos de prevención (IPS, rate-limiting, y detección de anomalías) integrados en los firewalls perimetrales (NGFW) del CPD y CAPD, habilitados y configurados según lineamientos de la Superintendencia..
- **Cifrado de Datos:** Deberá implementarse un cifrado robusto de datos en tránsito (TLS 1.2 o superior) y en reposo (AES-256).
- **Protección de datos biométricos:** Se deben implementar controles de protección de datos como el almacenamiento seguro en repositorios cifrados y segmentados, el uso de técnicas como hash biométrico o plantillas encriptadas, y una trazabilidad completa de accesos a la biometría con auditorías y alertas.
- **Control de acceso y auditoría:** La solución deberá contemplar control de accesos basado en roles (RBAC), autenticación multifactor y auditoría de accesos. Se requiere monitoreo continuo de la seguridad.

2.5.5.7. Resiliencia y recuperación

El CPD/CAPD deberá garantizar la recuperación del servicio y la información en caso de contingencia.

- **Respaldo y recuperación:** El sistema debe usar herramientas para realizar copias de seguridad/backups en entornos seguros tales como unidades de cinta, dispositivos NAS, almacenamiento en la nube, o PBBA. Deberá contar con mecanismos de respaldo automatizado y programado con una retención mínima de 90 días hábiles, replicación en el CAPD (activo-pasivo), y gestión de snapshots y puntos de restauración.
- **Plan de respaldo:** El proveedor deberá contar con un plan de respaldo de la información que defina la selección de datos, frecuencia de copias, métodos, medios de almacenamiento y pruebas de recuperación. Al menos una copia deberá ubicarse fuera del sitio del CPD, CAPD y la sede del proveedor.
- **Energía y Redundancia Eléctrica:** El sistema eléctrico debe contar con un sistema redundante N+1 para UPS y plantas eléctricas. Se requiere un respaldo mínimo de 96 horas de energía. El sistema de transferencia automática de potencia no debe tomar más de 10 segundos.

2.5.5.8. Condiciones físicas y ambientales

La ubicación y la estructura física del CPD/CAPD deberán cumplir con requisitos de seguridad y control ambiental.

- **Ubicación y diversificación:** Tanto el CPD principal como el Alterno deberán estar ubicados en territorio nacional.
- **Control de acceso físico:** Se requerirá control de acceso y seguridad perimetral, con sistema de control biométrico y clave, acceso y control de ingreso mediante portería y sistema de autorización personal con guardias 7x24x365.
- **Sistemas de protección:** El CPD debe contar con CCTV, un sistema de detección, notificación y extinción de incendios con agente limpio, un sistema de pararrayo**s**, y control de condiciones ambientales.
- **Infraestructura de cableado:** Deberá contar con piso falso o un sistema de distribución aérea o elevada de bandejas porta cables, con materiales incombustibles y retardantes al fuego, y los racks, gabinetes y bandejas porta cables deben contar con conexión a tierra.
- **Sistema de aire acondicionado:** Se suministrará, instalará y dejará en perfecto funcionamiento, aires acondicionados requeridos los cuales serán instalados en los centros de cableado y racks de los equipos.
- **Sistema de medición de condiciones ambientales:** Se deben instalar los sistemas necesarios para medir las condiciones de temperatura y humedad dentro del centro de cableado y racks de los equipos.

2.5.5.9. Soporte remoto y gestión de servicios

El proveedor deberá garantizar la atención oportuna de incidencias y requerimientos.

- **Servicio de manos remotas:** Deberá proveer un servicio de manos remotas de mínimo 5 horas mensuales, con una disponibilidad de 24x7x365.
- **Mesa de Ayuda (Help Desk):** Deberá contar con un sistema de información WEB para Mesa de ayuda, con un plan de comunicaciones para atención de incidentes, un formulario de solicitudes vía web y la consulta del histórico de casos.

2.5.5.10. Desarrollo y gestión de aplicaciones

- **Ambientes:** El CPD deberá disponer de la infraestructura requerida para crear e implementar ambientes independientes para desarrollo de software, pruebas y producción.
- **Herramientas y automatización:** Deberá contar con herramientas para la gestión de contenedores y orquestadores (Docker, Kubernetes, OpenShift) y gestionar la integración con herramientas de desarrollo colaborativo, control de versiones y y automatización CI/CD.

2.5.6. Red de Comunicaciones

2.5.6.1. Canal de internet del operador homologado

El proveedor homologado deberá disponer de un canal de internet dedicado para CRC que permita la interacción entre la infraestructura central del SICOV y estos organismos de apoyo.

Para la conectividad con los CRC, se requiere que la velocidad de conexión a internet dedicado sea del mínimo requerido para garantizar una operación eficiente del sistema central y en todo caso no podrá ser inferior a 200 MB simétricas o dedicado 1:1, con conectividad redundante provista por diferentes proveedores de servicio de internet (ISP).

2.5.6.2. Canal de internet del CRC y requisitos del canal de conexión

Para la correcta ejecución de la plataforma, la transmisión que asegure alta disponibilidad y seguridad controlada, con el fin de poder realizar de una forma fluida las validaciones biométricas y la estabilidad de la operación, cada sede de los CRC deberá contar con:

Un servicio de acceso a internet con un ancho de banda garantizado (reuso 1:1) mínimo de veinte (20) Megabits por segundo (Mbps), simétrico, garantizando respaldo y contingencia en alta disponibilidad que garantice la transmisión de video en tiempo real. Este canal deberá ser de uso exclusivo o prioritario para la operación del SICOV, evitando su saturación por tráfico no autorizado. El canal debe garantizar una capa de conectividad segura punto a punto con la infraestructura central del SICOV.

El proveedor de internet deberá instalar dos canales de datos tipo MPLS con la posibilidad de acceso a internet, en configuración de activo-activo, 7x24x365 bajo la modalidad de configuración dual homing. El proveedor deberá suministrar e instalar en cada CRC un (1) equipo de borde UTM donde deberán confluir las conexiones del servicio ofrecido.

Para garantizar la máxima disponibilidad del servicio, el proveedor deberá garantizar que tiene capacidad contratada de salida a internet internacional al menos por dos rutas, una por un cable submarino del océano Pacífico y la otra por un cable submarino del océano Atlántico.

El proveedor deberá certificar conexión directa con cada uno de los miembros del NAP para intercambio de tráfico local en Colombia, posibilitando el establecimiento de peering (intercambio entre proveedores de tráfico) con cada uno de los miembros del NAP, con el fin de garantizar una conexión directa con rápido acceso y enrutamiento del tráfico que sea recibido o generado hacia o desde destinos nacionales.

El servicio deberá contar con al menos una dirección IP pública fija dedicada, la cual deberá ser registrada en el SICOV (listas blancas) para autorizar exclusivamente el tráfico proveniente de la sede habilitada.

2.5.6.3. Seguridad de la información en tránsito:

El operador homologado del SICOV deberá exigir protocolos de seguridad para toda la comunicación entre los organismos de apoyo y la infraestructura central, incluyendo obligatoriamente:

Toda transmisión de datos deberá realizarse a través de túneles cifrados (VPN) o protocolos de seguridad de capa de transporte (TLS 1.2 o superior) que aseguren la confidencialidad e integridad de la información.

Autenticación de dispositivos: El sistema deberá validar que la conexión provenga de los equipos y la dirección IP autorizados, rechazando automáticamente conexiones desde redes no certificadas.

Latencia: Se deberá garantizar una latencia máxima de 20 ms hacia los servidores del SICOV.

Los CRC tendrán libertad para contratar el servicio de conectividad con cualquier proveedor de redes y servicios de telecomunicaciones (PRST) legalmente constituido en el país, siempre que este cumpla con los niveles de servicio (SLA) técnicos aquí descritos.

El cumplimiento de las exigencias de conectividad segura requeridas para los canales de internet de los CRC será supervisado por la Superintendencia de Transporte a través del SICOV.

El proveedor de internet contratado por cada CRC deberá implementar el servicio de DNS en entorno privado de red, que permita la implementación de funcionalidades y políticas de seguridad como:

- Bloqueo de APPs.; Bloqueo IPs, DoH (DNS encriptado).
- Geoblocking.
- Bloqueo de sitios de directiva nacional emitidos por el Ministerio de las TIC y otras entidades que lo requieran.
- Bloqueo de listas personales.
- Protección malware, blacklist; Control parental.
- Análisis y reportes en tiempo real.
- Nivel de calidad mínimo: 99.7% tiempo de atención a fallas en sitio, después de parada de reloj inferior a 4 horas.
- Pérdida de paquetes: Garantizar una perdida menor o igual al 0.3% hasta la salida a internet internacional.
- Latencia: Garantizar una latencia menor o igual a 20 milisegundos desde la red interna del CRC hasta el NAP.

Soporte y mantenimiento

El proveedor de comunicaciones contratado por cada CRC deberá operar y mantener la solución instalada sin que este incurra en costos adicionales. Se deben incluir al menos los siguientes puntos:

- Un centro de servicio al cliente 7x24x365.
- La apertura y seguimiento de servicios solicitados (llamadas), con manejo de prioridades de llamadas.
- Generar indicadores, reportes de tráfico y estadísticas de forma mensual, que registren el tráfico del canal utilizado y la capacidad de este.

Acuerdos de Niveles de Servicio: Se deberán asegurar como máximo los siguientes tiempos para la atención a fallas:

Desconexión total del Servicio: 1 Hora.

Operación degradada del servicio: 2 Horas.

Fallas intermitentes: 3 Horas.

2.5.6.4. Conectividad en CPD y CPAD:

Para garantizar la conectividad, los CPD y CPAD deberán contar con equipos de comunicaciones con las siguientes características como mínimo:

- **Switches de Red:**
    - Nivel 3 Administrable
    - 24 puertos Fast Ethernet, velocidad 10/100/1000 Mbps
    - Cifrado integrado por capa de sockets seguros (SSL)
    - Manejo de listas de control de acceso (ACL)
    - Funcionalidad VLAN
    - Permita la inspección dinámica del protocolo de resolución de direcciones (ARP), protección de IP de origen y detección del protocolo DHCP, que permiten detectar y bloquear ataques deliberados de la red.
    - Compatibilidad con IPv6.

2.5.7. Operación técnica de la Mesa de Ayuda

La Mesa de Ayuda debe contar con una herramienta o software que soporte la gestión de los siguientes canales de atención, asegurando su accesibilidad tanto para usuarios técnicos como para usuarios sin conocimientos especializados en tecnología:

- Chat en tiempo real con soporte.
- Atención telefónica.
- Chatbot inteligente.
- Correo electrónico.
- WhatsApp.
- Atención en los sitios web del operador homologado.

2.5.7.1. Procesos y gestión operativa

El homologado deberá garantizar la implementación y el cumplimiento de los siguientes procesos documentados para la operación de la Mesa de Ayuda:

Manual y procedimiento de atención: Disponer de un manual y procedimiento detallado para la atención al usuario.

Clasificación de peticiones: Disponer de un manual o procedimiento para la correcta clasificación de las peticiones realizadas.

Priorización de peticiones: Disponer de un manual o procedimiento para la adecuada priorización de las peticiones realizadas.

Gestión de tickets: Por cada incidencia o solicitud que presente un organismo de apoyo al tránsito, se creará un ticket en la Mesa de Ayuda, a través de una herramienta de gestión de tickets. Los tickets creados deberán escalar hasta que el operador homologado brinde una solución o respuesta aceptable y/o cierre el caso luego de haber hecho la gestión correspondiente con el usuario.

2.5.7.2. Gestión del conocimiento y capacitación

El proveedor deberá asegurar la constante actualización del conocimiento y la capacitación, tanto para su personal de Mesa de Ayuda como para los usuarios del SICOV:

Capacitación de Analistas: Capacitar permanentemente a los analistas de la Mesa de Ayuda sobre el software del Sistema de Control (incluyendo sus

versiones y actualizaciones), y sobre el uso y soporte de los dispositivos de hardware y software asociados a la operación del SICOV.

Manual de uso del SICOV: Disponer de un manual de uso del SICOV para orientar al usuario sobre las funcionalidades y casos de uso del SICOV.

Módulo de preguntas frecuentes (FAQ): Disponer de un módulo de preguntas frecuentes y actualizadas, accesible para el personal de los organismos de apoyo al tránsito que interactúan con el SICOV.

Material de orientación: Diseñar material gráfico y multimedia para orientar al personal que interactúa con el SICOV.

Planes de divulgación y capacitación: Contar con planes de divulgación y capacitación sobre el uso del sistema y las novedades.

2.5.8. Software de gestión y control de información del Sistema de Control y Vigilancia para Centros de Reconocimiento de Conductores

El Sistema de Control y Vigilancia contará con una solución de software que, ejecutándose en la infraestructura centralizada del operador homologado y en las sedes de los Centros de Reconocimiento de Conductores, permita capturar, procesar, gestionar y analizar la información, y llevar trazabilidad integral de su operación, en cada una de las etapas de la prestación del servicio de examen de aptitud física, mental y de coordinación motriz, bajo los parámetros definidos por la Superintendencia de Transporte. La parametrización precisa y segura de este Sistema permitirá vigilar y controlar el cumplimiento de las obligaciones de este grupo de vigilados, previniendo activamente el fraude y asegurando la integridad de los resultados.

Funcionalidades tecnológicas del software del SICOV para los Centros de Reconocimiento de Conductores:

Introducción

El presente capítulo describe las funcionalidades y capacidades tecnológicas que el Sistema de Control y Vigilancia deberá proveer para su operación en todos los Centros de Reconocimiento de Conductores.

2.5.8.1. Gestión del registro de información de los Centros de Reconocimiento de Conductores y administración de su identificador único ante la RNEC (IDClient).

El Sistema de Control y Vigilancia deberá disponer de las funcionalidades necesarias para gestionar el registro inicial y mantener permanentemente actualizada la información completa de cada Centro de Reconocimiento de Conductores. Este registro integral incluirá, como mínimo, los siguientes datos:

a) Identificación legal y comercial: Nombre o razón social completa; Número de Identificación Tributaria (NIT); y, conforme a su naturaleza jurídica, el número de matrícula mercantil vigente.

b) IDRUNT: Código ID asignado en el Registro Único Nacional de Tránsito (IDRUNT).

c) Ubicación y contacto: Departamento, municipio, dirección detallada y georreferenciada de su sede habilitada; números de teléfono de contacto actualizados; y direcciones de correo electrónico institucional designadas para notificaciones oficiales.

d) Representación legal: Información completa y vigente del representante legal principal y de los suplentes registrados, incluyendo nombres y apellidos

completos, tipo y número de documento de identidad. A través del mecanismo de interoperabilidad disponible entre operadores homologados, se consultará automáticamente si dicha(s) persona(s) figura(n) con la representación legal de otro(s) organismo(s) de apoyo al tránsito. El resultado de dicha consulta quedará registrado y estará disponible para consulta de la Superintendencia de Transporte en el CPD Analítico y de información.

e) Detalles operativos y de habilitación: Horarios de atención al público para cada sede; y la información detallada (número, fecha de expedición, entidad emisora y vigencia) de la resolución de habilitación expedida por el Ministerio de Transporte, en su defecto o de forma complementaria, la constancia que acredite su registro activo y habilitado en el RUNT.

f) Número de identificador único ante la RNEC (IDClient). El proveedor del Sistema procederá con el registro y la gestión centralizada del número único de IDClient asignado por la Registraduría Nacional del Estado Civil a cada CRC. Este IDClient es indispensable para que en el CRC se pueda realizar, a través del SICOV y del operador biométrico autorizado por la RNEC, las verificaciones de identidad mediante cotejo de huella dactilar y/o cotejo por reconocimiento facial contra las bases de datos de dicha entidad.

1. El registro de toda la información sobre el IDClient de cada CRC en el SICOV deberá estar respaldado por la constancia oficial de asignación expedida por la RNEC, a través de correo electrónico o el medio del que disponga esa entidad.
2. La parametrización del Sistema validará que ningún CRC se registre con el IDClient de otro organismo de apoyo. Esto implicará prioritariamente la consulta a través de mecanismos de interoperabilidad con todos los operadores homologados del SICOV.
3. El proveedor del SICOV, a través de su operador biométrico, debe garantizar la prestación del servicio mientras el IDClient del CRC se mantenga activo.
4. Como medida para prevenir la duplicidad de registros, el SICOV, a través de su operador, deberá implementar un mecanismo de verificación, al momento del registro o vinculación de un CRC, para constatar si dicho organismo de apoyo ya cuenta con un número de IDClient activo y previamente registrado en el Sistema SICOV para la prestación de servicios. De ser ese el caso, el SICOV debe asegurarse de que el operador biométrico con el que tenga relación contractual sólo pueda realizar consultas contra las bases de datos de la RNEC una vez quede efectuada formalmente la desvinculación del CRC con el operador del SICOV con el que tenga vínculo.

   Esto implica la consulta a través de mecanismos de interoperabilidad con todos los operadores homologados. Cualquier inconsistencia o posible duplicidad detectada deberá ser reportada a la Registraduría Nacional del Estado Civil y a la Superintendencia de Transporte para su debida gestión.

g) Constancia de registro en el Sistema Inteligente Nacional de Supervisión al Transporte – VIGIA 2. El Sistema registrará el soporte de registro exitoso del CRC en el Sistema Inteligente Nacional de Supervisión al Transporte – VIGIA 2.

h) Información adicional requerida: Cualquier otra información, dato o documento que la Superintendencia de Transporte determine como necesario. El Sistema deberá ser tecnológicamente flexible para permitir la incorporación y gestión estructurada de estos campos o documentos adicionales.

i) Generación de hash para la integridad de los datos: El Sistema de Control y Vigilancia deberá generar un hash criptográfico de cada registro de datos para garantizar su inalterabilidad y la integridad de la información. Este proceso se aplicará obligatoriamente a:

- Los registros de cada validación de identidad (exitosa o fallida) de los usuarios, personal de la salud y certificadores, al inicio y al final de cada evaluación o cada examen, y del momento de certificación.
- Los resultados de las evaluaciones o exámenes.

La herramienta deberá permitir cotejar el hash original de cualquier registro para verificar que no ha sido modificado.

Los Centros de Reconocimiento de Conductores deberán reportar al SICOV cualquier cambio o actualización de su información de registro u operación dentro de los cinco (5) días hábiles siguientes a su ocurrencia, sin perjuicio de las actualizaciones automáticas que se realicen por parte del operador homologado del Sistema conforme a lo descrito en el presente Anexo.

2.5.8.2. Gestión de enrolamiento, validación biométrica y activación de servicios.

El SICOV deberá disponer de un módulo especializado para el enrolamiento y la gestión de la identidad de los usuarios, el cual operará bajo un esquema híbrido que permita tanto la atención en sede como la autogestión digital, cumpliendo las siguientes condiciones:

1. **Enrolamiento presencial:** Para los usuarios que inician su trámite directamente en la sede del CRC, el sistema realizará el enrolamiento mediante la captura de datos biográficos, la digitalización del documento de identidad, la captura de las huellas dactilares para el cotejo biométrico contra la Base de Datos de la Registraduría Nacional del Estado Civil y la validación de identidad a través de reconocimiento facial, conforme a los protocolos que se establecen en los numerales subsiguientes del presente anexo.

2. **Pre-enrolamiento digital y activación**: Con el fin de facilitar el acceso, y permitir el agendamiento web, el SICOV habilitará para todos los CRC una funcionalidad de Pre-enrolamiento digital. Este proceso permitirá la creación preliminar del registro del usuario de manera remota, vía app o web, mediante:

   - La captura de datos biográficos.
   - La validación documental del documento de identidad original mediante tecnología OCR y lectura de códigos (MRZ/PDF417) con detección de prueba de vida del documento.
   - La captura biométrica facial con prueba de vida (liveness detection) para generar un registro temporal.

3. **Activación del servicio:** El usuario pre-enrolado podrá realizar el pago y la reserva de citas. Sin embargo, para hacer efectivo el servicio y dar inicio al examen, el usuario deberá presentarse en la sede del organismo con una antelación mínima de treinta (30) minutos a la hora programada para completar el enrolamiento.

El Enrolamiento se completará con la validación biométrica obligatoria en sitio (huella dactilar contra RNEC). Una vez surtida esta validación, el sistema activará automáticamente la cita agendada, permitiendo la ejecución del servicio y garantizando que quien agendó digitalmente es la misma persona que asiste a la sede.

2.5.8.3. Gestión y registro de pagos de servicios de examen de aptitud física, mental y de coordinación motriz.

El Sistema deberá facilitar y garantizar el registro seguro del pago de la tarifa correspondiente a la capacitación en conducción y la eventual certificación del usuario. Este proceso incluirá el manejo de los valores asociados que deban ser distribuidos a terceros autorizados, y se articulará mediante la generación de un

número único de identificación de pago (PIN), el cual estará obligatoriamente asociado al número de documento de identidad del usuario.

a) Condicionamiento para el pago: Como medida para prevenir el fraude, el SICOV, a través del recaudador, solo habilitará la generación del número único de identificación de pago (PIN) para un examen de aptitud física, mental y de coordinación motriz después de haber verificado de manera automática y en tiempo real, si el aspirante ha sido evaluado y examinado por otro CRC registrado en el SICOV.

Adicionalmente, el PIN de pago sólo podrá ser generado por parte del operador de recaudo una vez exista constancia del pago efectivo y de la aprobación de la transacción por el valor completo del servicio más los valores cobrados por los servicios de terceros. De lo anterior deberá quedar trazabilidad en los registros (logs) del SICOV.

b) Mecanismo de verificación: Esta verificación se realizará mediante la interoperabilidad o integración que el SICOV para CRC deberá garantizar con los demás operadores homologados.

En los casos en que la consulta de interoperabilidad arroje como resultado que el usuario fue calificado como "no apto" en otro CRC, el Sistema habilitará la generación del PIN de pago pero marcará el servicio con una alerta que será visible para la Superintendencia en el MOCVI del CPD Analítico y de Identificación y el CRC al que acuda el usuario, permitiéndole conocer inmediatamente el motivo de rechazo en el(los) anterior(res) Centro de Reconocimiento y las restricciones de salud registradas, conforme a la información disponible en el SICOV. Esta información quedará en la trazabilidad histórica de la prestación del servicio al usuario.

Los servicios marcados por esta causa serán objeto de seguimiento especial por parte de la Superintendencia de Transporte, con el apoyo de los operadores homologados. Para tal efecto, se analizarán las evidencias de estos servicios prestados. La Superintendencia podrá fijar condiciones específicas adicionales para la verificación de estas evidencias y la definición de planes de seguimiento a los CRC.

c) Trazabilidad del recaudo: El SICOV deberá registrar la información de la transacción y la entidad que procesó el recaudo. Para tal efecto, el operador de recaudo deberá transmitir al software del SICOV, de manera inmediata y automatizada, a través de un mecanismo de interoperabilidad o integración que se desarrolle, la información precisa del pago recibido en su cuenta por parte del usuario del servicio o de quien lo realice en nombre suyo, discriminando los valores dispersados o a dispersar a cada uno de los terceros, así como el tipo y número de documento de identidad del usuario que tomará el servicio, fecha y hora del ingreso del pago, e identificación (nombre, tipo y número de documento) de la persona natural representante de la persona que realizó el pago.

e) Facilidades de pago: El sistema permitirá que el usuario pueda hacer el pago del servicio y los pagos a terceros a través de pasarelas de pago y por intermedio del recaudador.

f) Vigencia del PIN de pago: Para garantizar la transparencia y la correcta conciliación de los recursos, se establece que el PIN de pago generado por el servicio de recaudo tendrá una vigencia máxima de quince (15) días. Cumplido este plazo, si el PIN no ha sido consumido para la prestación del servicio de examen de aptitud, el SICOV habilitará su anulación, la cual será ejecutada por el operador de recaudo dentro de los cinco días siguientes a la habilitación de anulación, quien deberá a su vez efectuar la devolución del valor de la transacción inicial al usuario a través del mismo medio de pago que este haya usado o que autorice para el efecto, de acuerdo con el procedimiento que se haya definido.

g) Integración transaccional para agendamiento en línea: Con el fin de facilitar el comercio electrónico y la autogestión del usuario, se permite el inicio de pagos desde plataformas de agendamiento web o móviles.

Para garantizar la correcta dispersión de los recursos, la pasarela de pagos o el botón de pago dispuesto en dichas plataformas deberá enrutar la transacción directamente hacia el aliado de recaudo autorizado por el operador homologado, o integrarse tecnológicamente con este.

Queda establecido que el recaudo final y la generación del PIN solo se considerarán válidos cuando la transacción haya sido procesada y confirmada exitosamente dentro del ecosistema financiero del aliado de recaudo autorizado, asegurando así que los recursos ingresan al sistema financiero formal y se dispersan automáticamente a las cuentas de los actores correspondientes en tiempo real o en los ciclos bancarios definidos.

2.5.8.4. Registro y almacenamiento seguro de información y datos personales.

Previa autorización expresa e informada del titular de los datos, y luego de la validación de identidad contra las bases de datos de la RNEC, conforme a lo descrito en el siguiente numeral, el SICOV deberá registrar y almacenar de forma segura la información personal de cada usuario del servicio y del personal vinculado al organismo de apoyo (tales como personal administrativo, profesionales de la salud y personal certificador) que interactúen con el Sistema. Este registro, que se realizará al momento del enrolamiento inicial, incluirá, como mínimo, lo siguiente:

a) Información del documento de identidad: Para el enrolamiento inicial para la prestación de un servicio, es obligatoria la presentación del documento de identidad original válido en Colombia. La información personal básica contenida en el anverso y reverso del documento será capturada digitalmente mediante dispositivos con cámaras o escáneres de alta resolución, su información extraída con tecnología de Reconocimiento Óptico de Caracteres (OCR) y lectura de Zona de Lectura Mecánica (MRZ) y su autenticidad verificada con prueba de vida (tecnología Document Liveness Detection), para asegurar que se trata del documento físico original y no de una fotografía, fotocopia o imagen digital. Esto se hará a través del uso de tecnología especializada como se describe en este Anexo Técnico, o superior.

b) Fotografía de referencia capturada en vivo (template): Una fotografía digital a color del rostro del individuo, capturada en el establecimiento del organismo de apoyo durante su enrolamiento. Dicha fotografía deberá ser tomada con cámaras de alta definición bajo condiciones que aseguren su calidad y compatibilidad con tecnologías de reconocimiento facial (ICAO) que cumplan con los estándares de precisión, fiabilidad y detección de vida (liveness detection) definidos en este Anexo Técnico. Para tal efecto, la fotografía deberá capturarse obligatoriamente con fondo unicolor neutro (blanco o gris claro), garantizando un alto contraste.

Esta fotografía será almacenada una vez se dé cumplimiento al siguiente procedimiento:

1. Primero se verificará la autenticidad del documento de identidad presentado por el usuario con la tecnología MRZ OCR + PDF 417.
2. Sólo si el resultado de validación de autenticidad del documento de identidad es positivo, se realizará una validación biométrica de identidad de la persona con el software o tecnología de reconocimiento facial, comparando el rostro de la persona presente en sitio, contra la foto del documento de identidad original validado (selfie vs. documento).
3. Sólo si esta validación de identidad es exitosa, la selfie o fotografía capturada para esa validación específica será la que se utilice para

la creación del único patrón biométrico (template) de referencia para los procesos internos y posteriores de validación de identidad que se realicen mediante la tecnología de reconocimiento facial del SICOV (antes, durante y después de la finalización de la sesión), como se detalla más adelante.

Con las fotografías de referencia (template) y la información biográfica de los usuarios se construirá un **Sistema Automatizado de Identificación Biométrica (ABIS) Facial** que servirá para todos los enrolamientos y validaciones de identidad que se realicen posteriormente al mismo usuario en otros organismos de apoyo al tránsito, para cualquier propósito: evaluar la aptitud física, mental y de coordinación motriz en un Centro de Reconocimiento de Conductores; capacitación en un Centro de Enseñanza Automovilística para obtener una licencia de conducción; capacitación en un Centro Integral de Atención u Organismo de Tránsito y Transporte para obtener un descuento en el valor de una multa por una infracción de tránsito; y para la realización de una evaluación teórica y práctica en un Centro de Apoyo Logístico para la Evaluación.

Este ABIS se alojará en el CPD Analítico y de Identificación cuyas características se detallan más adelante.

c) Consulta del ABIS Facial

El funcionamiento del ABIS seguirá las siguientes reglas:

- **Unicidad del template biométrico:** El sistema almacenará un único patrón biométrico (template) de referencia por cada usuario. Sin perjuicio de lo anterior, cada vez que sea actualice un template biométrico de un usuario, el sistema generará un log con la información y trazabilidad del cambio.
- **Consulta y reutilización en la red:** Cuando un CRC realice el escaneo del documento de identidad de un usuario, el SICOV consultará automáticamente al Subsistema ABIS central.
- El uso de patrones biométricos existentes para cotejos en diferentes organismos de apoyo al tránsito se limita exclusivamente a la validación de identidad del usuario.

Si el usuario ya existe en el ABIS, el sistema habilitará el mecanismo de validación biométrica de identidad usando para ello la tecnología de reconocimiento facial (selfie vs template).

De resultar exitosa la validación, se actualizará el template del usuario en el ABIS, almacenando la última selfie como template, y se habilitará su uso para realizar todos los cotejos con reconocimiento facial posteriores (selfie vs template) requeridos durante la prestación del nuevo servicio. Además, En estos casos no se requerirá una nueva validación biométrica dactilar del usuario contra la RNEC.

En los casos en que el usuario ya exista en el ABIS, pero los intentos de validación de identidad con reconocimiento facial **no sean exitosos**, se ejecutará un proceso de validación de identidad reforzada mediante la combinación de mecanismos de verificación documental y validación biométrica contra las bases de datos de la RNEC, asegurando la trazabilidad y auditoría del proceso. Si la validación es exitosa, se actualizará la información del template del usuario en el ABIS.

Si el usuario no existe en el ABIS, se procederá con el flujo completo de enrolamiento previsto en este capítulo, registro de datos y validación de identidad contra la RNEC, así como con la creación del template del usuario en el ABIS.

d) Firma manuscrita digitalizada: La firma manuscrita capturada a través de un dispositivo digitalizador que garantice su integridad y vinculación al individuo. Este mecanismo podrá ser utilizado para la aceptación de la política de tratamiento de datos personales del SICOV, la RNEC y otros consentimientos requeridos.

La captura de la información biométrica será utilizada únicamente para la realización de las validaciones de identidad ante la RNEC y para la validación de identidad durante la prestación del servicio, previa autorización del usuario. La conformación de mecanismos de validación con dicha información para fines distintos a los dispuestos por la RNEC y que van en contra con la Ley 1581 de 2011 y sus decretos reglamentarios conllevará la imposición de las sanciones establecidas en la norma por parte de la autoridad competente.

e) Protección de datos: La captura de la información biométrica y personal será utilizada para la realización de las validaciones de identidad ante la RNEC y para la validación de identidad durante la prestación del servicio, previa autorización expresa del usuario. La conformación de mecanismos de validación con dicha información para fines distintos a los dispuestos por la RNEC y que van en contra con la Ley 1581 de 2011 y sus decretos reglamentarios conllevará la imposición de las sanciones establecidas en la norma por parte de la autoridad competente. El operador homologado para la operación SICOV deberá garantizar la custodia debida, la seguridad e integridad de esta información.

Parágrafo: Para efectos del proceso de validación de identidad a través del cotejo Selfie vs. Documento, el umbral de aprobación automática se regirá por los estándares de seguridad definidos en la Ficha Técnica del Fabricante de cada solución, bajo las siguientes condiciones:

- El proveedor tecnológico debe respetar obligatoriamente dichos niveles. Cualquier ajuste no autorizado será considerado una falta grave a la seguridad del sistema.
- No se permiten aprobaciones manuales de identidad.

2.5.8.5. Autenticación y validación de identidad contra bases de datos de la RNEC

El Sistema de Control y Vigilancia deberá asegurar que todo usuario del servicio y miembro del personal de un CRC sea enrolado en el Sistema, previo a su primera interacción. Este proceso de enrolamiento inicial tiene como finalidad establecer de manera fehaciente la identidad del individuo ante el Sistema y estará condicionado obligatoriamente, como primer paso de la fase de enrolamiento, a la superación exitosa del procedimiento de verificación de identidad de la persona contra las bases de datos biográficas (Archivo Nacional de Identificación) y biométricas de la Registraduría Nacional del Estado Civil (RNEC).

1) Momentos de validación: Este proceso fundamental de verificación se empleará:

a) Por parte de todos los usuarios del servicio y miembros del personal del CRC, al momento del primer acceso o enrolamiento formal en el Sistema.

b) Por parte de todos los usuarios y profesionales de la salud, así:

- De manera aleatoria en al el porcentaje del total de validaciones de identidad que se realizan a lo largo de la prestación del servicio, según determine la Superintendencia de Transporte, así:

    i. Para los usuarios, en cualquiera de los cuatro exámenes.
    ii. Para los profesionales de la salud, en cualquiera de los dos momentos de validación de identidad de cada examen que realicen.

- Cuando lo requiera el SICOV, de acuerdo con las especificaciones y condiciones que llegue defina la Superintendencia de Transporte.

2) Mecanismos biométricos de validación: La validación de identidad se efectuará utilizando los siguientes mecanismos biométricos, conforme a las directrices de la RNEC y la Superintendencia de Transporte:

a) Cotejo biométrico dactilar (mecanismo base): Se realizará la confrontación de las minucias dactilares utilizando, como mínimo, tecnología como la de los lectores de huella especializados aquí descritos por la Superintendencia, debidamente homologados por la RNEC, los cuales deberán contar con funcionalidad certificada de detección de dedo vivo (liveness detection), de conformidad con lo previsto por la RNEC.

b) Reconocimiento facial contra RNEC (mecanismo principal condicionado): Se empleará tecnología de reconocimiento facial como mecanismo de verificación principal, una vez esta sea reglamentada, autorizada para su uso en este contexto por la Superintendencia de Transporte y provista a través de un operador de validación biométrica debidamente habilitado. En ausencia o indisponibilidad de este mecanismo principal, mientras no esté plenamente operativo según la normativa, o mientras no sea autorizado por la Superintendencia de Transporte, se recurrirá al cotejo biométrico dactilar.

El enrolamiento de los usuarios extranjeros que se identifiquen con cédula de extranjería, pasaporte y/o Permiso de Protección Temporal (PPT), y de los usuarios menores de edad que tengan tarjeta de identidad, no se realizará contra las bases de datos de la RNEC, sino con tecnología de reconocimiento facial Selfie vs. Documento, conforme a lo descrito en el numeral anterior.

Una vez que la RNEC reglamente oficialmente el uso del reconocimiento facial, este también podrá ser implementado como mecanismo válido para la validación de identidad en la fase de enrolamiento.

c) Procedimiento en caso de no validar mediante cotejo biométrico dactilar: En los procesos de validación de identidad durante el enrolamiento en los que no se logre o no sea posible hacer una verificación exitosa mediante el cotejo biométrico dactilar contra las bases de datos de la RNEC, por parte de nacionales colombianos mayores de edad, luego de tres (3) intentos fallidos consecutivos, se deberá proceder con la aplicación del procedimiento de validación con la tecnología de reconocimiento facial Selfie vs. Documento descrita en este Anexo Técnico.

La fotografía (selfie) con la que se valide la identidad del usuario se convertirá en el template único de referencia que se utilizará a lo largo de la prestación del servicio.

d) Protocolo de inconsistencia de identidad y actualización de datos biométricos: Si tras realizar tres (3) intentos de cotejo biométrico dactilar contra la base de datos de la RNEC, y posteriormente tres (3) intentos de validación de reconocimiento facial (selfie vs. documento original), el resultado persiste como negativo o inconsistente, el sistema bloqueará de manera inmediata el inicio o la continuación de cualquier servicio de evaluación.

El CRC deberá informar al usuario que, para prestarle el servicio, deberá acudir ante la autoridad de identificación correspondiente (RNEC para ciudadanos colombianos o Migración Colombia para extranjeros) con el fin de realizar la actualización de su información biométrica y la renovación de su documento de identidad (expedición de cédula digital).

La prestación del servicio quedará suspendida. Bajo ninguna circunstancia se permitirá al usuario avanzar. Solo una vez que el ciudadano haya actualizado su información ante la autoridad competente y el SICOV logre una validación exitosa contra la fuente maestra actualizada y el nuevo documento de identidad, se podrá retomar el servicio.

El SICOV deberá almacenar los registros (logs) detallados de todos los intentos fallidos que dieron lugar a la restricción, incluyendo los motivos técnicos del rechazo, lo cual será accesible para la consulta de la Superintendencia de Transporte en el Módulo de Supervisión y Control, para fines de auditoría y detección de patrones de fraude..

2.5.8.6. Gestión del registro y control de información del personal vinculado a los CRC

El Sistema de Control y Vigilancia deberá disponer de funcionalidades para el registro detallado, la actualización permanente y el control de la información de todo el personal vinculado a los CRC, incluyendo personal de la salud, personal administrativo y directivo que interactúe con el Sistema o participe en los procesos de registro de usuarios e información, administración de recursos del CRC.

El sistema deberá registrar y mantener actualizada la información de vinculaciones y desvinculaciones, así como la historia laboral/contractual de este personal. El tratamiento de esta información se sujetará en todo momento a la Ley 1581 de 2012 y demás normas concordantes sobre protección de datos personales.

1. Registro inicial del personal y validación de identidad:

a) Todo miembro del personal deberá ser registrado en el SICOV previo al inicio de sus labores. Este registro inicial estará condicionado 1) a la superación exitosa del procedimiento de enrolamiento y verificación de identidad contra las bases de datos de la RNEC o el mecanismo alterno, conforme a lo detallado en los numerales correspondientes de este Anexo y 2) a la existencia del registro en el RETHUS del personal de la salud, cuando aplique.

b) El Sistema registrará la fecha de vinculación y, cuando ocurra, la fecha de desvinculación efectiva del personal del CRC, información que deberá ser actualizada diligentemente por el Centro de Reconocimiento de Conductores de lo cual hará seguimiento continuo el operador homologado a través del SICOV.

c) El Sistema registrará la aceptación de la política de tratamiento de datos personales, los términos y condiciones de uso del SICOV y todas sus herramientas, y un aviso de advertencia sobre la finalidad del Sistema creado de conformidad con los lineamientos de la Superintendencia como un recurso técnico de soporte a la operación del CRC, cuya finalidad es asegurar la trazabilidad del servicio y permitir a la Superintendencia de Transporte verificar el cumplimiento de los estándares de calidad y seguridad exigidos por la ley y el reglamento para la actividad a su cargo, la confidencialidad de la información y las consecuencias ante malas prácticas y el uso indebido del Sistema por acciones en las que pueda llegar a incurrir el personal vinculado a estos organismos de apoyo.

2. Control de actividad y vigencia del registro de personal de la salud:

a) Inactivación temporal por inactividad prolongada: El SICOV identificará automáticamente a aquellos profesionales de la salud para los cuales no se registre actividad de realización de exámenes en el Sistema durante un periodo consecutivo de treinta (30) días calendario. En tal caso, el Sistema modificará el estado del profesional a "inactivo temporalmente" y generará una alerta dirigida al organismo de apoyo y, de ser posible, al profesional, informándoles sobre esta

situación y la necesidad de que el instructor realice una nueva validación de su identidad contra las bases de datos de la RNEC para reactivar su estado.

b) Inactivación definitiva por falta de revalidación: Si transcurridos diez (10) días hábiles contados a partir de la generación de la alerta, el profesional no ha completado satisfactoriamente la nueva validación de su identidad ante la RNEC, el SICOV procederá a cambiar su estado a "inactivo definitivamente". Para que un profesional de la salud en este estado pueda volver a realizar exámenes, el CRC deberá realizar un nuevo proceso de registro inicial completo. El SICOV dejará trazabilidad en los registros (logs) cuando esto ocurra.

c) Gestión de novedades y retiros: Una vez surtida la inactivación, el SICOV inhabilitará inmediatamente los permisos de acceso de dicho usuario, impidiendo la validación de cualquier examen posterior a la fecha/hora de la novedad.

d) Mecanismo de auto-exclusión: El SICOV habilitará un canal directo para que el propio instructor o certificador pueda reportar su desvinculación del CRC. Este reporte tendrá efectos inmediatos de bloqueo preventivo de su usuario en dicho centro, evitando que su identidad sea utilizada por terceros tras su salida.

3. Módulo de información detallada del personal: El SICOV deberá contar con un módulo específico para el registro y consulta de la información detallada del personal vinculado. Este módulo deberá permitir, como mínimo, el registro de:

a) Tipo de vinculación contractual.
b) Cargo o rol desempeñado.
c) Número, fecha de expedición y vigencia de la tarjeta profesional (cuando sea requisito para el cargo).
d) Certificados de títulos académicos y de formación relevantes para el ejercicio de sus funciones.
e) Un historial de las verificaciones de identidad realizadas contra las bases de datos de la RNEC y a través de tecnología de reconocimiento facial.
f) Registro médico ante las autoridades de salud, cuando ello aplique.

4. Mecanismos para la verificación de la información del personal: El SICOV deberá estar técnicamente preparado para facilitar la validación de la veracidad de la información del personal mediante la implementación de servicios de interoperabilidad con sistemas de información de entidades pertinentes, siempre que se cuente con las autorizaciones necesarias y se respeten las normas de protección de datos. La responsabilidad primaria de la veracidad de la información suministrada recaerá en el organismo de apoyo y en el titular del dato.

5. Mecanismo de interoperabilidad entre operadores homologados: El SICOV implementará mecanismos de interoperabilidad entre operadores homologados para el intercambio seguro de información sobre la vinculación, desvinculación y experiencia del personal de la salud en diferentes CRC, permitiendo así a la Superintendencia de Transporte detectar y analizar patrones de alta rotación de personal entre diferentes CRC que puedan ser indicativos de anomalías o irregularidades.

La interoperabilidad entre sistemas y su parametrización permitirá que el SICOV realice validaciones automáticas al cierre de cada día, a fin de establecer cuántos profesionales de la salud validaron su identidad en el día en más de una sede de un CRC, y, en cada caso, validará la hora de la primera y última validación en cada establecimiento. La parametrización del Sistema permitirá que se generen alertas automáticas cuando se detecten inconsistencias en los horarios de estas validaciones y marcará por irregularidad los servicios afectados en dicha franja de tiempo.

Adicionalmente, el Sistema generará alertas automáticas sobre aquellos CRC en los que advierta que laboran o prestan servicios profesionales de la salud que figuran con validaciones de identidad en más de dos de estos organismos, o en más de uno, cuando las sedes estén ubicadas en distintos municipios del país, en un mismo día.

El análisis de esta información servirá como insumo para focalizar y priorizar las acciones de inspección, vigilancia y control de la entidad.

2.5.8.7. Validación continua de identidad de los participantes en la realización del examen.

El Sistema de Control y Vigilancia deberá implementar y ejecutar un proceso robusto y continuo de validación de la identidad de los usuarios del servicio y del personal de la salud, así como del personal certificador, durante todas las etapas del proceso de evaluación y de certificación.

1. **Mecanismos biométricos de validación:** El SICOV utilizará una combinación de los siguientes mecanismos biométricos para las validaciones de identidad continuas, conforme se detalla a continuación:

   a) Reconocimiento facial (selfie vs. template): Como mecanismo ágil de verificación, comparando una imagen facial capturada en tiempo real contra el patrón biométrico de referencia previamente registrado en el SICOV para cada usuario.

   b) Cotejo biométrico dactilar contra RNEC: Como mecanismo de alta seguridad, confrontando la huella dactilar del individuo contra las bases de datos de la Registraduría Nacional del Estado Civil.

2. **Momentos de validación:** El SICOV deberá exigir y registrar la validación de identidad tanto de usuarios como de profesionales de la salud en dos momentos clave de cada examen: **al inicio y al finalizar**.

   La selección del tipo de validación de identidad la hará el Sistema de manera aleatoria, en al menos el 50 % del total de validaciones de identidad que se realizan a lo largo de la prestación del servicio, así:

   - Para los usuarios, en cualquiera de los cuatro exámenes.
   - Para los profesionales de la salud, en cualquiera de los dos momentos de validación de identidad de cada examen que realicen.

3. **Validación de identidad del personal certificador:** La validación de la identidad de la persona designada y registrada en el SICOV por el CRC para expedir los certificados se realizará obligatoriamente en la etapa final del proceso, previo a la generación y expedición de cada certificado. Esta validación se efectuará empleando el mecanismo de cotejo biométrico dactilar contra la réplica de las bases de datos de la RNEC, para garantizar la plena autenticidad del responsable del acto.

4. **Gestión de indisponibilidad y niveles de servicio:**

   a) Cualquier novedad o falla técnica que genere indisponibilidad de los servicios de validación de identidad deberá ser documentada detalladamente por el operador del SICOV y reportada en tiempo real a la Superintendencia de Transporte a través del Módulo de consulta, IVC e Inteligencia de Negocio para la entidad descrito en el presente Anexo Técnico.

   b) Los servicios biométricos implementados en el SICOV deberán garantizar altos niveles de disponibilidad y efectividad, conforme a las métricas que se definan en este Anexo Técnico, las cuales serán objeto de auditoría.

c) El operador del Sistema deberá informar al público y a los organismos de apoyo sobre cualquier indisponibilidad del servicio, sus causas y el plan de contingencia, especialmente si el inconveniente se presenta con los servicios de la RNEC, caso en el cual la comunicación a través de la cual se brinde esta información deberá estar suscrita conjuntamente con el operador biométrico si son diferentes.

5. **Procedimiento en caso de no validar mediante cotejo biométrico dactilar durante la prestación del servicio:** En los procesos de validación de identidad en los que no se logre una verificación exitosa mediante el cotejo biométrico dactilar contra la base de datos de la RNEC, luego de tres (3) intentos fallidos continuos, se deberá aplicar como procedimiento alternativo de validación de identidad el de reconocimiento facial (comparación entre selfie y template) tanto del aspirante como del profesional de la salud.

   Una vez que la RNEC reglamente oficialmente el uso del reconocimiento facial contra sus bases de datos, este podrá ser implementado como mecanismo biométrico válido como alternativa de validación de identidad, según lo disponga la Superintendencia de Transporte.

Parágrafo. El Sistema estará parametrizado de tal manera que restringirá el uso de cualquier mecanismo de excepción biométrica o validación manual a lo largo de la prestación del servicio a cualquier usuario. Si no resultan efectivos los tres (3) intentos de validación de identidad con el mecanismo de reconocimiento facial, se procederá con los siguientes tres (3) intentos a través de cotejo de minucias dactilares contra la RNEC.

2.5.8.8. Procesamiento analítico de datos de validación para la integridad del proceso de evaluación.

El Sistema de Control y Vigilancia deberá incorporar funcionalidades avanzadas para el almacenamiento seguro y el procesamiento analítico (CPD Analítico) de los datos derivados del proceso de validación de identidad de los usuarios del servicio y personal de la salud. Este procesamiento tendrá como finalidad primordial la prevención, detección y control de intentos de fraude, así como la verificación del cumplimiento de los parámetros normativos del proceso de capacitación o curso.

1. **Trazabilidad y análisis de intentos de validación para detección de anomalías:**

   a) El SICOV deberá registrar y mantener una trazabilidad completa y auditable de todos los intentos de validación de identidad (exitosos y fallidos) realizados por usuarios y personal de la salud y certificador. Este registro detallado deberá incluir, como mínimo: el mecanismo de validación empleado, el resultado de cada validación, el dispositivo empleado, la fecha y hora exactas, la identificación del usuario y personal de la salud involucrados, la información del CRC y el examen específico en el que se hizo la validación o intento de esta, así como la tipificación del fallo. Estos datos deberán transmitirse al CPD – Analítico y de Identificación de manera sincrónica.

   b) El Sistema empleará herramientas de analítica de datos para procesar esta información de trazabilidad con el objetivo de identificar patrones inusuales, comportamientos sospechosos o inconsistencias que puedan ser indicativos de fraude o elusión de controles. Los algoritmos y reglas para la detección de estas anomalías serán definidos y podrán ser actualizados conjuntamente entre el operador SICOV y la Superintendencia de Transporte. Los hallazgos relevantes deberán generar alertas automáticas para revisión por parte de la Superintendencia y del organismo de apoyo, según corresponda.

2. **Control de la duración de los exámenes:** El SICOV deberá contabilizar y llevar un registro preciso del tiempo de duración efectivo de cada examen realizado, verificando que la duración de cada uno cumpla o se ajuste al tiempo mínimo promedio de duración. Para estos efectos se tendrá en cuenta la información de los registros históricos de la operación de los CRC, la cual será suministrada a la Superintendencia por parte de los actuales operadores homologados. En caso de que se evidencie una duración inusualmente alta en un examen (30 % de tiempo superior al promedio), el sistema generará una alerta y el servicio quedará marcado.

2.5.8.9. Gestión de la programación de recursos.

El Sistema de Control y Vigilancia deberá proporcionar funcionalidades robustas para que el personal de los organismos de apoyo gestione integralmente la programación de los exámenes, así como la asignación y el control de los recursos necesarios y disponibles para su realización (tales como profesionales de la salud y consultorios), a través de la plataforma SICOV.

Programación y gestión centralizada: El personal debidamente autorizado del organismo de apoyo será responsable de realizar la totalidad de la programación de los exámenes y la gestión de los recursos asociados a través del SICOV, asegurando la optimización de su capacidad instalada y el cumplimiento de la normatividad.

La programación interna deberá sincronizarse en tiempo real con el agendamiento web, conforme a lo señalado en el numeral subsiguiente, asegurando que los cupos reservados digitalmente por los ciudadanos queden automáticamente bloqueados y asignados en el cronograma de recursos del CRC.

2.5.8.10. Gestión de agendamiento de citas vía web y/o a través de aplicación móvil.

Con el objetivo de garantizar la libre elección del usuario y promover la transparencia en la prestación del servicio, el SICOV deberá disponer de una funcionalidad de relacionamiento con el ciudadano para la consulta de información y gestión de agendamiento de servicios ofertados por los CRC, accesible vía web y/o app móvil, que cumpla con las siguientes condiciones:

1. El operador homologado deberá garantizar la disponibilidad de esta funcionalidad como mínimo a todos los CRC vinculados a su plataforma. Para ello, podrá proveer su propia solución de agendamiento o integrarse con plataformas de terceros especializadas. En cualquier caso, el SICOV deberá garantizar interfaces (API) abiertas y seguras que permitan la interoperabilidad efectiva para los distintos fines que aquí se describen.

2. La interfaz dispuesta para el usuario deberá permitir:

   a) Búsqueda y comparación: Ubicar los organismos de apoyo en un mapa interactivo, filtrando por cercanía, tipo de servicio y precio.
   b) Transparencia tarifaria: Visualizar el precio total del servicio, desglosando los valores de la tarifa del servicio y los cobros por servicios de terceros.
   c) Sistema de reputación: visualizar la calificación y comentarios de otros usuarios sobre el servicio prestado, así como calificar y emitir comentarios sobre el servicio recibido.
   d) Agendamiento en tiempo real: Agendamiento en tiempo real: Consultar la disponibilidad real de cupos disponibles en la agenda del organismo de apoyo y realizar la reserva de citas, la cual se sincronizará automáticamente con la agenda interna del centro, reservando ese espacio de tiempo y respetando sus derechos.

3. Para garantizar la coherencia de la agenda (editable por cuenta del agendamiento a través de los canales digitales y/o por la atención presencial) y respetar los derechos del usuario, se aplicarán las siguientes reglas:

a) La reserva se sincronizará automáticamente con la agenda interna del organismo, bloqueando el recurso (al menos del profesional de la salud y consultorio en donde comenzará el examen).
b) Para asegurar una adecuada planeación logística y no entorpecer la atención de usuarios que acuden espontáneamente a la sede, el agendamiento digital estará sujeto a una ventana de tiempo mínima que deberá determinar el organismo de apoyo.
c) El SICOV monitoreará la puntualidad y el respeto a las citas agendadas digitalmente. El sistema generará alertas e indicadores de desempeño sobre la atención de los usuarios que programan la atención en el organismo de apoyo virtualmente.

4. Para confirmar la reserva, el sistema exigirá el respaldo transaccional mediante la compra directa del PIN (a través de pasarelas de pago integradas con el aliado de recaudo que realice la dispersión automática).

5. El calendario de citas disponible para los usuarios estará limitado técnicamente por la vigencia del PIN. En consecuencia, el módulo de agendamiento no permitirá asignar citas con una fecha posterior a quince (15) días calendario contados desde la fecha actual.

El sistema deberá validar que la fecha de la cita programada se encuentre dentro del periodo de vigencia del PIN asociado.

6. El centro deberá mantener la reserva de la cita agendada por un periodo mínimo de quince (15) minutos. Transcurrido este tiempo sin que se registre el inicio del trámite mediante validación biométrica exitosa, el sistema permitirá la cancelación de la cita por inasistencia y la liberación inmediata del espacio en la agenda del centro.

2.5.8.11. Gestión del registro histórico detallado del proceso de examinación.

El Sistema de Control y Vigilancia deberá generar y conservar un registro histórico detallado, cronológico, seguro e inalterable de la participación de cada usuario en cada uno de los exámenes que componen el proceso de evaluación de aptitud física, mental y de coordinación motriz.

Este registro histórico constituirá la traza de auditoría principal del servicio prestado y deberá incluir, como mínimo, la siguiente información por cada examen:

a) Identificación del examen: Fecha, hora de inicio y finalización real de cada examen, consultorio utilizado (según aplique) e identificación del personal de la salud responsable de realizarlo.

b) Resultados obtenidos: los resultados obtenidos del examen con las observaciones del profesional y la indicación precisa de si el usuario reúne o no las condiciones mínimas para ser considerado apto para conducir.

c) Duración del examen: El SICOV contabilizará el tiempo total exacto de duración de cada examen y el tiempo total de evaluación del usuario, incluyendo la espera en el establecimiento. Para tal efecto, el Sistema contabilizará el tiempo que transcurra desde el momento en que se realiza el enrolamiento y la primera validación de identidad del usuario en un consultorio; hasta que se realice la última validación en el examen final.

d) Restricciones aplicables: la mención de las restricciones para conducir (cuando aplique), de acuerdo con los resultados obtenidos y el dictamen del profesional de la salud conforme a los lineamientos técnicos correspondientes.

Este registro histórico es fundamental para la implementación del mecanismo de interoperabilidad que debe existir entre proveedores homologados del SICOV para la consulta de información detallada de los servicios prestados, a fin de evitar el fraude.

e) Constancia de realización del examen: La clasificación final de cada examen como "Realizado" o "No realizado", basado en los resultados de las validaciones de identidad al principio y al final, conforme a lo establecido en los numerales correspondientes de este Anexo Técnico.

f) Historial de validaciones de identidad: Información detallada sobre todos los intentos de validación de identidad realizados por el usuario y el instructor durante la sesión, incluyendo el resultado (exitoso o fallido), el mecanismo biométrico empleado y la estampa de tiempo correspondiente.

g) Motivos de suspensión o no culminación de exámenes: De igual manera, este registro contendrá también, de manera inalterable, la información de aquellos exámenes suspendidos o que no hayan culminado en la expedición de un certificado, pese a que el PIN se haya consumido, incluyendo la información antes descrita hasta donde quiera que haya llegado la prestación del servicio. Dichos registros deberán incluir además una mención del(los) motivo(s) por los cuales no se expidió la certificación. El SICOV estará parametrizado de tal manera que al cierre de cada jornada de operación diaria del CRC requerirá el diligenciamiento de dicha información para cada servicio que se encuentre en dicha condición.

h) Registro de logs: Este registro se complementará con los log de uso que deberá arrojar y guardar la herramienta del software de gestión y control del SICOV para dar cumplimiento a todo lo descrito en este Anexo. Estos log o registros servirán para monitorizar cualquier uso anormal o intento de uso anormal de la herramienta. Para ello, deberá quedar registro del usuario que la hizo y la fecha y hora exacta del evento.

i) Operación offline: El Sistema deberá tener la capacidad de operar de forma desconectada y con contingencias asociadas a las comunicaciones con otros sistemas de información y plataformas. Las contingencias que se presenten, cualquiera que sea su causa (fallas con sistemas externos con los que se consulta información, fallas en la conexión de internet, etc.), deberán identificarse y documentarse.

De cada episodio que se presente el SICOV generará y almacenará registros (logs) con la información del motivo, fecha y hora exactas a las que se presentó la novedad, así como su duración hasta que se resolvió

2.5.8.12. Gestión del registro y control de equipos de evaluación empleados en los CRC.

a) Gestión de registro de información. El Sistema de Control y Vigilancia deberá gestionar y mantener un registro actualizado y detallado de los equipos empleados por los CRC para realizar los exámenes de audiometría, optometría y coordinación motriz. Esta funcionalidad se basará primordialmente en la información reportada y actualizada por el CRC. En el registro se reportará información como:

- Marca, referencia, año de fabricación, serial.
- Registro y control de todas las calibraciones anuales y mantenimientos preventivos y correctivos realizados a los equipos, con fecha, vigencia (según aplique) e información de la entidad que expide el certificado o

documento de calibración y que realiza los mantenimientos, con su respectivo soporte de realización y resultados.

Las calibraciones y mantenimientos deberán hacerse por parte de un laboratorio de calibración acreditado ante el ONAC.

El SICOV generará y enviará notificaciones de alerta automáticas al CRC, con una antelación mínima de treinta (30) días calendario antes de la fecha de vencimiento de cualquier calibración de los equipos. Estas alertas se dirigirán al correo electrónico oficial registrado por el CRC.

b) Verificación y alertas de mantenimiento: Cuando un CRC reporte una falla, avería o mantenimiento en un equipo, el operador del sistema estará obligado a verificar la veracidad de dicha situación a través de las evidencias disponibles. El sistema generará una alerta si detecta que el equipo está siendo utilizado durante el supuesto periodo de reparación o calibración.

Integración de equipos de evaluación empleados en los CRC.

El Sistema de Control y Vigilancia deberá integrar al software, los dispositivos y equipos empleados por los CRC para realizar los exámenes de audiometría, optometría y coordinación motriz y parametrizar el mecanismo de captura o recepción de resultados de las pruebas realizadas, de tal manera que estos no puedan ser alterados o manipulados y que quede la trazabilidad de los resultados que arroje cada examen practicado. El Operador del Sistema deberá emprender todos los esfuerzos necesarios para implementar procedimientos efectivos que le permitan recibir la información directamente de los equipos y dispositivos sin ningún tipo de alteración, de manera inmediata y sin retraso de tiempo, reduciendo la interacción de los profesionales con la evaluación.

2.5.8.13. Interfaz de validación para el registro de certificados en el RUNT.

El SICOV deberá disponer de un servicio de consulta o mecanismo de integración seguro y eficiente que permita al Registro Único Nacional de Tránsito verificar, previo al registro de un certificado expedido por un organismo de apoyo, que el usuario es apto para conducir por haber obtenido los resultados y valoración requerida y por haber realizado la totalidad de validaciones del proceso efectuados a través del SICOV.

Para tal fin, ante una solicitud de registro de dicho certificado, el RUNT podrá consultar al SICOV utilizando el número de documento de identidad del usuario y el IDRUNT del Centro. El SICOV deberá responder a esta consulta indicando, como mínimo:

a) La confirmación de la identidad del usuario registrado en SICOV (nombre completo y número de documento).

b) El estado de la "Decisión de Certificación" del usuario dentro del SICOV, señalando si este ha realizado satisfactoriamente la totalidad de validaciones del proceso, incluyendo el dato de la categoría autorizada de licencia de conducción.

Esta funcionalidad es esencial para asegurar que solo los certificados correspondientes a los exámenes debidamente verificados por el SICOV sean inscritos en el RUNT para los fines legales correspondientes.

2.5.8.14. Gestión de conformidad documental y continuidad operativa de los CRC.

El Sistema de Control y Vigilancia implementará funcionalidades integrales para la gestión y verificación continua del cumplimiento, por parte de los Centros de Reconocimiento de Conductores, de los requisitos documentales mínimos establecidos por la autoridad competente para su inscripción en el Registro Único

Nacional de Tránsito y para su operación legal y continua. El objetivo primordial de esta función es asegurar que ningún CRC pueda utilizar las funcionalidades del SICOV si no demuestra el cumplimiento vigente y verificable de dichos requisitos esenciales.

1. **Repositorio documental oficial y obligaciones del organismo de apoyo:**

a) El SICOV funcionará como repositorio digital oficial y centralizado donde cada CRC estará en la obligación de cargar, mantener permanentemente actualizadas y asegurar la disponibilidad de todas las copias digitales vigentes de los documentos que acreditan o certifican el cumplimiento de sus requisitos mínimos de operación.

b) Será responsabilidad exclusiva e indelegable del representante legal del organismo de apoyo garantizar la autenticidad, integridad, exactitud y correspondencia de los documentos cargados en el SICOV con sus originales, así como su renovación y actualización oportuna antes de su fecha de vencimiento.

Sin perjuicio de otros que pueda exigir el Ministerio de Transporte u otras autoridades competentes, los CRC deberán cargar y mantener vigentes en el repositorio del SICOV, como mínimo, los siguientes documentos para acreditar su operación legal y continua:

- Certificado de existencia y representación legal expedido por la Cámara de Comercio, que acredite su actividad económica principal y complementarias.
- Acreditación vigente, así como los informes de reacreditación y de seguimiento anual realizados por el Organismo Nacional de Acreditación en Colombia.
- Licencia de funcionamiento del establecimiento o establecimientos, expedida por la autoridad competente, cuando aplique según la normativa municipal o distrital.
- Póliza vigente de responsabilidad civil extracontractual que ampare los riesgos inherentes a la actividad realizada.
- Constancia de registro en el RUNT (ID RUNT).
- Constancia de registro del CRC en el Registro Especial de Prestadores de Servicios de Salud (REPS).

Las demás que determine el Ministerio de Transporte y la Superintendencia.

Estos documentos constituyen requisitos documentales críticos y por lo tanto su existencia en el repositorio del SICOV y vigencia constituye requisito para uso del Sistema.

2. **Verificación automatizada de vigencia y sistema de alertas preventivas**

a) El SICOV realizará una verificación automática y continua de la vigencia de los documentos registrados, contrastando la fecha actual, las fechas de vencimiento registradas en el Sistema por parte del CRC y el contenido del documento digitalizado para acreditar la vigencia del requisito

b) El Sistema generará y enviará notificaciones de alerta automáticas, con una antelación mínima de sesenta (60) y treinta (30) días calendario antes de la fecha de vencimiento de cualquier documento definido como crítico para la operación o el registro en RUNT. Estas alertas se dirigirán al correo electrónico oficial registrado por el CRC.

c) El Sistema generará y enviará alertas en caso de encontrar inconsistencias entre la información registrada por el CRC sobre la vigencia de estos documentos y la información contenida en los documentos digitalizados que soportan el cumplimiento y la vigencia de los requisitos críticos de operación. Esta información será reportada de manera automática al MOCVI del CPD

Analítico de la Superintendencia. El reporte incluirá: tipo de documento, campo inconsistente, evidencia del hallazgo y fecha de detección.

d) El SICOV deberá conservar un registro auditable del envío y, de la entrega de estas notificaciones.

Cuando la evidencia del vencimiento de un requisito de operación crítico, o de su inconsistencia, sea resultado de la revisión manual que realice el operador homologado, deberá informarlo a la Superintendencia a través del MOCVI del CPD Analítico y de Identificación y deberá activar una alerta que aplique una marca de irregularidad a todos los servicios que preste el centro mientras la misma se mantenga activa.

3. Interoperabilidad y mecanismos de consulta con entes públicos, privados, y registros de información necesarios para la IVC:

El SICOV deberá estar técnicamente preparado para facilitar el intercambio de información necesaria para ejercer las labores de inspección, vigilancia y control de la actividad a cargo de los CRC, mediante la implementación de servicios de interoperabilidad y/o consulta con sistemas de información de entidades públicas o privadas que administren registros o bases con información que se requiera para el cumplimiento de las funciones de la Superintendencia.

Entre las entidades/registros administradores de información que es importante para la Superintendencia se encuentran, entre otras:

Registraduría Nacional del Estado Civil: Fuente principal para la validación biométrica de identidad y verificación de datos personales. Sustenta la autenticación segura del personal enrolado y garantiza la consulta de información personal del individuo.

Organismo Nacional de Acreditación de Colombia: Validación del estado de acreditación de los CRC y del cumplimiento de los requisitos técnicos del personal vinculado, con miras a que se mantenga la coherencia entre la acreditación vigente y el cumplimiento de normas técnicas de operación.

Ministerio de Transporte – Registro Único Nacional de Tránsito: Para la confirmación de que los CRC se encuentran registrados y cumplen con los requisitos para desarrollar la actividad.

Ministerio de Salud y Protección Social: Permite consulta información sobre el registro del personal de la salud en el Registro Único Nacional del Talento Humano en Salud.

Cuando la interoperabilidad y/o canal de consulta directa e inmediata se viabilice con estos actores, deberán tenerse en cuenta las indicaciones y/o criterios que defina la Superintendencia de Transporte.

4. Gestión de incumplimientos, generación de alertas y marcación de irregularidades:

a) Definición de documentos críticos: Se entenderán como "documentos críticos" aquellos indispensables para el registro activo del CRC en el RUNT y para su operación legal continua, conforme a la reglamentación del Ministerio de Transporte.

b) Generación de alerta temprana por incumplimiento: Ante el vencimiento o la ausencia no subsanada de un documento crítico, el SICOV generará de forma automática e inmediata una alerta temprana por incumplimiento. Esta alerta quedará visible permanentemente en el perfil de administración del CRC dentro del SICOV y será comunicada de forma automática a su correo electrónico oficial y al Módulo de consulta, IVC e inteligencia de negocio de la Superintendencia de Transporte.

c) Marcación de irregularidad en servicios: Mientras la "alerta temprana por incumplimiento" se encuentre activa, todos los servicios que el CRC preste y registre en el SICOV (inscripciones, clases, cursos, evaluaciones) y, en especial, todos los certificados que expida, quedarán con una "Marcación de irregularidad". Esta marcación es una traza digital indeleble que indica que el servicio o certificado fue expedido mientras el organismo se encontraba en una situación de incumplimiento.

d) Categorización del examen como "No realizado". Los exámenes que generen la marcación de irregularidad por los motivos aquí expuestos se clasificarán automáticamente como "No realizados" conforme a lo desarrollado en el presente Anexo.

e) Visualización para la Superintendencia: El Módulo de consulta, IVC e inteligencia de negocio de la Superintendencia de Transporte alojado en el CPD Analítico contará con tableros de control de la información que le permitirán a la entidad visualizar en línea, entre otras cosas, las alertas activas por organismo de apoyo, así como cuantificar y detallar el número de servicios y certificados "marcados" por irregularidad, sirviendo como insumo priorizado para sus actuaciones de inspección, vigilancia y control.

Las marcaciones o alertas podrán generarse por el Sistema en cualquiera de las etapas del proceso. El SICOV registrará cada evento con trazabilidad completa, especificando la naturaleza de la alerta, la fecha y hora exacta de generación, servicio afectado, información del(los) personal de la salud involucrado(s) y del usuario del servicio.

Lo anterior constituirá insumo priorizado para las actuaciones de inspección, vigilancia y control de la Superintendencia.

f) Cese de alertas:

1. Para el cese de una alerta, el organismo de apoyo deberá cargar en el SICOV los documentos actualizados y vigentes que subsanen el incumplimiento.
2. En los casos que la alerta se active por el vencimiento o inexistencia de soporte del cumplimiento de requisitos críticos de operación, la Superintendencia de Transporte validará la conformidad, apoyándose en el proveedor homologado del Sistema, de los documentos cargados en un plazo máximo de cinco (5) días hábiles, con el apoyo de los proveedores homologados del Sistema.
3. Una vez validada satisfactoriamente la subsanación por parte del CRC, la Superintendencia procederá al cese de la alerta en el Sistema. A partir de ese momento, los nuevos servicios que preste el organismo ya no serán objeto de marcación. La marcación sobre los servicios pasados, sin embargo, persistirá en el registro histórico como evidencia de la irregularidad ocurrida.
4. La acción de validación de los documentos que soportan la subsanación realizada, deberá igualmente quedar guardada en los registros (logs) del Sistema, con la identificación del usuario que realizó dicha validación y la fecha y hora exacta de su realización.

2.5.8.15. Gestión y control de suspensiones y medidas cautelares.

El SICOV deberá contar con las funcionalidades necesarias para gestionar la información de las medidas de suspensión de servicio ordenadas por la Superintendencia de Transporte y ejecutadas por el RUNT. El sistema deberá garantizar lo siguiente:

Registro de la orden: La Superintendencia comunicará al operador SICOV cada vez que adopte una medida de suspensión en contra de un CRC, así como la información precisa sobre el momento (fecha y hora) exacto en que la medida de suspensión se haga efectiva en el Registro Único Nacional de Tránsito, así como el momento de su levantamiento.

Esta información, que será recibida en la Superintendencia por parte del concesionario del RUNT, será transmitida desde la entidad a los operadores homologados a través del mecanismo de interoperabilidad o consulta que se desarrolle para el efecto, con la periodicidad que se determine. El SICOV llevará dicho registro de información actualizado. Sin perjuicio de lo anterior, esta información también podrá ser consultada directamente en el RUNT por parte del operador homologado a través de interoperabilidad.

Contabilización precisa: El SICOV llevará un registro exacto del tiempo transcurrido de ejecución de la medida de suspensión, con base en la información que los operadores reciban por parte de la Superintendencia o directamente del RUNT. Este registro servirá para efectos de contabilizar y verificar el cumplimiento del tiempo de suspensión.

Esta capacidad se activará para dar estricto cumplimiento a:

a) Cualquier orden administrativa de la Superintendencia de Suspensión preventiva de actividades de un organismo de apoyo al tránsito, en ejercicio de las potestades derivadas de la Ley 1702 de 2013, o la norma que la modifique, adicione o derogue.

b) Cualquier otra medida o decisión administrativa, como la suspensión o cancelación del registro en el RUNT, que sea impuesta mediante acto administrativo en firme.

Alertas de cumplimiento de plazos: El sistema generará y enviará notificaciones y alertas automáticas a la Superintendencia con una antelación de diez (10) días hábiles antes de que se cumpla el plazo de la suspensión –en los casos en que no se haya levantado la medida antes–, a fin de coordinar de manera oportuna la reactivación del servicio y evitar la afectación de los derechos del administrado.

Trazabilidad histórica: Toda la información relacionada con la imposición de las medidas de suspensión, desde la expedición de la orden hasta el levantamiento de la misma, deberá quedar registrada en las bitácoras del sistema de manera inalterable para su posterior auditoría.

Esta constancia en el registro servirá para efectos de contabilizar el tiempo exacto de suspensión que haya cumplido un organismo de apoyo, ante las autoridades competentes

2.5.8.16. Gestión de hallazgos de auditorías de conformidad y seguimiento a planes de mejora.

El Sistema de Control y Vigilancia deberá facilitar el registro y seguimiento de los resultados de las auditorías anuales de seguimiento efectuadas por el ONAC. Esta funcionalidad debe permitir al organismo de apoyo cargar el informe completo de auditoría y sus anexos, emitido por el ONAC.

El CRC deberá cargar en el Sistema y reportar el contenido del informe de no conformidades, fortalezas y aspectos por mejorar al cierre de la auditoría (otorgamiento, seguimiento, ampliación o renovación) dentro de los tres (3) días hábiles siguientes al recibo de cada informe.

El Sistema deberá facilitar la extracción o el registro estructurado de información de los hallazgos, no conformidades y aspectos de mejora identificadas en dicho informe.

La presentación del informe de auditoría correspondiente en el SICOV dentro de los plazos establecidos, hace parte de un requisito documental crítico y por lo tanto su existencia en el repositorio del SICOV y vigencia constituye requisito para uso del Sistema.

El vencimiento del requisito de mantenimiento de la acreditación generará una alerta automática de irregularidad (documental), que será puesta en conocimiento de la Superintendencia de Transporte a través del módulo de consulta, IVC e inteligencia de negocio del Sistema.

La Superintendencia de Transporte realizará, a través del SICOV, seguimiento a los hallazgos, no conformidades y acciones correctivas o de mejora, en lo que sea de su competencia.

2.5.8.17. Verificación de la ubicación autorizada y transmisión segura de datos de operación.

El Sistema de Control y Vigilancia deberá incorporar mecanismos automáticos para asegurar que la prestación de los servicios, la expedición de certificados y el cargue de información por parte de los CRC se realicen exclusivamente desde las sedes autorizadas y a través de canales seguros.

a) Verificación del origen de las operaciones: El Sistema deberá constatar, a través de medios técnicos de geolocalización (GPS) de los dispositivos fijos o la validación de la dirección IP de origen, que la prestación de los servicios y el cargue de información al SICOV se realicen únicamente desde las sedes y ubicaciones físicas autorizadas por el Ministerio de Transporte y debidamente registradas en el Sistema. Para lograrlo, el Sistema deberá disponer de soluciones de hardware y software que cumplan con los requisitos mínimos mencionados en el acápite correspondiente del presente Anexo Técnico.

b) Garantía de transmisión segura de datos: El Sistema deberá facilitar y asegurar que toda la información operativa transmitida entre el CRC y los servidores centrales del SICOV se realice a través de canales de comunicación seguros y cifrados que preserven la integridad y confidencialidad de los datos, conforme a los estándares de seguridad definidos en este Anexo Técnico.

2.5.8.18. Gestión y control sistematizado de la capacidad instalada y operativa.

El Sistema de Control y Vigilancia deberá contar con funcionalidades para registrar, actualizar permanentemente y controlar la capacidad instalada y operativa real de cada CRC. Esta capacidad determinará el volumen máximo de servicios (evaluaciones y cupos) que el organismo puede programar y prestar simultáneamente a través del SICOV.

1. **Determinación de la capacidad instalada registrada en SICOV:** La capacidad instalada de cada CRC registrada en el SICOV se determinará y actualizará con base en la información proveniente de las siguientes fuentes, las cuales deberán ser consistentes entre sí:

   a) La información sobre capacidad certificada de acuerdo con la acreditación otorgada por el ONAC.

   b) La información detallada y actualizada que el organismo de apoyo registre directamente en el SICOV sobre sus recursos disponibles y habilitados, (ej. número de consultorios, aforo máximo, número de integrantes del personal de la salud, y número de consultorios).

   c) La información y evidencia sobre la capacidad real recabada y validada por la Superintendencia de Transporte durante las visitas de inspección, vigilancia y control que realice, o de las visitas que realicen los operadores homologados conforme a las instrucciones y lineamientos de la Superintendencia.

   En caso de discrepancia en la capacidad instalada u operativa de un CRC, se le dará prevalencia a la información obtenida en las visitas que se realicen a los establecimientos, seguida por la información oficial de la

Acreditación ONAC, sobre la información registrada por el CRC en el SICOV.

2. **Control automático de agendamiento y asignación de recursos:** El SICOV estará parametrizado para impedir el agendamiento de exámenes y la asignación de recursos que excedan la capacidad instalada registrada y validada para el CRC. Específicamente, el Sistema impedirá que se programe más de un examen simultáneamente en un mismo consultorio, o que un mismo profesional de la salud o aspirante sea asignado a más de un examen en el mismo horario.

   En el caso del examen de psicología, que puede aplicarse a varios aspirantes al mismo tiempo, el SICOV estará parametrizado de tal manera que impida el agendamiento de más aspirantes de los que permita la capacidad del consultorio de manera simultánea.

3. **Interoperabilidad para la consistencia de la capacidad entre operadores homologados del SICOV:** Para garantizar la consistencia de la información sobre la capacidad instalada y la asignación de recursos (humanos y físicos) de un organismo de apoyo, y prevenir el uso fraudulento de un mismo recurso a través de diferentes plataformas, se exigirá la implementación de mecanismos de integración e interoperabilidad para el intercambio seguro de información relevante entre los distintos software desarrollados por los proveedores autorizados del SICOV. Además de la información que aquí se indica, que debe ser consultada permanentemente a través de mecanismos de interoperabilidad, la Superintendencia de Transporte definirá estándares técnicos, protocolos y la información mínima a intercambiar para dar cumplimiento a esta función durante el periodo de implementación.

2.5.8.19. Herramientas de autoconsulta, reporte operacional y análisis de datos.

El Sistema de Control y Vigilancia facilitará a cada CRC un módulo integral y de autoservicio que le permita consultar, generar, visualizar, personalizar y descargar informes detallados sobre su propia operación, así como acceder a herramientas de inteligencia de negocio (Business Intelligence) para un análisis más profundo de sus datos. Estas capacidades tienen como fin facilitar la autogestión, la toma de decisiones basada en evidencia, la mejora continua y el cumplimiento de sus obligaciones de reporte, incluyendo la conciliación de información con el Registro Único Nacional de Tránsito y otros sistemas pertinentes.

El acceso a la información se limitará estrictamente a los datos operativos del CRC, sin incluir información personal o sensible de los usuarios finales que llegue a registrar el Sistema, garantizando seguridad, confidencialidad y segmentación de accesos.

Estas herramientas serán provistas a través del funcionamiento del CPD – Analítico.

1. **Condiciones de seguridad y trazabilidad de las descargas:**

Con el fin de garantizar el control sobre la información operativa descargada desde el SICOV, el módulo de reportes deberá cumplir con las siguientes características:

a) Registro de auditoría (Logs): El sistema deberá generar y almacenar un registro automático e inalterable de cada evento de generación y descarga de reportes. Este registro deberá contener, como mínimo:

- Identificación del usuario que realiza la descarga.
- Fecha y hora exacta de la descarga.

- Dirección IP de origen.
- Tipo de reporte y parámetros de búsqueda utilizados.

b) Marca de agua dinámica para PDF: Los reportes generados en formato de documento portátil (PDF) deberán incluir automáticamente una marca de agua visible y transversal en todas sus páginas, que contenga el nombre del usuario que generó el reporte, el nombre del organismo de apoyo y la fecha de descarga.

c) Advertencia de confidencialidad: Previo a la descarga de cualquier archivo (CSV, Excel, PDF), el sistema deberá desplegar un mensaje de advertencia que el usuario debe aceptar, recordando su responsabilidad legal sobre la custodia, confidencialidad y tratamiento adecuado de los datos personales contenidos en el reporte, conforme a la Ley 1581 de 2012.

2. **Generación de informes operativos estándar y personalizados:**

a) El SICOV ofrecerá un conjunto de informes operativos predefinidos que reflejen los principales indicadores de gestión del CRC. Adicionalmente, permitirá al organismo configurar y generar reportes con periodicidad personalizada (diaria, semanal, mensual, trimestral, anual, o rangos de fechas específicos), facilitando el análisis comparativo de la información entre diferentes periodos.

b) Los informes deberán poder ser descargados por el organismo de apoyo en formatos de uso común (ej. PDF, CSV, Excel) para su análisis local.

c) El SICOV garantizará que los datos presentados en estos informes sean exactos, íntegros y consistentes con la información registrada y validada en el Sistema.

La información de los reportes operativos estándar y personalizados deberá ser actualizada por el SICOV con una frecuencia de al menos una (1) vez al día.

3. **Herramientas de inteligencia de negocio (BI) para análisis avanzado:**

a) Adicionalmente a los informes operativos, el SICOV deberá proporcionar a los CRC y a la Superintendencia acceso a herramientas de inteligencia de negocio que permitan realizar análisis más profundos y personalizados sobre los datos de la operación (propia para el organismo, y del conjunto de organismos para la Superintendencia).

b) Estas herramientas podrían incluir funcionalidades como tableros de control (dashboards) interactivos, capacidades de desglose en los datos (drill-down) y construcción guiada de consultas sobre sus datos operativos, conforme a las especificaciones técnicas y los límites de seguridad y acceso que se definan.

4. **Facilitación de la conciliación de información con sistemas externos:**

Tanto los informes estándar como las capacidades de consulta avanzada permitirán a los CRC verificar y conciliar de manera eficiente la información de su operación registrada en el SICOV antes de realizar sus cargues o validaciones de información en el RUNT u otros sistemas de información de tránsito pertinentes.

2.5.8.20. Clasificación automática del estado de los exámenes del proceso de evaluación.

El Sistema de Control y Vigilancia deberá clasificar de manera automática cada uno de los cuatro exámenes de los usuarios como **"Realizado"**, **"No realizado" y/o "Suspendido"**. Esta clasificación se basará en el cumplimiento de los requisitos de validación de identidad, tanto del usuario, como del profesional de la salud y del reporte del resultado correspondiente a cada examen en el

Sistema, conforme a los procedimientos detallados en los numerales correspondientes de este Anexo Técnico.

1. **Criterios para clasificación como "Realizado":** Un examen se clasificará automáticamente como "Realizado" si, y solo si, el SICOV registra que se cumplieron de manera acumulativa y satisfactoria todos los puntos de control de identidad establecidos para dicha prueba (ej. al inicio y al finalizar) y si el examen cuenta con un resultado registrado en el Sistema. El SICOV registrará esta clasificación de forma inmediata y automatizada una vez se confirmen las validaciones aludidas.

2. **Criterios para clasificación como "No realizado":** Cualquier examen que no cumpla con la totalidad de los criterios establecidos en el numeral anterior será clasificado automáticamente por el SICOV como "No realizado". El Sistema habilitará un campo de diligenciamiento obligatorio para que el profesional de la salud del caso registre el motivo específico de dicha clasificación (ej. imposibilidad para hacer validación final de identidad del usuario por abandono del consultorio, fallas en el Sistema con su descripción con evidencia, entre otros) y esta información deberá estar disponible para consulta por parte del organismo de apoyo y, en lo posible, ser informada al usuario.

   La clasificación de algún examen como "no realizado" y las razones de tal situación serán objeto de consulta a través de los mecanismos de interoperabilidad que deben existir entre operadores del SICOV.

3. **Criterios para clasificación como "Suspendido":** Un examen que no puede culminar el mismo día en que se realizan las diferentes valoraciones, por requerirse de un concepto médico de un especialista o de un concepto médico, por condiciones de aptitud o de salud que no pueden ser valoradas. En estos casos, el examen quedará en estado de suspensión hasta que se cumpla la condición de valoración externa. En tal caso, la continuidad del examen y el resultado final del examen dependerá del certamen del especialista. El Sistema habilitará un campo de diligenciamiento obligatorio por parte del profesional de la salud en el que deberá informar esta situación.

Repetición de exámenes:

En los casos que resulte pertinente que se repita un examen según determine el profesional de la salud correspondiente, el Sistema así lo habilitará, guardando registro en el Sistema de la identificación del profesional de la salud que así lo decidió y del número de intentos o exámenes realizados. El sistema generará marcaciones de aquellos servicios que se repitan a un usuario en más de dos oportunidades.

No obstante la facultad del profesional de la salud para autorizar la repetición de las pruebas, el Sistema de Control y Vigilancia deberá estar parametrizado para generar automáticamente una Alerta de posible fraude por intentos múltiples cuando se registren tres (3) o más intentos fallidos o repeticiones consecutivas asociadas a un mismo usuario para un mismo examen. Dicha alerta se deberá remitir automáticamente y en tiempo real al Módulo de IVC de la Superintendencia y generará una 'Marcación de irregularidad' sobre el servicio, la cual permanecerá en el histórico del trámite para efectos de auditoría posterior.

2.5.8.21. Habilitación para la expedición de certificados.

El Sistema de Control y Vigilancia deberá gestionar el proceso de generación de los certificados de culminación del examen de aptitud física, mental y de coordinación motriz y habilitar su expedición por parte del personal autorizado del organismo de apoyo, únicamente para aquellos usuarios que hayan cumplido satisfactoriamente con la totalidad de los requisitos, conforme a la información validada y registrada en el Sistema.

1. **Condiciones para la habilitación de expedición de certificados:** El SICOV habilitará la funcionalidad para la expedición de un certificado a un usuario específico si, y solo si, se han verificado y registrado en el Sistema el cumplimiento de todos los requisitos aplicables, siendo condición indispensable que el proceso de evaluación completo, es decir cada uno de los cuatro exámenes, haya sido clasificado en el Sistema como **"Realizado"**, conforme a lo establecido en este Anexo Técnico.

2. **Proceso de expedición y restricción automatizada:**

a) Una vez cumplidas todas las condiciones señaladas, el SICOV habilitará automáticamente la opción para que el personal del organismo de apoyo debidamente autorizado y con identidad validada biométricamente, proceda con la expedición formal del certificado.

La decisión final de certificación debe ser tomada por uno de los profesionales de la salud vinculados al CRC que conozca los rangos de aprobación definidos en el esquema de certificación y que no haya participado en la evaluación del candidato a certificar.

La centralización de labores de certificación sólo se permitirá en los CRC que así lo puedan realizar en caso de contar con las capacidades y/o reunir las condiciones que así lo permitan, como una acreditación del ONAC con tal alcance, lo cual en todo caso será objeto de verificación por parte del Superintendencia de Transporte a través del operado homologado del SICOV.

b) El Sistema deberá generar el certificado con las características que defina el Ministerio de Transporte, incluyendo un número único de identificación y los mecanismos para su posterior validación y registro en el RUNT.

La responsabilidad del otorgamiento de la certificación recae exclusivamente en el Centro de Reconocimiento de Conductores y por ende conserva su autoridad al respecto sin delegar, o poder delegar, a terceros sus decisiones pertinentes a la certificación.

c) En caso contrario, si no se cumplen la totalidad de las condiciones requeridas, el SICOV mantendrá automáticamente restringida la opción de expedición de certificados para dicho usuario, indicando al organismo de apoyo los requisitos pendientes de cumplimiento.

d) Inclusión de imagen institucional en certificados: Cuando la regulación exija que la fotografía del usuario en el certificado o documento final incluya el logotipo o imagen corporativa del CRC, dicha característica deberá ser implementada mediante procesamiento digital de imágenes (superposición lógica o marca de agua) al momento de la generación del archivo visual o de impresión de la certificación. El software del SICOV deberá garantizar esta superposición estética en el entregable para dar cumplimiento a la normatividad aplicable.

2.5.8.22. Gestión del registro histórico de certificados expedidos.

El Sistema de Control y Vigilancia deberá crear y mantener un registro histórico, detallado, cronológico, seguro e inalterable de todos los certificados cuya expedición haya sido habilitada y gestionada a través del Sistema para cada CRC.

Este registro histórico deberá incluir, como mínimo, la siguiente información por cada certificado:

a) Número único de identificación del certificado generado por el SICOV.
b) Identificación del organismo de apoyo que expidió el certificado (NIT y Razón Social).

c) Identificación del usuario a quien se le expidió el certificado (tipo y número de documento de identidad, nombres y apellidos).
d) Fecha y hora exactas de la expedición del certificado en el SICOV.
e) Identificación de los profesionales de la salud que evaluaron al usuario.
f) Identificación del funcionario del organismo de apoyo que autorizó y formalizó la expedición del certificado en el SICOV.

2.5.8.23. Registro y actualización de tarifas de servicios.

El Sistema de Control y Vigilancia deberá disponer de una funcionalidad para que cada CRC registre y mantenga actualizada la información detallada de las tarifas que establece y ofrece al público por su servicio.

a) Responsabilidad del organismo de apoyo en el registro tarifario: Será responsabilidad exclusiva del organismo de apoyo ingresar y mantener actualizada en el SICOV, de manera veraz y oportuna, la tarifa vigente de sus servicios, atendiendo las disposiciones reglamentarias del Ministerio de Transporte en la materia. Cualquier modificación en sus tarifas deberá ser reflejada en el Sistema antes de su aplicación a los usuarios.

b) Finalidad del registro tarifario en SICOV: La información sobre las tarifas registrada en el SICOV tendrá como finalidades principales:

1. Facilitar la transparencia informativa hacia los usuarios del servicio.
2. Servir como insumo para las labores de supervisión sectorial y protección al usuario que ejerce la Superintendencia de Transporte, permitiendo el análisis de tendencias y el monitoreo del mercado, sin perjuicio del régimen de libertad tarifaria que pueda aplicar al servicio.
3. Proveer información de referencia para la funcionalidad de la aplicación móvil del SICOV destinada a usuarios, donde estos podrán consultar las tarifas ofrecidas por los organismos de apoyo.

c) Actualización automática de tarifas mínimas: el Sistema estará configurado te tal manera que, el primero de enero de cada año actualizará de manera automática la tarifa mínima del valor de los servicios de capacitación ofrecidos por los CRC, aplicando para ello el cálculo correspondiente conforme a lo dispuesto en la Resolución No. 20223040045295 de 2022 del Ministerio de Transporte, o la que norma que la modifique o sustituya. El SICOV actualizará de manera automática el valor de la tarifa de aquellos CRC que la tuvieran configurada en el mínimo monto tarifario al cierre del año inmediatamente anterior.

2.5.8.24. Capacidad tecnológica para la generación automática de alertas y marcación de irregularidades.

El Sistema de Control y Vigilancia deberá estar dotado de los desarrollos de software, herramientas técnicas y parametrizaciones necesarias para asegurar dos tipos de actuaciones automatizadas, claramente diferenciadas por su origen y efecto:

a) Generación automática de alertas y marcación de servicios por incumplimientos detectados por el sistema:

Cuando el SICOV, por la propia lógica y parametrización interna, detecte un incumplimiento a las reglas definidas explícitamente en el presente Anexo Técnico, procederá a:

1. Generar una "Alerta temprana por incumplimiento", notificando al organismo de apoyo y a la Superintendencia de Transporte.
2. Aplicar una "Marcación de irregularidad" a todos los servicios que se presten o certificados que se expidan mientras la alerta se encuentre activa.
3. Ponerlo en conocimiento de la Superintendencia de Transporte a través del módulo de consulta, IVC e inteligencia de negocio. En los casos de

alertas generadas por ausencia de soportes de cumplimiento de requisitos críticos, se deberá informar al CRC. La información para el CRC será visible en el módulo de administración del SICOV y deberá indicar claramente la naturaleza de la irregularidad y el servicio o servicios afectados.

Esta capacidad de generación de alertas y marcación aplicará, como mínimo, a las siguientes situaciones detectadas por el sistema:

Alertas por posible incumplimiento documental y de operación

- **Vencimiento o ausencia de documentos críticos:** Se generará una alerta si el sistema detecta que un CRC no ha subsanado el vencimiento o la ausencia de documentos críticos para su operación, como son aquellos que dieron lugar a la autorización de su registro en el RUNT. Esta alerta llevará a la marcación de irregularidad de todos los servicios que se presten bajo esa condición.
- **Uso de equipos durante mantenimiento:** Se activará una alerta si el CRC reporta una avería o si un equipo se encuentra en mantenimiento o calibración y el sistema detecta que el equipo se está usando para un servicio en ese período, generando una marcación de irregularidad.
- **Uso de equipos sin mantenimiento:** Si el sistema detecta que un equipo está siendo usado para una prueba sin un mantenimiento o calibración vigente, se generará una alerta de restricción automática y el servicio será marcado.
- **Inconsistencia en los datos de equipos:** Se generará una alerta de marcación si hay una diferencia entre la información de los equipos reportada por el CRC y la evidencia obtenida durante las visitas de verificación, o si se recibe información de equipos no identificados y registrados en el Sistema.
- **Fallas en equipos de evaluación:** El sistema generará una alerta si detecta que un equipo de audiometría, optometría o coordinación motriz está siendo utilizado durante un período de reparación o calibración, lo cual se considera una irregularidad.

Alertas por posible manipulación de datos:

- **Anomalías en la transmisión de datos:** Cualquier interrupción, retención indebida o disposición no autorizada de la información esencial para la continuidad de la función de vigilancia y control será un indicio de irregularidad.
- **Repetición inusual o intentos múltiples:** Se generará una alerta de evento atípico y la correspondiente marcación de irregularidad cuando el Sistema detecte que, para un mismo usuario y dentro del curso de un mismo proceso de certificación, se han registrado tres (3) o más intentos de inicio, reinicio o repetición de un mismo examen (independientemente de si el motivo registrado fue suspensión, fallo técnico o criterio médico).

Otras alertas por posible manipulación de dispositivos o suplantación de identidad:

- **Manipulación de dispositivos SICOV:** Se activará una alerta si se detecta la manipulación, alteración, desinstalación o daño de los equipos del SICOV instalados en las sedes de los CRC.
- **Duplicidad o inconsistencias en el IDClient:** El sistema generará una alerta si se detecta que un CRC está utilizando un identificador único (IDClient) de la RNEC que no corresponda al asignado.
- **Intentos fallidos consecutivos de validación de identidad:** Se registrará una alerta de evento atípico si un usuario del servicio registra en dos o más oportunidades, a lo largo de la prestación del servicio incluyendo la fase de enrolamiento, cuatro (4) o más intentos fallidos de validación de identidad consecutivos utilizando cualquier mecanismo disponible, en cualquier momento del servicio.

Alertas de operación e infraestructura:

- **Interrupciones en la transmisión de datos:** Cualquier interrupción, retención indebida o disposición no autorizada de la información esencial del SICOV generará una alerta y acarreará consecuencias legales.
- **Fallos técnicos de la infraestructura:** El sistema generará alertas ante la ausencia de fluido eléctrico, fallas en la red de comunicaciones o cualquier otro evento que comprometa la disponibilidad del sistema.

Otras alertas:

- El incumplimiento de los parámetros de capacidad instalada o su uso indebido, según se detalla en la función de gestión y control de capacidad.
- La detección de movimientos inusuales de personal y la falta de reporte de desvinculación, conforme a lo establecido en la función de gestión del registro y trazabilidad de personal.
- Identificación de casos en los que la duración de un examen o del proceso completo es inusualmente larga o corta en comparación con el promedio histórico, lo que podría indicar un intento de manipulación en el proceso.
- Cualquier otra situación específica que el presente Anexo Técnico defina como susceptible de generar una alerta automática.

Los promedios de referencia empleados por el SICOV se determinarán a partir del análisis estadístico de los datos históricos recolectados a nivel nacional y serán objeto de actualización cuando así se requiera.

Periodo de estabilización y afinamiento analítico: Sin perjuicio del seguimiento permanente que se le debe hacer a la operación del SICOV, a partir de la entrada en operación del CPD Analítico y de Identificación, se establece un periodo de seguimiento y supervisión especial de seis (6) meses sobre el comportamiento de los modelos de detección de anomalías y los mecanismos de generación de alertas.

Durante este término, se adelantará un análisis técnico sobre los resultados de las marcaciones de irregularidad, con el propósito de evaluar la efectividad de los algoritmos, optimizar la precisión en la identificación de patrones de riesgo y minimizar la ocurrencia de falsos positivos.

Los hallazgos derivados de esta supervisión permitirán realizar ajustes técnicos y de lógica de negocio necesarios para asegurar que el sistema de alertas sea una herramienta de supervisión robusta, objetiva y ajustada a la realidad operativa de los centros, a fin de garantizar la integridad de la información y la eficacia de la función de inspección, vigilancia y control.

b) Trazabilidad de las actuaciones:

Toda alerta generada por el Sistema, deberá quedar registrada de forma inalterable en las bitácoras de auditoría del SICOV, indicando su causal, el momento exacto y los detalles pertinentes para garantizar su plena trazabilidad y valor probatorio ante las autoridades competentes.

Toda alerta que se active en el sistema generará además una marcación de examen de aptitud con la especificación de la causal de activación, y dejará, para efectos de supervisión, un registro informativo detallado con la trazabilidad histórica del servicio marcado.

Con estas evidencias, la Superintendencia de Transporte podrá solicitar, visualizar y descargar informes técnicos de los operadores homologados del SICOV, sobre exámenes de aptitud realizados por CRC de todo el país, según los criterios de aleatoriedad u otros específicos que determine la entidad a través del Comité Técnico Operativo.

La Superintendencia de Transporte, a través del Comité Técnico Operativo, con el apoyo de las herramientas de analítica y de los expertos del SICOV, podrá ajustar y ampliar los parámetros de detección para otros patrones similares de fraude que se puedan identificar en la operación. Esta información será el principal insumo para las actuaciones de Inspección, Vigilancia y Control de la entidad.

c) Registro de medidas adoptadas por la Superintendencia de Transporte:

El SICOV deberá contar con las funcionalidades necesarias para gestionar la información de las medidas de suspensión del servicio ordenadas por la Superintendencia de Transporte y ejecutadas por el RUNT. El sistema deberá garantizar lo siguiente:

Registro de la orden: La Superintendencia comunicará al operador SICOV cada vez que adopte una medida de suspensión en contra de un CRC, así como la información precisa sobre el momento (fecha y hora) exacto en que la medida de suspensión del organismo se haga efectiva en el Registro Único Nacional de Tránsito. Esta información será comunicada a la Superintendencia por parte del concesionario del RUNT y será transmitida desde la entidad a los operadores homologados a través del mecanismo de interoperabilidad o consulta que se desarrolle para el efecto, con la periodicidad que se determine. El SICOV llevará dicho registro de información actualizado.

Contabilización precisa: El SICOV llevará un registro exacto del tiempo transcurrido de ejecución de la medida de suspensión, con base en la información que los operadores reciban. Este registro servirá para efectos de contabilizar y verificar el cumplimiento del tiempo de suspensión.

Esta capacidad de ejecución de órdenes se activará para dar estricto cumplimiento a:

- Cualquier orden administrativa de la Superintendencia de Suspensión preventiva de actividades de un CRC, en ejercicio de las potestades derivadas de la Ley 1702 de 2013, o la norma que la modifique, adicione o derogue.
- Cualquier otra medida administrativa, como la suspensión o cancelación del registro en el RUNT, que sea impuesta mediante acto administrativo en firme y debidamente motivado.

Alertas de cumplimiento de plazos: El sistema generará y enviará notificaciones y alertas automáticas a la Superintendencia con una antelación de diez (10) días hábiles antes de que se cumpla el plazo de la suspensión, a fin de coordinar de manera oportuna la reactivación del servicio y evitar la afectación injustificada de los derechos del administrado.

Esta constancia en el registro servirá para efectos de contabilizar el tiempo exacto de suspensión que haya cumplido un organismo de apoyo, ante las autoridades competentes.

d) Trazabilidad histórica de las actuaciones:

Toda acción ejecutada por el sistema, sea la generación de una alerta, la aplicación de una marcación o la activación de una restricción por orden administrativa, deberá quedar registrada de forma inalterable en las bitácoras de auditoría del SICOV, indicando su causal, el momento exacto y los detalles pertinentes para garantizar su plena trazabilidad y valor probatorio.

e) Alcance de la marcación de irregularidad:

Se entiende por "Marcación de Irregularidad" la etiqueta digital inalterable que el SICOV asocia a un registro de servicio en cualquiera de sus etapas (clase,

curso, evaluación o expedición de certificado). Esta marcación tendrá dos (2) fuentes de activación:

1. **Por causal específica:** Cuando la anomalía se detecta únicamente en el desarrollo de ese servicio particular (ej. presunto intento de suplantación de identidad en una clase, inconsistencia en tiempos de duración, geoposicionamiento del vehículo fuera de zona).
2. **Por causal estructural:** Cuando la anomalía proviene de un incumplimiento de los requisitos de operación del Organismo de Apoyo (ej. documentos que soportan requisitos críticos). En este escenario, el SICOV aplicará la marcación de manera masiva y automática a todos los servicios que se gestionen bajo la vigencia de dicha irregularidad.

En el Módulo de Consulta, IVC e Inteligencia de Negocio, la Superintendencia podrá filtrar y visualizar las irregularidades de cada CRC, discriminando si su origen fue específico o estructural, a través de una opción de consulta por perfil individualizado para cada organismo de apoyo al tránsito.

2.5.8.25. Analítica de datos para la detección proactiva de fraude en los procesos de evaluación.

El Sistema de Control y Vigilancia deberá implementar módulos de analítica de datos avanzados e inteligencia artificial para la detección proactiva de patrones de fraude o comportamientos anómalos en la prestación de servicios por parte de los CRC.

La analítica de datos se utilizará para identificar, entre otras, las siguientes conductas que pueden ser indicativas de manipulación o fraude:

- Inconsistencias en los datos.
- Inconsistencias en las validaciones de identidad.
- Inconsistencias en registros de personal vinculado a los centros.
- Porcentajes de activación de mecanismos de excepción biométrica superiores al 5 % de servicios prestados.
- Cualquier otro patrón de comportamiento o anomalía en los datos de la operación que sea identificado por la Superintendencia de Transporte y que pueda constituir un riesgo de fraude, elusión de controles o incumplimiento normativo.

2.5.8.26. Interoperabilidad entre operadores homologados.

El SICOV deberá garantizar el intercambio de información técnica y operativa de manera automática, recíproca y en tiempo real entre los diferentes operadores homologados, con el fin de garantizar el cumplimiento de las mismas reglas de funcionamiento del Sistema a nivel nacional.

Condiciones generales de la funcionalidad:

Los operadores homologados deberán garantizar el funcionamiento de los mecanismos de interoperabilidad necesarios para asegurar el funcionamiento de los flujos de información y mecanismos de verificación automática previstos en el presente Anexo.

La interoperabilidad se basará en un modelo de reciprocidad absoluta entre operadores homologados. Ningún operador podrá cobrar a otro por las consultas de vinculación o concurrencia, entendiendo que esta funcionalidad es un requisito esencial para la integridad del SICOV.

Para proteger el Habeas Data y evitar el intercambio de bases de datos, todas las consultas de datos personales se realizarán mediante el intercambio de identificadores anonimizados (Hashes). Sólo se deberá acceder a información estrictamente necesaria para efectos de la inspección, vigilancia y control.

Como garantía de trazabilidad de las operaciones de interoperabilidad, el sistema deberá almacenar registros (logs) de las consultas realizadas entre operadores y sus respuestas. Estos logs serán reportados al MOCVI del CPD Analítico y de identificación de la Superintendencia de Transporte y permitirán supervisar la efectividad de la interoperabilidad distribuida.

2.5.8.27. Garantía de disponibilidad del SICOV.

El operador del SICOV deberá garantizar una disponibilidad mínima del software de gestión y todas sus funcionalidades del noventa y nueve punto cuatro por ciento (99,4%), medida mensualmente.

a) La fórmula para el cálculo de la disponibilidad será: [(Tiempo Total del Periodo de Medición - Tiempo Total de Indisponibilidad No Justificada) / Tiempo Total del Periodo de Medición] * 100.

b) El Tiempo Total del Periodo de Medición corresponde al número total de horas en un mes calendario.

c) Se considerará Tiempo Total de Indisponibilidad No Justificada la suma de todos los periodos en los que cualquier funcionalidad crítica del SICOV no esté operativa para los usuarios o la Superintendencia, excluyendo las ventanas de mantenimiento programado debidamente informadas y justificadas en detalle con antelación a la Superintendencia de Transporte y los eventos de fuerza mayor o caso fortuito debidamente comprobados.

d) El operador del SICOV deberá implementar herramientas de monitoreo permanente de la disponibilidad del Sistema y generar reportes en tiempo real, que deberán ser visibles en el Módulo de consulta, IVC e inteligencia de negocio de la Superintendencia de Transporte.

Asimismo, deberá elaborar y remitir a la Superintendencia de Transporte reportes mensuales de operación y disponibilidad del Sistema, informando sobre cualquier evento y/o circunstancia que haya causado indisponibilidad de algún componente del Sistema, la causa de su ocurrencia y las medidas adoptadas para su solución.

Estos informes deberán ser entregados a la Superintendencia de Transporte dentro de los cinco (5) primeros días hábiles de cada mes y deberán también poder descargarse desde el Módulo de consulta, IVC e inteligencia de negocio de la Superintendencia de Transporte.

Ventanas de mantenimiento programado: Las ventanas de mantenimiento programado deberán ser notificadas a la Superintendencia de Transporte y a los CRC con una anticipación mínima de cinco (5) días hábiles, explicando las razones de su realización. En el caso de los CRC, estas deberán informarse a través de los correos registrados por estos centros en el SICOV y a través de avisos visibles en el módulo de administración del software de gestión y control del SICOV para estos organismos.

A la Superintendencia la información deberá transmitirse a la entidad a través del Módulo de consulta, IVC e inteligencia de negocio del CPD Analítico, en donde aparecerá la alerta.

Cambios o mantenimientos de emergencia en el software o la infraestructura: Para los cambios de emergencia en software o infraestructura que requieren atención inmediata para evitar la interrupción del servicio o mitigar fallas críticas, el operador homologado deberá poner en conocimiento de la Superintendencia y de los CRC tales circunstancias de manera inmediata, a través de los canales antes indicados.

Al finalizar los cambios o mantenimientos, deberá entregar posteriormente un informe técnico a la Superintendencia que documente el incidente, las acciones realizadas y los resultados.

2.5.9. Centro de Operaciones de Seguridad (NOC – SOC).

El proveedor del SICOV deberá implementar y operar un **Centro de Operaciones de Seguridad (SOC)**, que operará de manera cooperativa con el Centro de Operaciones de Red (NOC), para monitorear y asegurar de manera proactiva y reactiva la totalidad de la infraestructura tecnológica del SICOV, sus componentes y sus operaciones. El SOC tiene como objetivo principal monitorear, detectar, analizar y responder a incidentes de seguridad, amenazas y vulnerabilidades para minimizar su impacto en el sistema. El NOC tiene como objetivo principal monitorear, gestionar todas las redes de comunicaciones informáticas y de telecomunicaciones que forman parte del SICOV supervisando, manteniendo y asegurando la disponibilidad y rendimiento óptimo 24x7x365.

2.5.9.1. Componentes y funcionalidades principales del SOC

El SOC deberá contar con la infraestructura de hardware y software y las capacidades operativas para desarrollar las siguientes funciones:

2.5.9.1.1. Monitoreo y gestión centralizada de la infraestructura.

El SOC deberá monitorear y gestionar la infraestructura, aplicaciones, redes, almacenamiento, seguridad y rendimiento del SICOV. Deberá contar con una consola de administración para vigilar y controlar toda la infraestructura principal y alterna.

Para ello, deberá:

- Generar alertas proactivas.
- Realizar análisis de tendencias y elaborar reportes técnicos (diarios, mensuales y por eventos).
- Garantizar el acceso a consolas centralizadas y tableros de control para equipos técnicos y de operación.
- Supervisar de manera proactiva el estado y disponibilidad de activos de red y sistemas.

2.5.9.1.2. Gestión de seguridad y prevención de amenazas

El SOC deberá implementar soluciones especializadas para proteger el sistema contra amenazas internas y externas, y gestionar incidentes de seguridad.

2.5.9.1.2.1. Gestión de vulnerabilidades:

Deberá implementar un ciclo continuo de detección, análisis y remediación de vulnerabilidades. Esto incluye realizar pruebas de seguridad, escaneo de vulnerabilidades y gestión de parches y control de cambios.

2.5.9.1.2.2. Gestión y análisis de logs:

Se deberán definir con claridad descripciones y tipos de eventos críticos y efectuar su monitoreo centralizado. El SOC deberá definir e implementar un esquema de alertas ante incidentes, así como registrar y llevar la trazabilidad de los logs de estos eventos.

2.5.9.1.2.3. Detección y respuesta a amenazas:

El SOC debe contar con plataformas y herramientas para:

- **SandBoxing:** Implementación de entornos aislados para el análisis de archivos sospechosos antes de su ejecución en el entorno de producción.
- **Protección Avanzada contra Amenazas (ATP):** Herramientas para la identificación y respuesta ante amenazas persistentes avanzadas (APT), accesos maliciosos o actividades sospechosas internas y externas.

- **Inteligencia artificial:** Contemplar el uso de herramientas de Inteligencia Artificial para realizar análisis predictivo de vulnerabilidades y amenazas.

2.5.9.1.3. Seguridad de endpoints y correo electrónico

Todos los equipos de cómputo y dispositivos móviles que intervienen en la operación del NOC-SOC y del SICOV, al igual que el correo electrónico de dominio corporativo, deben contar con medidas de seguridad provistas por el proveedor. Esto incluye:

- Instalación de una solución Endpoint y un software antivirus y antimalware actualizado en todos los equipos y servidores.
- Control centralizado de dispositivos conectados al SICOV, permitiendo la gestión remota, la prevención de malware vía USB u otros dispositivos y la restricción de uso indebido.
- Seguridad del correo electrónico, con protección ante suplantación de identidad (spoofing), phishing, malware y spam, y autenticación reforzada (DKIM, SPF, DMARC).

2.5.9.1.4. Respaldo y Recuperación de la Información

El SOC deberá contar con herramientas para realizar copias de seguridad (backups) en entornos seguros. Deberá contar con mecanismos de respaldo automatizado y programado, con una retención mínima de 90 días hábiles, y replicación en el CAPD (activo-pasivo).

El proveedor deberá contar con un plan de respaldo de la información que considere la selección de datos, la frecuencia de copias, los métodos de copia (completas, incrementales o diferenciales), los medios de almacenamiento, las pruebas de recuperación y la ubicación de las copias (al menos una copia deberá ubicarse fuera del sitio del CPD).

2.5.9.1.5. Herramientas de seguridad lógica y operación

El SOC deberá disponer de las siguientes herramientas de software para gestionar la seguridad lógica y la operación:

- **SIEM (Security Information and Event Management):** Para la correlación y análisis de eventos de seguridad.
- **Monitor de Infraestructura y Servicios (NOC):** Para la supervisión del estado y disponibilidad de activos de red y sistemas.
- **Sistema de Gestión de Incidentes (ITSM):** Para el registro, seguimiento y resolución de eventos, con ticketing automatizado y escalamiento por criticidad.
- **Plataforma de Automatización de Seguridad (SOAR):** Para la respuesta automatizada ante incidentes, con playbooks de respuesta y automatización de acciones.
- **Analizador de Vulnerabilidades:** Para la identificación proactiva de debilidades técnicas.
- **Detección y Respuesta en Endpoints (EDR):** Para la supervisión y protección de dispositivos finales, con análisis de comportamiento y aislamiento remoto.
- **Gestión de Identidades (IAM):** Para el control de acceso a recursos críticos, con autenticación multifactor y gestión de privilegios.
- **Monitor de Bases de Datos y Aplicaciones:** Para la protección de operaciones y datos en sistemas críticos.
- **CMDB (Configuration Management Database):** Para el inventario y la relación de activos tecnológicos.
- **Plataforma de Inteligencia de Amenazas:** Para la contextualización de riesgos externos conocidos.
- **Log Management (LM) y correlación de eventos:** El SOC deberá operar una plataforma SIEM/SOAR con capacidad para ingesta, normalización y

análisis de eventos de seguridad provenientes de toda la infraestructura del SICOV.

Las funciones de IPS, DAMN, Firewall, ADC y escáner de vulnerabilidades podrán implementarse con equipos, dispositivos o appliance con soluciones multifuncionales, siempre y cuando se encuentren posicionados en los últimos cuadrantes Mágicos de Gartner o Forrester según el caso.

Requisitos mínimos esperados de algunos componentes:

Firewall Perimetral UTM: Solución basada en hardware o software que deberá tener los servicios activos de Firewall, IPS (Intrusion Prevention System), Escáner de Vulnerabilidades de Red y Antivirus de Red. El firewall debe contar con un throughput de 100Gbps; en los servicios de IPS : 20 Gbps y NGFW :10 Gbps como mínimo y fuente redundante y en alta disponibilidad por cada SICOV. La solución deberá encontrarse como Leaders en el Magic Quadrant for Unified Threat Management (UTM) de Gartner.

SIEM: Solución basada en hardware o software para la correlación de eventos de seguridad generados por el equipamiento y aplicaciones de la red de la plataforma tecnol6gica del Sistema de Control y Vigilancia. La solución utilizada deberá encontrarse en el último cuadrante de Leaders del Magic Quadrant Security Information and Event Management (SIEM) de Gartner

WAF - Hybrid Mesh Firewalls (HMF): Solución basada en hardware. Debe tener como mínimo funcionalidades Firewall de Aplicaciones Web, Protección de APIs y Mitigación de Bots. La solución utilizada deberá encontrarse en el último cuadrante de Leaders del Magic Quadrant for Hybrid Mesh Firewalls (HMF) de Gartner

Protección de EndPoint: Solución basada en software para protección antimalware de los servidores utilizados del Sistema de Control y Vigilancia. La solución utilizada deberá encontrarse en el último cuadrante de Leaders del Magic Quadrant for Endpoint Protection Platforms.

2.5.9.1.6. Desarrollo de aplicaciones y entornos de prueba

El SOC que disponga el homologado para la operación del SICOV deberá contar de la infraestructura requerida para crear e implementar ambientes independientes para el desarrollo de software, pruebas y producción. Deberá contar con herramientas y equipo de soporte para la gestión de contenedores y orquestadores (Docker, Kubernetes, OpenShift, entre otros). También debe gestionar la integración con herramientas de desarrollo colaborativo, control de versiones y automatización CI/CD.

2.5.10. Infraestructura tecnológica en los CRC para el funcionamiento del software SICOV

Los CRC deberán contar con la infraestructura tecnológica necesaria para la correcta operación del SICOV en sus instalaciones. El operador homologado del SICOV será el responsable de suministrar, instalar, configurar, mantener y soportar todos los dispositivos y periféricos mínimos necesarios, conforme a lo aquí previsto, así como de asegurar la compatibilidad y el adecuado funcionamiento del software del SICOV con cada uno de estos.

Los requisitos que se establecen a continuación son de carácter **mínimo**. El proveedor deberá garantizar que el *hardware* y *software* suministrados y operados estén en capacidad de soportar todas las funcionalidades del SICOV y que, ante la aparición de nuevas y mejores tecnologías que reemplacen o superen lo aquí previsto, la infraestructura sea actualizada para evitar la obsolescencia tecnológica y garantizar la mejora continua del sistema, previa validación y directriz de la Superintendencia de Transporte a través del Comité Técnico Operativo para el Fortalecimiento del SICOV.

Los operadores homologados del SICOV tendrán libertad para adquirir equipos de hardware y/o solución tecnológica especializada de cualquier marca, siempre que cumpla con las condiciones y funcionalidades mínimas exigidas por la Superintendencia en este acápite.

Será responsabilidad del proveedor homologado del SICOV garantizar la correcta integración de su software con los equipos adquiridos y/o empleados por el organismo de apoyo para prestar el servicio, y prestar el soporte técnico sobre dicha integración.

Como referentes técnicos mínimos esperados, se describirán detalles y características técnicas mínimas exigidas para la tecnología esperada, con miras a lograr un adecuado y efectivo funcionamiento de la infraestructura técnica que soporta la prestación del servicio y asegura la veracidad de la información operativa.

Características mínimas de los componentes esperados de hardware y software para el funcionamiento del SICOV:

2.5.10.1. Hardware para el funcionamiento del SICOV

Los operadores homologados del SICOV deberán suministrar y soportar dispositivos y periféricos, con las características y funcionalidades mínimas que a continuación se detallan, que permitan la operación segura y eficaz del sistema en cada Centro de Reconocimiento de Conductores:

2.5.10.1.1. Lectores biométricos especializados de huellas

Los lectores de huellas especializados que se utilizarán para validar biométricamente la identidad de usuarios y personal del CRC deberán tener como mínimo la tecnología que ofrecen huelleros especializados como los que a continuación se referencian, cuyas características mínimas se detallan:

En cualquier caso, los dispositivos de lectura de huellas dactilares que se utilicen deberán contar con la homologación por parte de la Registraduría Nacional del Estado Civil (RNEC).

Requisitos técnicos detallados:

2.5.10.1.1.1. Lector de huella multiespectral

FUNCIONES Y CARÁCTERÍSTICAS	
Tecnología	Imagen Multiespectral - Multispectral Imaging (MSI)
Template Extractor y Matcher	MINEX III Certificado
Resolución de imagen de salida / Profundidad de bits	500 dpi / 8-bit, 256 escala de grises
Formato de salida de imagen	Imágenes sin comprimir o comprimidas WSQ (certificadas por el FBI)
Formato de salida de plantilla	ANSI 378 / ISO 19794-2 / ISO-19784 (MINEX III certificado)
Match sobre dispositivo	Entradas de plantilla ANSI 378 / ISO 19794-2
Adquisición de imágenes	Adquisición de imágenes estructuradas (SIA) para mayor velocidad, rechazo de la luz ambiental y calificación de la posición de los dedos
USB	USB 2.0 alta velocidad (480 Mbps)
Sistemas Operativos	Windows 10/11; Linux x86/x64
SEGURIDAD	

Detección de Ataques de Presentación (PAD) / Detección de Dedos en Vivo (LFD)	-ISO/IEC 30107-3, Level 2 Presentation Attack Detection (PAD) Certificado. -Multispectral Imaging (MSI), Live Finger Detection (LFD)
Protección física contra manipulaciones	Actualizaciones de firmware cifradas Elemento seguro con borrado de clave activa
Criptografía	AES 128/256, TDES 2/3 Key, SHA-256, RSA-2048
Número de claves simétricas de usuario	10
ID estática única	64 bits
Generador de bits aleatorios determinista (DRBG)	NIST CAVP Certificado
SOPORTE DEL MODELO DE TRANSACCIÓN	
Inyección de llave de fábrica	Soportado
Sesión maestro/esclavo	Soportado
Remote Key Load (RKL)	Soportado

2.5.10.1.1.2. Lector de huella óptico infrarrojo:

FUNCIONES Y CARÁCTERÍSTICAS	
Tecnología	Optical technology que cuentes con Diodos emisores de luz (LED) infrarroja
Template Extractor y Matcher	MINEX III Certificado
Resolución de imagen de salida / Profundidad de bits	500 dpi / 8-bit, 256 escala de grises
Formato de salida de imagen	Imágenes sin comprimir o comprimidas WSQ (certificadas por el FBI)
Formato de salida de plantilla	ANSI 378 / ISO 19794-2 / ISO-19784 (MINEX III certificado)
Match sobre dispositivo	Entradas de plantilla ANSI 378 / ISO 19794-2
Adquisición de imágenes	Adquisición de imágenes estructuradas (SIA) para mayor velocidad, rechazo de la luz ambiental y calificación de la posición de los dedos
USB	USB 2.0 alta velocidad (480 Mbps)
Sistemas Operativos	Windows 10/11; Linux x86/x64
SEGURIDAD	
Detección de Ataques de Presentación (PAD) / Detección de Dedos en Vivo (LFD)	-ISO/IEC 30107-3, Level 2 Presentation Attack Detection (PAD) Certificado / Live Finger Detection (LFD)
Protección física contra manipulaciones	Actualizaciones de firmware cifradas Elemento seguro con borrado de clave activa
Criptografía	AES 128/256, TDES 2/3 Key, SHA-256, RSA-2048
Número de claves simétricas de usuario	10
ID estática única	64 bits
Generador de bits aleatorios determinista (DRBG)	NIST CAVP Certificado

SOPORTE DEL MODELO DE TRANSACCIÓN	
Inyección de llave de fábrica	Soportado
Sesión maestro/esclavo	Soportado
Remote Key Load (RKL)	Soportado

Ubicación: Estos dispositivos deberán estar instalados **(i)** en la recepción de los CRC para el enrolamiento inicial del personal y los usuarios servicio, así como en **(ii)** los puntos de validación de identidad ubicados al interior de los consultorios en los que se realizan los diferentes exámenes, conforme se detalla en las siguientes líneas.

Los lectores de huella a los que se hace referencia podrán estar incorporados o integrados en tabletas, siempre que esta integración sea segura y facilite la realización del proceso con eficiencia.

2.5.10.1.2. Dispositivo fijo o móvil con Cámara para captura de fotografías y validación de identidad:

Debe permitir la captura de fotografías para el uso del software de decodificación de la información de documentos de identidad (tecnología OCR) y verificación de autenticidad de documentos (tecnología Document Liveness Detection) a través del software de las capacidades descritas en este Anexo Técnico.

Deben permitir la captura de fotografías para el enrolamiento inicial del personal y usuarios del organismo de apoyo al tránsito y para la realización de los procesos de validación de identidad con software de reconocimiento facial.

Estos dispositivos deberán estar instalados (i) en la recepción de los CRC y en (ii) los puntos de validación de identidad ubicados al interior de los consultorios en los que se realizan los diferentes exámenes.

Deberán contar con cámaras de sensor digital de alta definición que produzcan imágenes nítidas con alto grado de detalle, compatibles con la tecnología de reconocimiento facial descrita en este Anexo Técnico.

2.5.10.1.3. Dispositivos para la validación de identidad en recepción y consultorios:

Los proveedores homologados del SICOV deberán suministrar y soportar dispositivos móviles (tipo tablet o móvil) que permitan la captura de fotografías y la realización de procesos de validación de identidad mediante software de reconocimiento facial. Estos dispositivos, provistos por el proveedor del Sistema, deberán ser instalados o ubicados de la siguiente manera, según la naturaleza del servicio prestado por el organismo de apoyo:

1. **Ubicación:**

La recepción y todos los consultorios del CRC deberán contar con puntos fijos de validación de identidad de usuarios y del personal de la salud.

2. **Especificaciones técnicas mínimas:** Estos dispositivos deberán contar con las siguientes características:

    - **Cámaras:** Cámaras de sensor digital de alta definición que produzcan imágenes nítidas con alto grado de detalle, compatibles con la tecnología de reconocimiento facial descrita en este Anexo Técnico.

    - **Tecnología de GPS:** Integrada para georreferenciación.

3. **Capacidades integradas de validación de identidad (biometría dactilar):** En los puntos del establecimiento o sede del CRC, estos dispositivos móviles deberán contar adicionalmente con un huellero (lector biométrico especializado) integrado de forma segura y dedicada, homologado por parte de la Registraduría Nacional del Estado Civil. De esta manera, los puntos de validación de identidad de los participantes asegurarán:

    - Capacidad para realizar reconocimiento facial, compatible con la tecnología de reconocimiento facial descrita en este Anexo Técnico.
    - Capacidad para realizar la validación de identidad a través de cotejo de minucias dactilares contra las réplicas de la base de datos de la RNEC.

4. **Uso y función complementaria:** Estos puntos de validación serán indispensables para la validación de identidad de usuarios e instructores al inicio y al final de las clases teóricas y cursos. Asimismo, funcionarán como mecanismo alternativo para la revalidación durante la clase o curso, en caso de que la persona no sea reconocida con la tecnología de reconocimiento facial instalada al interior del aula (como cámaras tipo domo).

Estos puntos serán indispensables para la validación de identidad de usuarios y personal de la salud al inicio y al final de cada examen.

2.5.10.1.4. Pad de firmas digitalizador

Para la captura de la firma manuscrita digitalizada de los usuarios y personal del organismo de apoyo.

El pad de firmas servirá para obtener la autorización previa, expresa e informada del personal del organismo de apoyo y de los usuarios del servicio, para el tratamiento de sus datos personales y biométricos a través del SICOV, informándoles claramente sobre las finalidades del tratamiento, el uso de tecnologías de reconocimiento facial, monitoreo de permanencia, y demás aspectos relevantes conforme a la Ley 1581 de 2012 y las demás normas reglamentarias.

2.5.10.1.5. Infraestructura descentralizada para el reconocimiento facial:

Los operadores homologados del SICOV deberán instalar infraestructura descentralizada en la sede de los organismos de apoyo, a fin de permitir el funcionamiento eficiente de los equipos y la tecnología de reconocimiento facial (SDK de captura, liveness y margen) deben contar con lo mínimo exigido por fabricante, tener en cuenta la GPU o CPU según su fabricante.

Los equipos y la tecnología para el reconocimiento facial deben contar con lo mínimo exigido por fabricante, teniendo en cuenta las necesidades de GPU o CPU que indique el fabricante.

Deberá instalarse una NAS con capacidad de almacenar la información necesaria para la validación biométrica facial, registros y log transaccionales del CRC, atendiendo la política de conservación de información indicada por la Superintendencia de Transporte.

Al ser instalado en los centros, deberá disponerse también de un armario o rack de protección y una UPS Online con autonomía de 4 horas para soportar la operación por caída del servicio de energía. El operador deberá garantizar alta disponibilidad y redundancia para esa tecnología desplegada.

El proveedor del SICOV deberá garantizar la infraestructura de procesamiento necesaria para garantizar el funcionamiento eficiente de los componentes, equipos y la tecnología de reconocimiento facial, cumpliendo estrictamente con

las exigencias previstas en el presente Anexo, con los ANS definidos y la eficiencia requerida para la normal operación de los CRC.

La infraestructura debe cumplir con normativa de seguridad informática y protección de datos biométricos, asegurando trazabilidad y auditoría.

Se relacionan, a continuación, se relacionan las características mínimas de cada componente que se deberán garantizar:

2.5.10.1.5.1. Workstation

Requisitos mínimos:

- Procesador: Arquitectura x86-64, mínimo 8 núcleos físicos (Core i9, Ryzen 9, Xeon, o equivalentes de generaciones recientes con soporte vigente del fabricante).
- Memoria RAM: 64GB DDR5
- Almacenamiento: Disco de Estado Sólido (SSD) de 1 TB ó Superior
- RAID: 5/6
- Puertos Ethernet RJ45: 2 x2.5 GbE
- Ranuras PCIe: 2 Generación 3 para expansión
- Tarjeta de Video: Unidad de procesamiento gráfico independiente con soporte para librerías de inteligencia artificial. Deberá contar con una memoria de video dedicada (VRAM) mínima de 24 GB, capaz de procesar inferencias de modelos biométricos en un tiempo no superior a dos (2) segundos por validación. Debe tener 512 núcleos de tensor de cuarta generación o superior, con una GPU que sirva como multiplicador de rendimiento y de aceleración para garantizar la eficiencia de la tecnología de reconocimiento facial.

2.5.10.1.5.2. NAS

Requisitos mínimos:

- Bahías: 6
- Procesador: Quad Core AMD Ryzen ó Intel Core I5 ó I7Compatible (ó Superior)
- Memoria RAM: 16GB expandible

2.5.10.1.5.3. Switches de red administrables:

Los switches administrables capa 3, deberán contar con funcionalidades de Seguridad como son:

- Control de Acceso a Puertos y Seguridad de puertos. Permitiendo restringir el acceso a la red solo a dispositivos autorizados, basándose en sus direcciones MAC y que pueda configurarse para que un puerto solo acepte tráfico de una lista específica de direcciones MAC.
- Listas de Control de Acceso (ACL): Deben definir reglas para permitir o denegar el tráfico de red específico, basándose en varios criterios como direcciones IP, direcciones MAC, números de puerto o protocolos.
- VLAN (Segmentación de Red): La segmentación lógica de la red en diferentes dominios de difusión (VLANs) aísla el tráfico y hace más difícil que los intrusos accedan a otras partes de la red.
- Seguridad contra Suplantación: Deberá incluir funciones integradas para proteger contra amenazas como los ataques de suplantación de ARP (ARP spoofing).
- Monitoreo y Gestión Segura: Deben soportar protocolos de gestión segura como SNMPv3 (Simple Network Management Protocol versión 3) para el monitoreo de la red, y SSH/SSL para un acceso de gestión cifrado.

Capacidades de Enrutamiento

- Capa de operación: Deberá Operar tanto en la capa de enlace de datos como en la capa de red, combinando la funcionalidad de un switch tradicional con la de un router. Deberá reenviar paquetes IP utilizando direcciones IP y debe realizar enrutamiento entre diferentes segmentos de red o VLANs.
- Deberá utilizar protocolos de enrutamiento (como OSPF o BGP, de forma más sencilla que un router dedicado) y mantener tablas de enrutamiento para tomar decisiones sobre la mejor ruta para el tráfico.
- Contar con capacidad para redes más grandes que requieren una conectividad VLAN robusta y un rendimiento de enrutamiento más rápido dentro de la red local (LAN).

2.5.10.1.5.4. SAI o UPS:

Se debe suministrar, instalar y configurar una UPS On-Line de Doble Conversión UPO de 3KVA 3.000va/2700w. Monofásica. Onda SENO para RACK. Respaldo mínimo: 15 min a media carga -7 minutos a full carga, con opción de crecimiento con banco adicional y monitoreo remoto desde el SOC.

A esta UPS se deben conectar y debe soportar el rack de comunicaciones que contiene los equipos que integran el Sistema de Control y Vigilancia para los Centros de Reconocimiento de Conductores.

2.5.10.1.5.5. Rack de equipos.

Con las siguientes características mínimas:

- Rack de piso, tipo metálico con pintura electrostática, con llave y con rodachinas.
- Altura mínimo de 1.80 metros, 38 Unidades de Rack.
- Compuerta de seguridad y alarma antivandálica.

2.5.10.2. Software y componentes de software especializados requeridos para el funcionamiento del software SICOV CRC

El operador homologado del SICOV deberá disponer del software y/o componentes de software necesarios que garanticen que el software SICOV cumpla con cada una de las funcionalidades tecnológicas descritas. Por lo tanto, el aspirante o actual homologado será el responsable de configurar, mantener y soportar el software aquí descrito, así como de asegurar la compatibilidad y su adecuado funcionamiento dentro del software del SICOV:

2.5.10.2.1. Software de reconocimiento facial para validación de identidad

El operador homologado deberá incorporar al software SICOV un servicio/tecnología de reconocimiento facial de alto rendimiento y eficiencia, especialmente diseñado para la identificación de personas a través de:

- Validación de identidad selfie vs. documento.

Esta solución deberá mostrar efectividad en la validación de identidad aún con eventos de obstrucción de rostro como el uso de gafas formuladas, cambios en la expresión facial, condiciones difíciles de iluminación y rotaciones moderadas de rostro.

Para el adecuado funcionamiento de la tecnología de reconocimiento facial se deberá advertir a los usuarios del servicio que el uso de cualquier otro accesorio durante la prestación del servicio no está permitido.

El servicio debe tener mínimo las siguientes características:

- Capacidad de trabajar sobre cámaras IP de alta resolución,

- Realizar la validación de identidad de manera automática (sin intervención humana) y no invasiva,
- Capacidad para identificar personas a partir de una o varias fotografías o video (templates).
- Contar con una API de integración disponible para integrarse al SICOV.

1. **Componentes técnicos:**

El software de reconocimiento facial debe contar, como mínimo, con los siguientes componentes técnicos:

SDK o APK que permita hacer captura automática de foto para el proceso de detección de vida y cifrado de foto.

En el momento del enrolamiento inicial, la captura de fotografía que constituirá el patrón biométrico de referencia (template) se hará atendiendo lo previsto por la ICAO (Organización de Aviación Civil Internacional) para reconocimiento facial, atendiendo, entre otras, y como mínimo, las siguientes:

- La fotografía debe mostrar ambos ojos con claridad (Eyedistance)
- El rostro debe estar mirando directamente a la cámara (Non_frontal)
- La imagen debe tener un foco nítido y claro (Blurred)
- Se requiere iluminación, brillo y contraste adecuados (Bad_lighting).
- No debe haber exceso de brillo o reflejos que afecten la calidad (Hot_spots).
- El rostro debe ocupar el 80% o más de la fotografía (Low_dynamic).
- Los ojos deben estar abiertos y claramente visibles (Eye_closed).
- Se requiere una exposición neutra, sin filtros ni efectos (Bad_exposure).
- No debe haber reflejos en los lentes (gafas) (Glasses_reflections).

Para la validación de identidad de los usuarios antes y después los exámenes, en los términos dispuestos en este Anexo Técnico, también será necesario el cumplimiento de lo previsto en la norma de la ICAO.

2. **Algoritmo de reconocimiento de rostro vivo o liveness detection** (activo o pasivo) certificado por el NIST o por un laboratorio autorizado por el NIST en ataques de presentación PAD nivel 1 y 2 con fecha de presentación no mayor a dos años. El agoritmo debe contar con un APK o SDK para dispositivos móviles por lo menos compatibles con sistemas operativos iOS y Android.

3. **Cotejador facial (matcher):** los algoritmos de cotejo facial deben estar certificados por el NIST en:

- Face Recognition Technology Evaluation (FRTE) 1:1.
- Galería MUGSHOT, Prueba MUGSHOT ΔT ≥ 12 YRS debe ser menor o igual a 0.0040 puntos de precisión.
- Galería VISA Prueba Border. El resultado debe ser menor o igual a 0.0040 puntos precisión.

La fecha de presentación de las pruebas no puede ser superior a los 2 años y deberán realizarse nuevamente cada 2 años. Las constancias del cumplimiento de esta obligación se remitirán a la Superintendencia dentro del mes siguiente a la obtención de los resultados.

2.5.10.2.2. Software MRZ OCR + PDF 417 para verificar autenticidad de documentos de identidad y proteger contra el fraude.

El operador homologado deberá contar con un software que permita hacer Reconocimiento Óptico de Caracteres de la Zona Legible por Máquina (MZR OCR), es decir, que pueda leer y extraer datos de los documentos de identidad presentados por el personal y usuarios del organismo de apoyo del en el momento de su enrolamiento inicial en el software del SICOV.

El software deberá, igualmente, ofrecer protección integral contra el fraude de identidad, incorporando tecnologías avanzadas como verificación de vida (Document Liveness Detection Technology). Estas funcionalidades deberán permitir verificar su autenticidad e integridad para prevenir el fraude.

2.5.10.2.3. Software de gestión de tickets y Mesa de Ayuda.

El operador homologado deberá contar con un software de gestión de tickets para la operación de la Mesa de Ayuda del SICOV.

2.5.10.2.4. Software de Mobile Device Management (MDM).

El operador homologado deberá contar con una herramienta que permita administrar, supervisar y proteger los dispositivos móviles y equipo de cómputo que será dispuesto y entregado por estos a los CRC, así como los que sean adquiridos directamente por los últimos para la prestación del servicio, en los términos señalados en el presente Anexo y según determine la Superintendencia de Transporte.

2.5.10.2.5. Software para la de identificación de geoposición (GPS) de equipos de cómputo

Para gestionar la geolocalización de los equipos de cómputo fijos empleados en el CRC para la prestación del servicio, el operador homologado deberá contar con una solución integral de gestión de geolocalización de equipos de cómputo que reúna tres componentes: (i) una etiqueta adhesiva de control de activos, (ii) un gateway o puerta de enlace y (iii) un software o plataforma de gestión y control del mismo fabricante, que reúnan como mínimo las siguientes características:

a) Etiqueta o tamper bluetooth con botón antimanipulación para control de activos que en el caso de ser removido a la fuerza genere una señal de alarma al servidor y a la administración del Sistema.

Esta tecnología deberá reunir las siguientes especificaciones de fábrica como mínimo:

- Conexión - Bluetooth LE 5.0
- Botón antimanipulación y alarma.
- Chip serie nRF52
- Rango de transmisión o cobertura - 150 metros
- Configurable en la plataforma del fabricante
- Certificado de Protección IP65(impermeable y polvo)
- Temperatura de Funcionamiento -20°C ~ 60°C
- Batería tipo CR 220mAh
- Vida útil o autonomía de 2 años.
- Debe garantizar la inalterabilidad.
- Debe permitir conectarse por bluetooth a un gateway o puerta de enlace del mismo fabricante.

b) Gateway o puerta de enlace bluetooth para IoT (Internet de las Cosas), a donde se conectarán a través de Bluetooth diferentes tipos de sensores o dispositivos IoT, como las etiquetas o tamper descritos en el literal anterior.

Esta puerta de enlace deberá tener las siguientes características como mínimo:

- Procesador: CPU 575Mhz 32-bit Procesador de Aplicación
- Memoria Flash: 16 Mbyte SPI NOR
- Memoria RAM: 64 Mbyte 16-bit DDR2
- Conexión Ethernet: 10/100 con conexión PoE 802.3
- Soporta: HTTP (SSL/TLS) / MQTT (SSL /TLS & Proxy) /TCP
- 2 Puertos USB 2.0

- Slot TF card o U disk de almacenamiento portable.
- Compatible con: Plataformas en la nube AWS/Azure/Google IoT/ARM mBed Iot Cloud.
- Temperatura de Funcionamiento: -25°C ~ 65°C
- Actualización de Firmware: por método OTA (Sobre el Aire)
- CPU Wi-FI y WPA 2.0 de cifrado empresarial para seguridad y transmisión de datos, que permita parametrizar los equipos de cómputo a través de una geo-cerca de 50mt controlada a través del software o plataforma del fabricante.
- Tecnología de comunicación inalámbrica de bajo consumo y de Largo alcance LoRa para IoT con arquitectura de red LoRaWAN (gestión de red, seguridad y administración de dispositivos).

Especificaciones de Bluetooth

- Conexión Bluetooth LE 5.0 (Baja Energía) Procesador 64Mhz 32bit.
- Chip amplificador de potencia incorporado que escanea con precisión el BLE. Soporte al menos bluetooth 4.0 (solo para BLE)
- Frecuencia Bluetooth: 2.4-2.4835 Ghz
- Modulación Bluetooth: GFSK
- Emitiendo Potencia: 18dBm (máx.)
- Número de paquetes de difusión recibidos: cerca de 400 paquetes por segundo.
- Cobertura de Escaneo: cerca de 300 metros de radio cubierto (área abierta)

Rendimiento WiFi RF

- Conexión WiFi IEEE 802.11 b/g/n
- Frecuencia 2.4 GHz
- Velocidad de transferencia de 2T2R 300Mbps
- Modos de Modulación DBPSK, DQPSK, CCK y OFDM (BPSK/QPSK/16-QAM/64-QAM)
- Encriptación inalámbrica PSK WPA /WPA2-PSK, WPA-EAP/WPA2-EAP Y TKIP
- Debe soportar configuración WIFI con Failover y conmutación de wifi de múltiples Puntos de Acceso (support wifi failover & Mult-Higher Level AP)

Consideración sobre la integración de componentes:

Con el objetivo de garantizar la seguridad, integridad e inalterabilidad de la información de geoposicionamiento, se recomienda el uso de soluciones integrales (hardware y firmware del mismo ecosistema). Sin perjuicio de lo anterior, se permite la integración de componentes de distintos fabricantes (Tag y Gateway) siempre y cuando el Operador Homologado certifique y garantice técnicamente que:

- La comunicación entre la etiqueta (Tag) y la puerta de enlace (Gateway) se realiza mediante protocolos seguros y cifrados que impidan la clonación o repetición de señales.
- La solución integrada es capaz de detectar y reportar en tiempo real cualquier intento de manipulación física (tamper) o desvinculación del dispositivo.

El Operador Homologado asumirá la responsabilidad integral por cualquier vulnerabilidad de seguridad derivada de la integración de componentes heterogéneos.

2.5.10.3. Gestión de la infraestructura y la obsolescencia tecnológica

Los operadores homologados del SICOV por la Superintendencia de Transporte deberán:

- Mantener actualizado y reportar el equipamiento tecnológico desplegado en los CRC, conforme a las disposiciones técnicas y de reporte de la Superintendencia de Transporte.
- La actualización del *hardware* y *software* deberá ser proactiva, incorporando las mejores tecnologías disponibles en el mercado que cumplan con los objetivos de seguridad, eficiencia y transparencia del SICOV. La Superintendencia podrá emitir directrices específicas sobre la adopción de nuevas tecnologías o la discontinuación del soporte a versiones obsoletas de *hardware* o *software* base.
- En todo caso la renovación tecnológica de los equipos de cómputo y dispositivos móviles provistos por el operador homologado se deberá realizar cada cuatro (4) años, contabilizados a partir de la fecha de instalación por parte de los organismos de apoyo.

2.5.11. Visitas y requerimientos de verificación técnica y tecnológica a los operadores homologados del SICOV

2.5.11.1. Objetivo de las visitas de verificación

Las visitas de verificación y requerimientos de información tienen como objetivo principal validar el cumplimiento inicial y permanente de las condiciones, obligaciones y requerimientos jurídicos, administrativos, financieros, técnicos y de operación establecidos en el presente Anexo Técnico y demás actos administrativos que lo complementen, por parte de los operadores homologados SICOV para el sostenimiento y actualización de su homologación.

2.5.11.2. Alcance y modalidad de las visitas

La Superintendencia de Transporte, a través del personal delegado para tal fin, realizará las visitas que determine necesarias a todas las sedes y componentes de la infraestructura del SICOV, sin limitación alguna, incluyendo:

- Las instalaciones del **Centro de Procesamiento de Datos** principal y de respaldo (CAPD) del proveedor del SICOV, o las del tercero con quien tenga contratado este servicio.
- Las instalaciones/equipos del **NOC-SOC** del homologado, o las del tercero con quien tenga contratado este servicio.
- Las sedes de los Centros de Reconocimiento de Conductores a los que el actual proveedor preste el servicio del SICOV.
- Cualquier otra ubicación relevante donde se operen o gestionen componentes críticos del SICOV.

Las visitas podrán ser programadas o no programadas (sorpresivas), de acuerdo con los criterios de la Superintendencia de Transporte.

Para la verificación del cumplimiento inicial de condiciones, obligaciones y requerimientos exigibles conforme a lo desarrollado en el presente Anexo se deberán realizar visitas a al menos dos (2) Centros de Reconocimiento de Conductores a los que el actual proveedor preste el servicio del SICOV.

2.5.11.3. Procedimiento general de la visita de verificación

Durante las visitas, el personal de la Superintendencia de Transporte llevará a cabo las siguientes acciones, de manera enunciativa más no limitativa:

2.5.11.3.1. Verificación del cumplimiento de requerimientos.

Se verificarán los diferentes componentes y funcionalidades del SICOV para constatar el cumplimiento de las condiciones, requisitos y obligaciones descritos en el presente Anexo Técnico y sus complementos. Esta verificación incluirá, pero no se limitará a:

- La idoneidad y seguridad de la **infraestructura tecnológica centralizada** (CPD, CAPD, redes), conforme a los estándares y requisitos establecidos.
- La operación y capacidades del **Centro de Operaciones de Seguridad (NOC-SOC)**, incluyendo sus componentes, herramientas de monitoreo y controles de seguridad.
- El correcto funcionamiento y la integridad del **software de gestión y control del SICOV**, abarcando la totalidad de las funcionalidades tecnológicas exigidas (gestión de registros, autenticación, expedición de certificados, registros, interoperabilidad, etc.).
- La correcta implementación y operación de los **dispositivos y tecnologías en los organismos de apoyo** (lectores, capturadores, computadores, etc), su vinculación al sistema y su inalterabilidad.
- El desempeño de los **operadores y aliados externos** (recaudo, biométricos) y su conformidad con los niveles de servicio y requisitos acordados.
- La aplicación de los **controles automáticos y restricciones** definidos en el SICOV ante incumplimientos o inconsistencias.

2.5.11.3.2. Realización de pruebas y comprobaciones.

Para cerciorarse del efectivo cumplimiento y la integridad del Sistema, el personal de la Superintendencia de Transporte realizará durante las visitas las pruebas técnicas y operativas que considere necesarias, incluyendo, entre otras:

- Pruebas de funcionalidad de las características del software.
- Comprobaciones de seguridad, integridad y disponibilidad de la información.
- Pruebas de validación de identidad de usuarios y profesionales de la salud.
- Verificaciones de la trazabilidad y geolocalización de operaciones.
- Pruebas de resistencia del sistema ante intentos de vulneración o frustración de funcionalidades.

2.5.11.3.3. Recopilación de evidencia y colaboración.

El personal que en representación de la Superintendencia realice las visitas, registrará las evidencias documentales, fotográficas, fílmicas y todas las demás que sean necesarias para demostrar el estado de cumplimiento de los requerimientos. Los operadores homologados del Sistema y los organismos de apoyo deberán brindar todo el apoyo y la información necesaria, y poner a disposición todos los recursos técnicos y humanos requeridos para facilitar al personal de la Superintendencia el cumplimiento de su objetivo de verificación.

2.5.11.3.4. Consecuencias del incumplimiento detectado en visita u acciones de verificación

El hallazgo de incumplimientos a las condiciones y requerimientos establecidos en el presente Anexo Técnico durante las visitas de verificación o en los ejercicios de verificación de cumplimiento de obligaciones podrá dar lugar, según la gravedad y reiteración de la falta, y en los términos que establezca la Superintendencia, a:

- Requerimientos para la subsanación en un plazo perentorio.
- La aplicación de restricciones automáticas del uso del SICOV, conforme a lo establecido en el presente Anexo Técnico.
- El inicio de procesos administrativos sancionatorios por parte de la Superintendencia de Transporte, sin perjuicio de las demás acciones legales a que haya lugar.
- La adopción de las medidas administrativas que resulten necesarias para la garantía del eficiente ejercicio de las funciones de inspección, vigilancia y control.

2.5.12. Centro de Procesamiento de Datos Analítico y de Identificación y Módulo de Consulta, IVC e Inteligencia de Negocio (MOCVI)

Con el objetivo de garantizar la independencia entre la operación transaccional crítica del servicio y las labores de procesamiento masivo de datos para la vigilancia, los operadores homologados deberán implementar, operar y mantener una infraestructura tecnológica dedicada exclusivamente a la analítica, consulta y visualización de datos de la operación de los CRC y del SICOV (CPD Analítico y de Identificación).

Esta infraestructura será la fuente única y oficial para el despliegue del "Módulo de Consulta, IVC e Inteligencia de Negocio" (MOCVI) de la Superintendencia de Transporte, asegurando que las consultas masivas, la generación de reportes y la ejecución de modelos de inteligencia artificial no degraden el rendimiento ni la disponibilidad del SICOV operativo en los CRC.

2.5.12.1. Arquitectura y condiciones de infraestructura del CPD-Analítico y de Identificación

El CPD – Analítico y de Identificación constituye la infraestructura tecnológica centralizada mediante la cual se consolida, almacena, procesa y analiza la información proveniente de la operación. Su implementación deberá cumplir con las siguientes especificaciones técnicas de hardware, comunicaciones y seguridad:

1. **Redundancia y ubicación:** El CPD - Analítico y de Identificación deberá estar conformado obligatoriamente por dos sitios físicos independientes:

    - Un Centro de Procesamiento Analítico Principal (CPD-A).
    - Un Centro Alterno de Procesamiento Analítico (CAPD-A).
    - **Condición de operación:** Ambos deberán operar en esquema activo-pasivo o activo-activo, capaces de asumir el 100% de la carga operativa en caso de contingencia.
    - **Georreferenciación:** Las dos instalaciones deberán ubicarse dentro del territorio de la República de Colombia, en zonas geográficas distintas, a una distancia física no superior a 50 km (para garantizar replicación síncrona o asíncrona eficiente) pero suficiente para mitigar riesgos de desastres localizados.
    - **Certificación:** Ambos centros deben cumplir, como mínimo, con las características de la certificación TIA-942 TIER III.

2. **Capacidad de Procesamiento y servidores:**

    - **Arquitectura:** Servidores empresariales en configuración redundante N+1 o 2N, organizados en granjas físicas y/o virtuales.
    - **Potencia de Cómputo:** Procesadores multinúcleo de última generación (mínimo 32 núcleos físicos por nodo).
    - **Aceleración para IA:** Incorporación obligatoria de unidades de procesamiento gráfico (**GPU**) con soporte para tecnologías como CUDA o Tensor Cores, dimensionadas para soportar el procesamiento de modelos de machine learning, el Subsistema ABIS de reconocimiento facial y la inferencia en tiempo real.

3. **Almacenamiento no estructurado y Data Lake:**

    - **SAN (Storage Area Network):** Arquitectura redundante 2N para datos calientes, con capacidad inicial mínima de 50 TB escalable, latencia de acceso inferior a 5 ms y replicación síncrona o asíncrona entre el CPD-A y el CAPD-A.

El esquema de replicación deberá garantizar un Punto de Recuperación (RPO) de máximo treinta (30) minutos, asegurando que ante una eventualidad, la pérdida de información sea marginal y no afecte la integridad probatoria del sistema.

- **Almacenamiento no estructurado y Data Lake: NAS (Network Attached Storage):**

  Para el almacenamiento histórico, evidencias biométricas y datasets de entrenamiento de modelos de IA, se deberá disponer de una solución tipo NAS o Almacenamiento Definido por Software (SDS) que cumpla con:

  Capacidad y Protección: Capacidad mínima inicial de 100 TB escalable horizontalmente, con protección mediante RAID 6, Erasure Coding o esquemas de replicación distribuida.

  Compatibilidad Data Lake: Soporte nativo o mediante pasarela para protocolos de almacenamiento de objetos (compatibilidad tipo S3 API), permitiendo la integración directa con plataformas de Big Data, Spark y frameworks de Machine Learning.

  Gestión de Ciclo de Vida: Capacidad para definir políticas automáticas de jerarquización (tiering) que muevan los datos menos consultados a capas de almacenamiento de menor costo y rendimiento, optimizando la inversión.

  Inmutabilidad y Versionado: Funcionalidades de versionado de objetos y bloqueo de retención (Object Lock / WORM) para garantizar la inalterabilidad de la evidencia digital y la trazabilidad de los datasets utilizados en auditorías.

4. **Subsistema de Integración (ETL/ELT):**

- Se debe garantizar un entorno que permita la extracción, transformación y carga de datos de forma automática desde las fuentes primarias del SICOV transaccional.
- **Latencia máxima permitida:** La sincronización de datos entre el SICOV Operativo y el CPD-Analítico deberá garantizar los siguientes tiempos máximos de actualización (latencia):
  - **Inmediata**, para validaciones de identidad con reconocimiento facial en la fase de enrolamiento.
  - **Cinco (5) minutos** para otros datos transaccionales críticos (disponibilidad, validaciones biométricas durante la prestación del servicio, recaudo) por lotes de datos, y por operador SICOV, de acuerdo con los lineamientos que defina la Superintendencia.
  - **Una (1) hora** para la totalidad de la operación detallada (exámenes, evidencias, alertas, información del personal de la salud, etc.).
  - **Diaria** para datos históricos consolidados y reportes estadísticos agregados.

La latencia aquí definida aplica estrictamente a la ingesta y disponibilidad del dato primario. Los procesos de procesamiento analítico avanzado, consolidación histórica y generación de reportes de inteligencia de negocio podrán ejecutarse de manera asíncrona en los ciclos técnicos que defina la Superintendencia, asegurando siempre la integridad de la información.

5. **Aislamiento y gestión de cargas de trabajo:**

La infraestructura del CPD Analítico y de Identificación deberá garantizar el aislamiento lógico de los recursos de cómputo.

El operador homologado implementará mecanismos de segregación que aseguren que los procesos de analítica avanzada y entrenamiento de modelos no afecten el rendimiento ni la disponibilidad de las inferencias operativas del ABIS 1:N. Se deberá priorizar en todo momento la capacidad de respuesta de los servicios transaccionales frente a las tareas de procesamiento batch o analítica predictiva.

2.5.12.2. Funcionalidades del Módulo de Consulta, IVC e Inteligencia de Negocio

Sobre la infraestructura del CPD-Analítico, el operador homologado deberá habilitar un módulo de software web, de acceso seguro y restringido para la Superintendencia de Transporte, que provea las siguientes funcionalidades e información sin depender de solicitudes manuales al operador:

1. **Monitoreo del desempeño y disponibilidad del SICOV:** Incluyendo indicadores de disponibilidad del sistema medidos de manera permanente; información del estado en tiempo real de disponibilidad (up o down) de los diferentes componentes del Sistema; acceso en tiempo real a reportes detallados sobre incidentes técnicos que se presenten y/o hayan presentado anteriormente, que hayan afectado la operación del Sistema, y la duración de estas interrupciones o fallas y el número de centros afectados; así como un tablero de seguimiento del cumplimiento de los Acuerdos de Nivel de Servicio (ANS) definidos para la operación del SICOV, incluyendo el del servicio del operador de recaudo, y el del operador tecnológico de autenticación biométrica de la RNEC.

   Se permite que la información de disponibilidad y desempeño del sistema sea extraída de las herramientas de observabilidad y monitoreo (NOC/SOC) utilizadas por el operador homologado, bajo las siguientes condiciones:

   - Los datos extraídos deben permitir la construcción y visualización de la totalidad de los indicadores exigidos por la Entidad (disponibilidad por componente, latencia de respuesta, estado Up/Down en tiempo real, entre otros).
   - No se aceptará el cargue manual de reportes de disponibilidad. El flujo de datos entre las herramientas de observabilidad del operador y el Módulo de Consulta e IVC de la Superintendencia debe ser automático y mediante servicios web (API).
   - La Superintendencia se reserva el derecho de auditar las fuentes primarias de estas herramientas de monitoreo para asegurar que los datos reportados coincidan con la realidad operativa del sistema.

   Independientemente de la herramienta de origen, la información deberá visualizarse de manera consolidada en el tablero de control de la Superintendencia para facilitar las labores de inspección y vigilancia en tiempo real.

2. **Gestión de peticiones, quejas, reclamos, sugerencias y denuncias (PQRSD) relacionadas con el SICOV:** Visualización de estadísticas actualizadas sobre las PQRSD recibidas y gestionadas por el operador del SICOV a través de su Mesa de Ayuda, con corte al día del mes en el que se realiza la consulta. Esta información también se podrá consultar por mes y año, y el dato histórico general. El sistema, además, permitirá consultar la fecha de creación de las PQRSD activas, el estado de resolución de las PQRSD por mes, tiempos promedio de respuesta por cada una y clasificación por motivo.

3. **Consulta de datos operativos e históricos de los organismos de apoyo:** Capacidad para que la Superintendencia de Transporte consulte información específica e individualizada de cada CRC (perfil único con información) y agregada de todos los CRC del país, utilizando diversos criterios de búsqueda. El acceso a la información histórica estará limitado por la política de retención de datos que se define más adelante para el SICOV.

4. **Capacidades de análisis estadístico y tendencias:** El módulo deberá ofrecer herramientas de inteligencia de negocio para el análisis estadístico de la información operativa, permitiendo a la Superintendencia identificar tendencias, patrones, e indicadores de riesgo para planificar y focalizar sus actividades de IVC.

5. **Servicios marcados:** información de los servicios que fueron marcados automáticamente por el Sistema, con toda la información asociada al servicio (datos del usuario, instructores, vehículos, establecimiento del CRC, fecha, hora, motivo de generación de la alerta, entre otros) o sesión específica, ante la evidencia de presuntas anomalías en la prestación del servicio.

6. **Generación de constancia de disponibilidad del SICOV para fines probatorios**: El Sistema de Control y Vigilancia deberá contar con la capacidad para que la Superintendencia de Transporte genere y descargue una constancia con valor probatorio sobre la disponibilidad y funcionalidad del Sistema. Este documento deberá poder ser generado para una fecha y hora específicas, que correspondan con el momento en que se detectó y se aplicó la "marcación de irregularidad" a un servicio o grupo de servicios de capacitación/impartición de cursos. La constancia deberá incluir:

    - La fecha y hora exactas en que se realizó la marcación del servicio como irregular.
    - El porcentaje de disponibilidad de los componentes del SICOV en el momento preciso.
    - Un registro de los incidentes técnicos, fallas o alertas que se hayan presentado en el sistema en la ventana de tiempo de la marcación, en caso de que los haya habido.
    - Una declaración que certifique que la funcionalidad de detección y marcación de irregularidades operaba correctamente.

    Para garantizar su valor probatorio, esta constancia deberá cumplir los siguientes requisitos:

    a) Contenido: Deberá indicar explícitamente el porcentaje de disponibilidad de los componentes críticos (Web Services, Biometría, Base de Datos), el registro de incidentes reportados en ese lapso y la confirmación de si existían o no "Marcaciones de irregularidad" activas.

    b) Firma digital: El documento generado (formato PDF/A) deberá incorporar automáticamente la firma digital del Operador Homologado (su Representante), emitida por una Entidad de Certificación Digital, garantizando la autenticidad e integridad del documento conforme a la Ley 527 de 1999.

    c) Trazabilidad y retención: Una copia idéntica de cada constancia generada deberá almacenarse automáticamente en el repositorio seguro del CPD Analítico por un periodo mínimo de cinco (5) años, asociándola al expediente del organismo de apoyo consultado y al funcionario de la Superintendencia que la solicitó.

Esta funcionalidad permitirá a la Superintendencia de Transporte obtener evidencia digital irrefutable sobre el estado del sistema, fortaleciendo el sustento de las investigaciones administrativas que se inicien contra los CRC por irregularidades detectadas a través del SICOV.

7. **Generación automática de informes en caso de medidas administrativas de suspensión adoptadas.** El SICOV deberá permitir la generación automática de informes descargables con la información actualizada de las medidas administrativas preventivas y sancionatorias (suspensión) adoptadas por la Superintendencia, diferenciando aquellas que ya se encuentran en ejecución de las que no, con base en la información reportada por el RUNT a la Superintendencia de Transporte. Con esta información el Sistema permitirá la generación automática de informes para la Superintendencia de Transporte que deberán contener:

   - **CRC:** Especificación en número y datos de los organismos respecto de los cuales se ha ordenado una medida de suspensión, tanto de carácter preventivo, como por fallo sancionatorio, en el RUNT, con la indicación de si la misma fue ejecutada por el Concesionario RUNT, o no, con base en la información disponible para el efecto.
   - **Relación de PIN generados** e información de los usuarios del servicio a los que no se haya terminado de prestar el servicio.
   - **Razones de la no-culminación:** Consignar, si la hubiera, la información de las razones particulares por las cuales el servicio no fue completado, de acuerdo con la información registrada y con trazabilidad en el SICOV.

   El SICOV pondrá los informes requeridos a disposición de la Superintendencia a través del MOCVI, para su descarga y uso como elemento probatorio en el proceso sancionatorio correspondiente. Estos informes deberán ir con la firma digital del proveedor homologado.

   El SICOV deberá mostrar una notificación visible en la interfaz de administración del CRC con una alerta indicando que se encuentra incurso en un proceso administrativo sancionatorio de la Superintendencia de Transporte.

8. **Consulta y generación de informes sobre la operación de CRC a necesidad.**

   El Sistema deberá permitir la consulta y generación de informes sobre la operación de cualquier CRC, en periodos de tiempo determinables por la Superintendencia de Transporte.

   Para la generación de informes la Superintendencia podrá seleccionar la información de interés, entre la que se incluye: datos de registro en el RUNT y en el SICOV del CRC, estado actual de la vigencia de los requisitos críticos de operación, alertas generadas y servicios marcados por cualquiera de las causales descritas en el presente Anexo en la temporalidad deseada, número de servicios prestados en diferentes temporalidades, número de usuarios y/o servicios activos, identificación de los usuarios y del personal actualmente vinculado a los centros, fechas de enrolamiento y desvinculación de usuarios y personal, entre otros. En general, el Sistema permitirá la consulta de toda la información de operación capturada a través del SICOV descrita en este Anexo.

   El SICOV pondrá los informes requeridos a disposición de la Superintendencia a través del Módulo de consulta, IVC e inteligencia de negocio, para su descarga y uso como elemento probatorio en el proceso

sancionatorio correspondiente. Estos informes deberán ir con la firma digital del proveedor homologado.

9. **Consulta de información sobre visitas realizadas a CRC.** El Sistema deberá permitir consultar el registro con la información de las visitas realizadas por parte de los operadores homologados a CRC en el curso del año, con la información de la fecha de visita, informe y evidencias de la misma**.**

10. **Visualización y descarga de información crítica de operación de CRC.** El Sistema deberá permitir la consulta, visualización y descarga de documentos digitalizados que soportan el cumplimiento de los requisitos críticos de existencia y operación de los CRC.

11. **Trazabilidad y auditoría de la interoperabilidad:** Visualización gráfica de la información contenida en los registros (logs) detallados de todas las transacciones, consultas y operaciones de interoperabilidad de datos realizadas entre los distintos proveedores homologados del SICOV, permitiendo la verificación de la correcta ejecución de los mecanismos de intercambio de información y la identificación de posibles fallos o interrupciones en el flujo de datos entre operadores.

    El Comité Técnico Operativo de la Superintendencia definirá la estructura de metadatos para los registros de interoperabilidad y el formato estándar en que estos deben generarse para la consulta y verificación de la Superintendencia. La política de retención de estos logs será de cinco (5) años, garantizando la inmutabilidad de los registros históricos.

12. **Trazabilidad y registro de la fuente de evidencia:** Los reportes de incumplimiento y la trazabilidad histórica generados por el sistema deberán incluir, de manera inalterable, la identificación específica de la cámara o del dispositivo del SICOV (ej. cámara fija, lector de huella, tablet, etc.) que permitió advertir la irregularidad o que generó la evidencia. Esta información garantizará la pertinencia y conducencia de la evidencia digital en los informes que sustenten las actuaciones de Inspección, Vigilancia y Control de la Superintendencia de Transporte.

La información histórica al nivel de detalle especificado y descrito en este acápite estará disponible para todos los servicios prestados en los cinco (5) años anteriores al año en que se realiza consulta. La información de los servicios prestados con anterioridad a los cinco años, solo se podrá visualizar en datos agrupados, por año.

2.5.12.3. Requisitos de capacidad de análisis:

Nivel de acceso y autoservicio (BI): El operador homologado deberá garantizar la funcionalidad de inteligencia de negocio de autoservicio, permitiendo a la Superintendencia generar consultas analíticas dinámicas y libres con los datos de la operación aquí referidos, además de acceder a los tableros de control y reportes adicionales que sean definidos.

Para garantizar la integridad y consistencia de los análisis, el Sistema deberá implementar una Capa Semántica y un Catálogo de Datos. El ejercicio de autoservicio deberá realizarse preferiblemente sobre Datasets Certificados por el operador homologado, con criterios validados por la Superintendencia, asegurando la uniformidad en los indicadores de gestión y la protección de la información sensible.

Validación y gobernanza de modelos: El Comité Técnico Operativo para el Fortalecimiento del SICOV será la instancia encargada de establecer y validar la metodología e hipótesis de los modelos de detección de fraude y de análisis de tendencias.

Frecuencia de actualización de datos: La información dispuesta en el módulo de BI para la consulta de la Superintendencia deberá tener una frecuencia de actualización con una latencia máxima de:

- Cinco (5) minutos para los datos transaccionales que permiten establecer los niveles de disponibilidad del sistema (mecanismos de validación biométrica, recaudo, disponibilidad del software de gestión)
- Una (1) hora para conocer la operación de los CRC como información, evidencias y alertas, al igual que para aquella información necesaria
- Actualización diaria para los datos operativos históricos y reportes estadísticos agregados, cumpliendo los ANS que la Superintendencia determine.

2.5.12.4. Subsistema ABIS y capacidades de Inteligencia Artificial

El CPD – Analítico y de Identificación alojará y procesará los modelos avanzados requeridos para la seguridad del sistema, incluyendo:

1. **Subsistema ABIS:** Conforme a lo descrito en el capítulod de requisitos técnicos y tecnológicos, actuará como el repositorio centralizado oficial para el proceso de validación de reconocimiento facial. Deberá soportar la identificación 1:N (uno a muchos) y 1:1 (uno a uno) con algoritmos de alta precisión para evitar la suplantación de identidad.

2. **Modelos de detección de fraude:** Ejecución de algoritmos de Machine Learning orientados a la detección de patrones anómalos (ej. instructores dictando clase en dos sitios, telemetría simulada, patrones de huellas atípicos).

3. **Propiedad Intelectual:** Todo modelo de datos, tablero de control, algoritmo de detección de fraude o reporte desarrollado específicamente para la función de IVC en este componente será propiedad exclusiva de la Superintendencia de Transporte en cuanto a su uso y explotación para fines públicos.

2.5.12.5. Seguridad, licenciamiento y soporte del CPD-Analítico y de Identificación.

- **Seguridad:** Implementación de controles de acceso lógico basados en roles (RBAC), autenticación multifactor (MFA) para funcionarios de la Superintendencia, y cifrado de datos en reposo (AES-256) y en tránsito (TLS 1.2 o superior).
- **Software Base:** Todas las soluciones de analítica, bases de datos y virtualización deberán contar con soporte de fabricante vigente y estar posicionadas en reportes de industria reconocidos (como Gartner Magic Quadrant o Forrester Wave).
- **Personal Dedicado:** El operador deberá garantizar la disponibilidad de un equipo técnico especializado para la administración de este componente (analistas de datos, DBAs, oficiales de seguridad), cuyos costos serán asumidos por el operador como parte de su obligación de homologación.

2.5.12.6. Ciclo de vida y retención de datos

Política de ciclo de vida y retención de datos: El operador deberá implementar una política diferenciada de retención de información en el CPD Analítico.

Categoría A (misión crítica): Biometría y evidencias de trámites. Retención: 10 años.

Categoría B (operativa): Logs de eventos y auditoría. Retención: 5 años.

Categoría C (analítica): Datasets de entrenamiento y resultados de BI será definida por ciclo de utilidad técnica. Retención: 10 años.

Cualquier proceso de depuración o eliminación de datos de Categoría B o C deberá ser documentado y estar sujeto a los protocolos de seguridad que se definan en las mesas técnicas de estandarización convocadas por la Superintendencia.

2.5.12.7. Seguridad y control de acceso del Módulo de IVC

El Módulo de Consulta e Inteligencia de Negocio deberá implementar un esquema de seguridad robusto que garantice que la información estratégica de la Superintendencia no sea accesible por terceros no autorizados, ni siquiera por el personal técnico del operador (salvo tareas de mantenimiento auditadas). Se deberán cumplir los siguientes requisitos mínimos:

a) Autenticación Multifactor (MFA): El acceso para los funcionarios de la Superintendencia de Transporte deberá exigir obligatoriamente un segundo factor de autenticación (OTP, Token blando, biometría o certificado digital), además de las credenciales de usuario.

b) Control de Acceso Basado en Roles (RBAC): El sistema deberá permitir la creación de perfiles granulares (ej. Auditor, Investigador, Director), asegurando que cada usuario solo acceda a la información estrictamente necesaria para su función ("Need-to-know").

c) Bitácora de accesos (Logs de auditoría): El sistema deberá registrar de manera inalterable cada acceso exitoso o fallido al módulo, indicando usuario, fecha, hora, dirección IP y la consulta o reporte específico visualizado. Estos logs deberán estar disponibles para auditoría por parte de la Entidad.

El acceso a los componentes críticos del CPD Analítico y de Identificación y al Módulo de IVC estará restringido por defecto. Se permitirá el acceso técnico al personal del operador exclusivamente para labores de soporte, mantenimiento y solución de incidentes, siempre que se realice bajo protocolos aquí establecidos.

2.5.12.8. Gobernanza de algoritmos y gestión de falsos positivos.

Con el fin de garantizar la fiabilidad de las alertas automáticas y las marcaciones de irregularidad generadas por los modelos de analítica e inteligencia artificial del SICOV, el operador homologado deberá implementar el siguiente protocolo:

a) **Calibración y entrenamiento:** Los algoritmos de detección de fraude deberán someterse a un periodo de aprendizaje y calibración, con el fin de minimizar la tasa de falsos positivos. Los umbrales de precisión serán aprobados por el Comité Técnico Operativo.

b) **Procedimiento de revisión técnica:** Se deberá habilitar un canal específico en la Mesa de Ayuda para que los Organismos de Apoyo puedan reportar "Marcaciones por Error Técnico". El operador dispondrá de un equipo especializado para analizar estos casos.

- Si se determina que la marcación obedeció a una falla del sistema, un error de lectura del sensor o una inconsistencia de la plataforma, la marcación será reversada y el incidente se registrará como insumo para el reentrenamiento del modelo.
- Si el análisis técnico confirma que la alerta se generó correctamente por un incumplimiento de los parámetros normativos o técnicos, la marcación se mantendrá en firme y el caso quedará disponible para las acciones de IVC de la Superintendencia.

2.5.12.9. Gobierno de modelos analíticos

El CPD Analítico deberá contar con una metodología de operación de aprendizaje automático (MLOps) que garantice la trazabilidad de todo el ciclo de vida de los modelos predictivos y de detección de fraude.

Todo modelo analítico utilizado para el ejercicio de la vigilancia deberá contar con un expediente técnico de validación que incluya métricas de desempeño, descripción de las variables utilizadas, registro de versiones y protocolos de monitoreo. La Superintendencia de Transporte supervisará la aplicación de este gobierno para asegurar la transparencia y legalidad de las decisiones automatizadas.

2.6. Comité Técnico Operativo para el Fortalecimiento del SICOV

2.6.9. Estandarización y fortalecimiento del Sistema de Control y Vigilancia

La Superintendencia de Transporte, creará un Comité Técnico-Operativo para el fortalecimiento del SICOV, con el fin de estandarizar los procesos de reporte de información para robustecer el análisis, a validación y mejoras tecnológicas y operativas que permitan la definición de nuevos controles que fortalezcan la función de vigilancia y control para la toma de decisiones en tiempo real.

El Comité Técnico-Operativo del SICOV deberá verificar el cumplimiento de los distintos requerimientos técnicos establecidos en la Resolución 60832 de 2016 y sus actos administrativos modificatorios, así mismo, deberá establecer los controles que fortalezcan la función de vigilancia y control de acuerdo con la normatividad que regula los procesos y procedimientos a cargo de a Agencia Nacional de Seguridad Vial y el Ministerio de Transporte, en especial el cumplimiento de las disposiciones relacionadas con las mallas curriculares emitidas para la prestación del servicio de enseñanza.

TÍTULO 3

3. AUDITORÍA A LA INFRAESTRUCTURA TECNOLÓGICA PROVISTA POR LOS OPERADORES HOMOLGADOS DEL SICOV

3.1. Objetivo de las auditorías

Las auditorías a la infraestructura tecnológica de soporte del Sistema de Control y Vigilancia serán realizadas por terceros y tienen como objetivo primordial verificar de manera independiente la idoneidad técnica de los recursos y componentes tecnológicos empleados en los OAAT para la prestación de sus servicios, de conformidad con los estándares de integridad y trazabilidad requeridos para garantizar la autenticidad de los certificados expedidos por los CRC.

Las directrices, periodicidad, alcance y metodología de las auditorías serán definidas por la Superintendencia de Transporte a través del Comité Técnico Operativo para el Fortalecimiento del SICOV.

3.2. Ámbito y periodicidad de las auditorías

La infraestructura tecnológica del SICOV provista por los operadores homologados, así como las instalaciones y procesos relacionados con su operación (serán objeto de auditorías periódicas, con una frecuencia mínima de una auditoría cada dos (2) años, según lo determine la Superintendencia de Transporte a través del Comité Técnico Operativo para el Fortalecimiento del SICOV, sin perjuicio de las auditorías extraordinarias que la entidad pueda ordenar cuando lo considere necesario.

3.3. Independencia del auditor

Las auditorías deberán ser realizadas por auditores con idoneidad técnica e independencia elegidos por la Superintendencia de Transporte conforme a los criterios que para tal efecto se definan.

3.4. Costos de las auditorías

Los costos asociados a la realización de las auditorías de verificación del SICOV serán asumidos con recursos de su operación, los cuales son pagados por los usuarios de los servicios de los Centros de Reconocimiento de Conductores, siempre garantizando la independencia y objetividad de su ejecución.

3.5. Obligaciones del proveedor homologado frente a las auditorías

El proveedor homologado del SICOV tendrá las siguientes obligaciones relacionadas con las auditorías:

1. Brindar todas las facilidades y acceso a la información, sistemas, instalaciones y personal requerido por el auditor para el desarrollo de su labor.
2. Responder de manera oportuna a todos los requerimientos de información, documentación y aclaraciones que el auditor formule.
3. Presentar y ejecutar un plan de mejora detallado para la subsanación de los hallazgos y no conformidades identificadas en el informe de auditoría, en los plazos que establezca la Superintendencia de Transporte. La Superintendencia realizará seguimiento al cumplimiento de dicho plan.
4. Suministrar a la Superintendencia de Transporte los informes de auditoría en los plazos y formatos que esta determine.

TÍTULO 4

4. ACUERDOS DE NIVELES DE SERVICIO, TRATAMIENTO DE DATOS Y OBLIGACIONES DE LAS PARTES

4.1. ACUERDOS DE NIVELES DE SERVICIO

Los proveedores homologados del SICOV deberán cumplir con los Acuerdos de Niveles de Servicio de los componentes del SICOV, que a continuación se indican.

Los indicadores previstos para el seguimiento y monitoreo de calidad, desempeño del servicio y en general las herramientas necesarias para determinar el cumplimiento de los ANS que a continuación se establecen, deberán ser visibles para la Superintendencia de Transporte a través del del Módulo de consulta, IVC e inteligencia de negocio para la Superintendencia.

4.1.1. CPD/CAPD y NOC – SOC

El CPD y CAPD deben garantizar una disponibilidad de, como mínimo 99,9 %.

4.1.2. Mesa de Ayuda

El proveedor homologado del SICOV deberá cumplir con los tiempos máximos de respuesta a los incidentes, solicitudes, quejas y reclamos que presenten los organismos de apoyo al tránsito a los que preste el servicio; la Superintendencia de Transporte y/o las entidades administrativas y judiciales que lo soliciten, los cuales se establecen en la siguiente tabla.

Adicionalmente, deberán calcular permanentemente el indicador establecido para el seguimiento y monitoreo de calidad y desempeño del servicio. Dichos indicadores deberán ser visibles para la Superintendencia de Transporte a través del Módulo de consulta, IVC e inteligencia de negocio para la Superintendencia.

La Mesa de Ayuda debe cumplir con los siguientes Acuerdos de Niveles de servicio:

PETICIONARIO	TIEMPO EN DÍAS HÁBILES	INDICADOR DEL SERVICIO	PORCENTAJE DE CUMPLIMIENTO MÍNIMO
Clientes del servicio (OAAT) (derechos de petición)	15 días	No. de días en los cuáles se da respuesta	95 %
Superintendencia de Transporte y operador SICOV	5 días	No. días en los cuáles se da respuesta desde el momento de Ia radicación/5	98 %
Autoridades administrativas y judiciales	10 días	No. días en los cuáles se da respuesta desde el momento de Ia radicación/10	95 %

Niveles de atención de incidentes

Categoría	Nombre	Descripción	Objetivo	Rango de cumplimiento	Formula de calculo
Disponibilidad	Disponibilidad de la Mesa de Servicios	Tiempo ininterrumpido de operación de la mesa de servicios entendiendo los que canales de comunicación y la plataforma de atención son los elementos incluidos dentro del ANS	99% del tiempo acordado – 7x24	= 99%: cumplimiento satisfactorio. < 99% y >= 96,5%: Incumplimiento Moderado. (Sujeto a Plan de Mejora Inmediato). < 96,5%: Incumplimiento Crítico. (Sujeto a inicio de actuación administrativa sancionatoria y/o conminación de cumplimiento según Art. 20).	DMS = Disponibilidad de la Mesa de Servicio TTD = Total tiempo de disponibilidad (total de horas del mes) TCMS = Tiempo de caída de la Mesa de Servicio. Fórmula: DMS = (TTD – TCMS)/ TTD * 100

Disponibilidad	Disponibilidad de canales	Tiempo promedio de disponibilidad de canales		99,9%	Horas totales – horas paradas) / Horas totales) * 100
Soporte Técnico – Mesa de Servicios	Tiempo medio de espera	Tiempo promedio que un usuario debe esperar hasta ser atendido por un analista de la mesa	Menor a 120 segundos	<= 120 segundos: Cumplimiento satisfactorio. 120 seg y <= 150 seg: Incumplimiento Moderado. 150 seg: Incumplimiento Crítico.	TME = Tiempo Medio de espera para la Mesa de Servicio
Soporte Técnico – Mesa de Servicios	Tasa de abandono	Cantidad de llamadas abandonadas por no atención o por demora en la misma	Menor a 5% del total de llamadas	<= 5% >5% y <= 6% Incumplimiento moderado 6%: Incumplimiento crítico.	
Soporte Técnico – Mesa de Servicios	Registro de casos	Cantidad de casos registrados respecto de las llamadas recibidas	99,9%		
Soporte Técnico – Mesa de Servicios	Tiempo de resolución	Tiempo máximo para resolver un caso de soporte registrado en la mesa de servicios según su criticidad.	Crítico: 4 horas Alto: 8 horas Medio: 16 horas Bajo: 32 horas Casos escalados a terceros: Mejor esfuerzo		

4.1.3. Operador de recaudo

El operador de recaudo deberá cumplir con los siguientes Acuerdos de Niveles de servicio.

PETICIONARIO	TIEMPO EN DÍAS HÁBILES	INDICADOR DEL SERVICIO	PORCENTAJE DE CUMPLIMIENTO MÍNIMO
Clientes del servicio de recaudo	24 horas	No. horas en los cuáles se da respuesta desde el momento de la radicación/24	95 %
Superintendencia de Transporte y operador SICOV	5 días	No. días en los cuáles se da respuesta desde el momento de la radicación/5	95 %
Autoridades administrativas y judiciales	7 días	No. días en los cuáles se da respuesta desde el momento de la radicación/5	95 %

El incumplimiento de los rangos mínimos de servicio (moderado o crítico) se considerará una falla en la operación verificable por parte de la Superintendencia de Transporte.

4.2. POLÍTICA GENERAL DE TRATAMIENTO, CONSERVACIÓN Y SUPRESIÓN DE LA INFORMACIÓN DEL SICOV.

Los datos personales y la información de la operación de los organismos de apoyo a las autoridades de tránsito y del SICOV son recopilados con el fin de garantizar la trazabilidad y validez de los certificados expedidos por los CRC. Así mismo, dicha información permite a la Superintendencia el cumplimiento de sus funciones de supervisión sobre el servicio público a cargo de esos organismos de apoyo al tránsito.

Los proveedores de la infraestructura tecnológica del SICOV para CRC actúan en calidad de Encargados del Tratamiento y custodios temporales de dicha información. En consecuencia, dado que la información operativa soporta una actividad vinculada a un servicio público de tránsito, los proveedores no podrán invocar derechos de propiedad o exclusividad.

El presente numeral establece la política para el archivo, la conservación y la supresión segura de la información y los documentos gestionados por el Sistema de Control y Vigilancia. Esta política se fundamenta en los principios de finalidad, necesidad y temporalidad establecidos en la Ley Estatutaria 1581 de 2012, en las directrices de la Ley General de Archivos (Ley 594 de 2000), y en la consideración de los términos de prescripción de las acciones administrativas, sancionatorias, civiles y penales aplicables.

El operador del SICOV será el responsable de implementar y garantizar el cumplimiento de esta política a través de los mecanismos técnicos y procedimientos necesarios, bajo la supervisión de la Superintendencia de Transporte y previa aprobación por parte del usuario de los Términos y Condiciones del servicio, así como del Acuerdo de Tratamiento de Datos Personales.

4.2.1. Categorías de información y plazos de conservación:

a) Registros del proceso de evaluación y certificación: Comprende el conjunto de datos que constituyen el expediente electrónico de cada servicio prestado a un usuario, incluyendo el resultado de los exámenes, los resultados

de todas las validaciones de identidad (exitosas y fallidas), y el certificado de aptitud física, mental y de coordinación motriz expedido.

Plazo de conservación: Esta información deberá conservarse en el SICOV por un término mínimo y máximo de **diez (10) años**, contados a partir de la fecha de expedición del certificado correspondiente. Este plazo busca garantizar la disponibilidad de la información como material probatorio para eventuales investigaciones o procesos judiciales y administrativos.

b) Documentación de habilitación y operación de los organismos de apoyo: Comprende los documentos cargados por el CRC para acreditar el cumplimiento de sus requisitos de registro y operación, tales como acreditación, informes de auditoría del ONAC, pólizas de responsabilidad civil, licencias de funcionamiento y registro en el REPS, entre otros.

Plazo de conservación: Esta documentación deberá conservarse de forma accesible en el SICOV durante todo el tiempo en que el organismo de apoyo se encuentre activo en el Sistema y, posteriormente a su desvinculación formal o cese de operaciones, deberá archivarse por un término adicional de **cinco (5) años** para fines de auditoría histórica y la determinación de responsabilidades.

c) Datos biométricos primarios (patrones o templates): Se refiere específicamente a las plantillas o patrones biométricos (faciales) de los usuarios y del personal, que son utilizados por el SICOV para realizar las comparaciones en los procesos de validación de identidad.

Plazo de conservación y supresión: Los datos biométricos conservados en el ABIS para efectos de la prestación del servicio, por su naturaleza altamente sensible, solo se conservarán mientras el individuo (usuario o personal) se encuentre activo en el SICOV. Una vez que el usuario culmine satisfactoriamente su proceso de capacitación o curso y se expida el certificado, o una vez que el miembro del personal sea formalmente desvinculado del organismo de apoyo en el Sistema, sus plantillas biométricas serán sometidas a un proceso de **supresión segura y definitiva** de las bases de datos activas del SICOV. Dicha supresión se deberá ejecutar en un plazo de **diez (10) años** contados a partir de la finalización del proceso o de la desvinculación, con el fin de atender posibles reclamaciones post-servicio o procesos de cierre administrativo. Los operadores homologados deberán certificar semestralmente ante la Superintendencia que han ejecutado los procesos de purga y eliminación de datos que han cumplido su ciclo de vida, a partir del momento en que transcurran los primeros diez (10) años.

d) Registros y bitácoras de auditoría del sistema SICOV: Incluye todos los registros técnicos (logs) generados por el SICOV sobre eventos del sistema, acciones de los usuarios, accesos, consultas, errores, aplicación de restricciones, y cualquier otra actividad relevante para la seguridad y la trazabilidad de la plataforma.

Plazo de conservación: Esta información deberá conservarse por un término mínimo de **cinco (5) años**, con el fin de permitir la investigación de incidentes de seguridad, el análisis y la auditoría técnica del sistema.

4.2.2. Obligaciones del operador del SICOV respecto a la política de conservación:

a) Implementar los mecanismos técnicos necesarios para aplicar de forma automática y segura los plazos de conservación y los procedimientos de supresión definidos en este numeral.

b) Garantizar que los procedimientos de supresión de datos, especialmente los biométricos sensibles, sean seguros, permanentes e irreversibles, y dejar una constancia auditable de su ejecución.

c) Asegurar la disponibilidad, integridad y confidencialidad de toda la información durante su respectivo periodo de conservación.

d) Desarrollar, implementar y mantener actualizadas, bajo la dirección y aprobación de la Superintendencia de Transporte y siguiendo los lineamientos técnicos del Archivo General de la Nación, las Tablas de Retención Documental (TRD) específicas para los expedientes y series documentales electrónicas gestionadas por el SICOV.

e) Garantizar que el CPD Analítico implemente capas de segregación de datos. Mientras que la evidencia primaria se conservará con su PII íntegra para fines probatorios, los procesos de analítica e inteligencia de negocios deberán ejecutarse preferiblemente sobre datos seudonimizados o anonimizados, cuando la identidad no resulte ser un dato indispensable –como en aquellos casos en que existan alertas frente a determinados usuarios del Sistema– aplicando los estándares de seguridad definidos por la Superintendencia de Transporte para mitigar riesgos de exposición innecesaria de información personal.

4.3. OBLIGACIONES DE LOS OPERADORES HOMOLOGADOS DEL SICOV.

Son obligaciones indelegables del proveedor u operador autorizado por la Superintendencia de Transporte para desarrollar, implementar, operar y mantener el Sistema de Control y Vigilancia para Centros de Reconocimiento de Conductores, las siguientes:

1. **Mantenimiento de la homologación y cumplimiento normativo continuo:** Cumplir permanentemente con todos los requisitos técnicos, jurídicos, administrativos, financieros y de calidad que dieron lugar a su homologación y autorización, así como con todas las disposiciones del presente Anexo Técnico y cualquier modificación o adición posterior que expida la Superintendencia de Transporte.

2. **Protección de datos y seguridad de la información:** Implementar, operar, mantener y mejorar continuamente un Sistema de Gestión de Seguridad de la Información (SGSI) ISO 27001, que garantice la confidencialidad, integridad, disponibilidad, autenticidad y no repudio de toda la información y datos personales (incluidos los biométricos y otros datos sensibles) gestionados por el SICOV. Asegurar el cumplimiento estricto de la Ley Estatutaria 1581 de 2012, sus decretos reglamentarios, las directrices de la Superintendencia de Industria y Comercio, y las políticas de la Superintendencia de Transporte sobre tratamiento de datos sensibles.

3. **Gestión del ciclo de vida de la información y cumplimiento de la política de conservación de datos:** Implementar, operar y garantizar el estricto cumplimiento de la Política general de tratamiento, conservación y supresión de la información del SICOV, conforme a lo previsto en el presente Anexo Técnico. Esta obligación incluye la aplicación de los plazos de retención para cada categoría de información, la ejecución de los procedimientos de supresión segura y definitiva de los datos una vez cumplido su término de conservación, y el desarrollo y mantenimiento de las Tablas de Retención Documental (TRD) del Sistema, bajo la supervisión y aprobación de la Superintendencia de Transporte.

4. **Innovación, vigilancia tecnológica y propuestas de mejora continua:** Realizar una vigilancia tecnológica constante sobre avances aplicables a los sistemas de control, inspección, vigilancia y control y seguridad vial, y proponer proactivamente a la Superintendencia de Transporte, con la periodicidad que esta defina, mejoras funcionales, tecnológicas o de seguridad para el SICOV, orientadas a optimizar su

efectividad, eficiencia, evitar la obsolescencia tecnológica y adaptarse a nuevas amenazas o requerimientos regulatorios.

5. **Plan de salida y reversión tecnológica:** El proveedor deberá diseñar, mantener actualizado y presentar para aprobación de la Superintendencia un Protocolo de Salida y Reversión, el cual se activará en caso de renuncia, pérdida o cancelación de la homologación. Este protocolo deberá garantizar:

   a) Entrega de información: La exportación y entrega segura de la totalidad de la base de datos (estructurada y no estructurada), logs de auditoría, repositorios documentales y evidencias biométricas, en formatos estándar abiertos (SQL, JSON, CSV, PDF) que permitan su migración, conforme a los lineamientos que defina la Entidad.

   b) Destrucción segura: Una vez certificada la recepción de la información por parte de la Superintendencia o el nuevo operador, el proveedor saliente deberá proceder con el borrado seguro y certificado de los datos sensibles de sus repositorios, para garantizar el Habeas Data.

   c) Continuidad transitoria: El mantenimiento de la operación crítica durante el periodo de empalme que determine la Superintendencia, para evitar la interrupción del servicio público a los usuarios.

Provisión, desarrollo, operación y mantenimiento técnico del SICOV

6. **Infraestructura tecnológica y de software base:** Proveer, configurar, administrar y mantener actualizada toda la infraestructura de hardware, software base, sistemas de gestión de bases de datos, redes de comunicaciones y demás componentes tecnológicos necesarios para garantizar la plena implementación, el correcto funcionamiento, la seguridad y la evolución de todas las funcionalidades del SICOV descritas en el presente Anexo Técnico. Esto incluye la gestión proactiva de la capacidad y el rendimiento del sistema para asegurar su escalabilidad y óptimo desempeño, así como la garantía de niveles de servicio establecidos.

7. **Desarrollo y mantenimiento de funcionalidades del SICOV:** Desarrollar, implementar, probar exhaustivamente y mantener actualizadas todas las funcionalidades del software de gestión y control del SICOV, incluyendo el Módulo de consulta, IVC e inteligencia de negocio para la Superintendencia y todas las demás especificadas en el presente Anexo Técnico, asegurando su correcta operación.

8. **Integraciones e interoperabilidad:**

   a) Desarrollar, implementar y mantener seguras y eficientes todas las integraciones e interfaces necesarias del SICOV con el Registro Único Nacional de Tránsito (RUNT), con con otros operadores SICOV autorizados de CRC y con cualquier otro sistema externo que la Superintendencia de Transporte determine como necesario para la operación integral del SICOV.

   b) Implementar los mecanismos de integración e interoperabilidad para el intercambio seguro de información relevante sobre capacidad instalada y asignación de recursos con otros operadores SICOV autorizados, trazabilidad, resultados de los exámenes y avances en los procesos de evaluación de los usuarios, entre otros que se lleguen a determinar, conforme lo defina la Superintendencia de Transporte, con el fin de garantizar la consistencia de dicha información a nivel del sistema y evitar el fraude.

   c) Mantener un registro (logs) detallado e inalterable de todas las transacciones, consultas y operaciones de interoperabilidad realizadas con

otros operadores homologados del SICOV, que incluya, como mínimo, el origen y destino de la información, la fecha y hora exactas de la operación, el tipo de dato intercambiado, el resultado de la transacción y cualquier incidencia o error detectado. Estos logs deberán ser accesibles y reportados en tiempo real a la Superintendencia de Transporte a través del Módulo de consulta, IVC e inteligencia de negocio para la Superintendencia, conforme a los estándares técnicos que esta defina.
d) Transmitir la información del SICOV a la Superintendencia de Transporte de manera uniforme y estandarizada, adhiriéndose estrictamente a los formatos, estructuras y protocolos de datos que para tal fin defina el Comité Técnico Operativo para el Fortalecimiento del SICOV.

9. **Continuidad del negocio y recuperación ante desastres (BCP/DRP):** Diseñar, documentar, implementar, probar periódicamente (al menos dos veces al año) y mantener actualizados Planes de Continuidad de Negocio (BCP) y Recuperación ante Desastres (DRP) que aseguren la operación ininterrumpida de los componentes críticos del SICOV y la recuperación oportuna del servicio y la información ante cualquier contingencia, cumpliendo estrictamente con los objetivos de tiempo de recuperación (RTO) y puntos de recuperación (RPO) que se definen en este Anexo Técnico.

10. **Gestión formal y documentada de cambios en el sistema:** Establecer y aplicar un procedimiento formal y documentado para la gestión de todos los cambios (actualizaciones de software, modificaciones de infraestructura, nuevas funcionalidades) en el SICOV, que incluya análisis de impacto, pruebas rigurosas, documentación, bitácoras de auditoría y comunicación coordinada permanente con la Superintendencia.

Gestión de información, reportes y soporte a la IVC de la Superintendencia

11. **Provisión de acceso y herramientas de consulta para la Superintendencia:** garantizar a la superintendencia de transporte el acceso seguro, continuo y en tiempo real al Módulo de consulta, IVC e inteligencia de negocio del SICOV, proveyendo todas las funcionalidades de visualización, reporte, análisis estadístico y consulta de datos históricos y operativos de los organismos de apoyo y del propio SICOV, conforme a lo detallado en el presente Anexo Técnico y a los requerimientos de información que establezca la Superintendencia de Transporte.

12. **Procesamiento de datos, generación de alertas y aseguramiento de calidad de la información:** procesar la información operativa recabada a través del SICOV, aplicando herramientas de analítica de datos e inteligencia artificial para identificar patrones, tendencias y generar las alertas automáticas sobre posibles incumplimientos, conductas anómalas o riesgos de fraude, según los criterios definidos por la Superintendencia. Implementar mecanismos robustos para asegurar la calidad, integridad, consistencia, trazabilidad y no repudio de la información gestionada por el SICOV.

13. **Reporte de alertas y novedades del sistema a la Superintendencia:** Documentar y remitir de forma oportuna, detallada y automática al Módulo de consulta, IVC e inteligencia de negocio, toda la información, evidencias y alertas generadas por el sistema conforme a las reglas predefinidas en el presente Anexo Técnico. Esto incluye, entre otros, eventos como el vencimiento de documentos, excesos de capacidad, o anomalías técnicas reportadas. En estos reportes se deberá indicar la cámara o dispositivo del SICOV que permitió detectar la irregularidad. La información se entregará como un registro objetivo de los hechos para que la Superintendencia califique si dichos eventos constituyen presuntas faltas o incumplimientos a la normatividad vigente.

14. **Notificación automática de alertas y marcaciones:** Garantizar que, ante cualquier alerta o marcación de irregularidad generada por el sistema, el CRC sea informado de forma automática e inmediata, a través de los canales establecidos, sobre la naturaleza del incumplimiento y el hecho de que el servicio afectado ha sido marcado en el SICOV, de conformidad con lo establecido en el presente Anexo Técnico.

15. **Soporte a la verificación documental y de capacidad:** Apoyar a la Superintendencia en la verificación técnica preliminar y gestión documental para el levantamiento de restricciones impuestas a los organismos de apoyo por incumplimientos documentales, así como en las inspecciones que esta ordene para la redefinición de la capacidad instalada, cuyo costo deberá ser asumido por cada CRC.

16. **Visitas técnicas de mantenimiento y reporte de anomalías:** Realizar, con la periodicidad que defina el contrato con el organismo de apoyo o cuando las circunstancias lo requieran, visitas técnicas de instalación, mantenimiento y soporte a las sedes de los CRC. El objetivo de estas visitas será verificar el correcto estado y funcionamiento de los componentes de hardware y software que integran el SICOV.
    Si durante estas visitas técnicas, el personal del proveedor evidencia de manera objetiva una presunta manipulación física, daño intencional, desinstalación no autorizada u obstrucción de los dispositivos del SICOV, o algún incumplimiento de la normatividad vigente aplicable a la prestación del servicio, deberá documentar el hecho (mediante fotografías, descripción técnica, etc.) y reportarlo de inmediato a la Superintendencia de Transporte como un reporte de novedad. Este reporte no constituirá una calificación de la conducta del vigilado, sino un insumo técnico para la Superintendencia.
17. **Facilitación y soporte técnico durante las inspecciones y auditorías de la Superintendencia:** Brindar soporte técnico y facilitar el acceso irrestricto y oportuno a la información del SICOV (plataforma, bases de datos, bitácoras, reportes, etc.) a la Superintendencia de Transporte o a los auditores externos que esta designe, cuando la autoridad realice sus propias auditorías o visitas de inspección, vigilancia y control a los organismos de apoyo.

18. **Colaboración con autoridades:** Atender de manera oportuna y completa los requerimientos de información, soporte o colaboración presentados por la Superintendencia de Transporte, los órganos de control e investigación competentes y las autoridades judiciales. Denunciar o alertar a dichas autoridades y a la Superintendencia sobre cualquier conducta detectada que pueda constituir una falta grave o un presunto delito.

19. **Reporte y soporte técnico en incidentes:** Documentar y reportar diligentemente a la Superintendencia de Transporte cualquier falla técnica generalizada o recurrente del sistema SICOV o de sus componentes que afecte la prestación de servicios en los CRC. Proveer a la Superintendencia la información técnica y los registros del sistema que esta requiera para el análisis de casos específicos de incidentes reportados.

20. **Aseguramiento de la conectividad y control de acceso por red:** Implementar y mantener activos los controles de seguridad perimetral necesarios para validar que toda conexión entrante al SICOV provenga exclusivamente de las Direcciones IP públicas fijas registradas y autorizadas para cada sede de los organismos de apoyo. El operador deberá rechazar automáticamente cualquier intento de conexión que no curse a través del túnel cifrado (VPN) establecido o que provenga de direcciones IP no certificadas, reportando estos eventos como alertas de seguridad a la Superintendencia de Transporte.

Servicio y soporte a los organismos de apoyo

21. **Calidad del servicio, soporte técnico y capacitación a organismos de apoyo:** Garantizar la prestación del servicio SICOV a los CRC con altos estándares de calidad y disponibilidad (mínima del 99.4%, medida mensualmente). Esto incluye proveer un servicio de Mesa de Ayuda eficiente, con cobertura nacional y tiempos de respuesta definidos en los Acuerdos de Nivel de Servicio. Suministrar documentación técnica y de usuario clara y actualizada sobre el SICOV, y ofrecer programas de capacitación continua para el personal de los organismos de apoyo, tanto para nuevas funcionalidades como para el uso correcto y seguro del sistema.

22. **Gestión del registro de IDClient:** Gestionar activamente el proceso de registro en el SICOV del IDClient asignado por la RNEC a cada organismo de apoyo, incluyendo la implementación del mecanismo de verificación para constatar la no duplicidad de IDClient activos para un mismo organismo dentro del Sistema SICOV, y el reporte de cualquier inconsistencia o posible duplicidad detectada a la Registraduría Nacional del Estado Civil y a la Superintendencia de Transporte.

4.4. OBLIGACIONES DE LOS CRC FRENTE AL SICOV

Además de las obligaciones generales derivadas de la normatividad que rige su actividad y de aquellas específicas contenidas en otros apartados del presente su Anexo Técnico, los CRC deberán cumplir como mínimo con las siguientes obligaciones en relación con el SICOV y su funcionamiento:

Uso del sistema, gestión de información y cumplimiento normativo

1. **Uso obligatorio y adecuado del SICOV:** Utilizar el software de gestión y control del SICOV para la totalidad de los procesos de registro, inscripción, programación, validación de identidad, evaluación, certificación y reporte de información relacionados con la prestación de sus servicios de evaluación de la aptitud física, mental y de coordinación motriz, conforme a los procedimientos y funcionalidades establecidos en este Anexo Técnico y demás directrices que imparta la Superintendencia de Transporte. La expedición de certificados sin el cumplimiento de lo establecido en el SICOV carecerá de validez por todo concepto.

2. **Veracidad e integridad de la información registrada:** Ser enteramente responsables por la veracidad, exactitud, integridad, completitud y oportunidad de toda la información y datos (incluyendo los de sus usuarios, personal del organismo de apoyo, equipos y operación general) que registren o carguen en el SICOV, asumiendo las consecuencias de cualquier omisión, inconsistencia o falsedad, sin perjuicio de las responsabilidades que correspondan al proveedor del SICOV en el aseguramiento tecnológico.

3. **Mantenimiento de información de habilitación y operación:** Mantener permanentemente actualizada en el SICOV toda la información y documentación que soporta el cumplimiento vigente de sus requisitos de registro en el RUNT y de aquellos indispensables para su operación legal y continua, incluyendo licencias de funcionamiento, certificados de conformidad, pólizas, registro de programas, y demás que exija el Ministerio de Transporte. Será su responsabilidad exclusiva la renovación y actualización oportuna de dichos documentos.

4. **Gestión de recursos propios en SICOV:** Mantener permanentemente actualizada en el SICOV la información detallada y veraz de todos los recursos humanos (personal de la salud, certificadores, administrativos, directores), físicos (consultorios, infraestructura de puntos de validación, computadores, equipos) y tecnológicos propios o vinculados que utiliza para la prestación del servicio, incluyendo su estado (activo/inactivo) y

las novedades pertinentes. Será responsabilidad exclusiva e indelegable del CRC informar de manera inmediata y precisa cualquier desvinculación o cambio de personal al sistema, a fin de garantizar la veracidad de la información y la trazabilidad de la operación.

5. **Gestión del IDClient ante RNEC:** Realizar oportunamente, a través del operador del SICOV, el trámite para la obtención y registro en el Sistema de su Identificador Único ante la RNEC (IDClient), y ser responsable de su correcta utilización y de no incurrir en la obtención o uso de múltiples IDClient para eludir controles. Deberá informar cualquier anomalía o presunta duplicidad de IDClient a la Superintendencia de Transporte y a la Registraduría Nacional del Estado Civil.

Cumplimiento de protocolos, seguridad y manejo de infraestructura SICOV

6. **Custodia y uso adecuado de la infraestructura SICOV:** Utilizar de manera adecuada y exclusivamente para los fines previstos, bajo estrictas condiciones de seguridad, la infraestructura de hardware y software del SICOV (dispositivos biométricos, cámaras, pads de firmas, GPS, computadores y cualquier otro elemento) instalada en sus dependencias por el proveedor homologado.

7. **Disposición y adecuación del espacio para el funcionamiento de la infraestructura descentralizada del SICOV**. Disponer y adecuar, para garantizar el ejercicio de las funciones de IVC a cargo de la Superintendencia, el espacio físico necesario para la instalación del rack, equipos y dispositivos de infraestructura descentralizada del SICOV, con las condiciones de acceso y ambientales requeridas para su funcionamiento (aire acondicionado).

8. Se prohíbe de manera expresa el traslado de ubicación de los dispositivos y suministros asignados a un CRC a otro centro o lugar no autorizado. Asimismo, se prohíbe cualquier intento de manipulación, alteración, desinstalación o daño a dichos equipos.

   La Superintendencia de Transporte, en ejercicio de sus funciones, podrá imponer las sanciones administrativas correspondientes y ordenar la suspensión provisional inmediata del servicio en el organismo de apoyo implicado, hasta que se resuelva la situación.

   La sanción se aplicará directamente al CRC infractor, por ser el custodio directo y responsable de la integridad de los equipos.

9. Velar por la custodia diligente y el mantenimiento básico de dichos equipos conforme a los lineamientos del operador del SICOV o la Superintendencia de Transporte.

10. Reportar de inmediato al proveedor del SICOV y a la Superintendencia cualquier daño, pérdida, hurto, falla, manipulación no autorizada, intento de alteración o funcionamiento anómalo de estos componentes.

11. **Adhesión a protocolos operativos y de seguridad:** Cumplir estrictamente y asegurar que todo su personal observe los protocolos operativos, manuales de usuario, guías técnicas y directrices de seguridad (física y lógica) emitidas por la Superintendencia de Transporte o el operador del SICOV para el correcto funcionamiento del Sistema y la seguridad de la información.

12. Cumplir con las condiciones que garantizan la operatividad de los equipos con los que se presta e servicio, incluyendo el mantenimiento, calibración y actualización de los equipos que hacen parte de las funciones del CRC. Esto implica que los equipos deben cumplir con las condiciones mínimas de operación sugeridas por el proveedor o en su defecto los organismos

que acreditan su funcionamiento, y realizar las actualizaciones por obsolescencia tecnológica o la no calibración de equipos que afecten la prestación del servicio.

13. **Reporte de incidentes de seguridad y fraudes:** Reportar de forma inmediata al operador del SICOV cualquier incidente de seguridad informática, acceso no autorizado, intento de fraude, suplantación de identidad, vulnerabilidad detectada en el sistema o uso indebido del SICOV del que tengan conocimiento, ya sea por parte de su personal, usuarios o terceros.

14. **Garantía de conectividad segura y dedicada:** Garantizar, con el proveedor de telecomunicaciones de su elección, un servicio de acceso a internet que cumpla permanentemente con las condiciones técnicas de canal dedicado, ancho de banda garantizado, simetría y Dirección IP Pública Fija exclusiva, descritas en el presente Anexo Técnico. El CRC deberá abstenerse de utilizar este canal dedicado para fines distintos a su operación como organismo de apoyo que puedan comprometer el ancho de banda disponible o la seguridad del túnel de conexión.

Colaboración, transparencia y debida diligencia

15. **Información sobre novedades operativas:** Informar de manera oportuna y veraz al operador del SICOV que le presta el servicio, cualquier novedad, contingencia o situación particular (técnica, administrativa o de otra índole) que pueda afectar la normal y continua prestación de sus servicios o la correcta operación del SICOV en sus instalaciones, incluyendo interrupciones del servicio de energía, internet o comunicaciones, entre otros.

16. **Capacitación del personal propio:** Asegurar que todo su personal que interactúa con el SICOV reciba la capacitación inicial necesaria y participe en los programas de actualización continua sobre el uso adecuado del sistema, sus funcionalidades, los protocolos operativos y de seguridad, y las obligaciones normativas asociadas, conforme a los lineamientos que establezca la Superintendencia o el operador del SICOV.

17. **Facilitación de auditorías e inspecciones:** Permitir, facilitar y prestar toda la colaboración necesaria, diligente y oportuna al personal de la Superintendencia de Transporte y/o del operador del SICOV (cuando este actúe bajo directrices de la Superintendencia) durante la realización de auditorías, visitas de inspección, vigilancia o control, y pruebas del Sistema. Suministrar sin dilación el acceso irrestricto a sus instalaciones, documentos físicos y electrónicos, registros del sistema, personal y cualquier otra información o recurso que sea requerido para el cumplimiento de dichas labores, incluyendo la disponibilidad de los recursos informáticos y humanos necesarios para las verificaciones.

18. **Colaboración en investigaciones:** Colaborar diligentemente con la Superintendencia de Transporte y otras autoridades competentes, suministrando la información y documentación que le sea requerida en el marco de investigaciones relacionadas con la prestación de sus servicios o la información generada por el SICOV.

19. **Obtención de autorizaciones para tratamiento de datos:** Obtener y conservar la autorización previa, expresa e informada de sus usuarios y de todo su personal para el tratamiento de sus datos personales y biométricos a través del SICOV, informándoles claramente sobre las finalidades del tratamiento, el uso de tecnologías de reconocimiento facial, validaciones de identidad y demás aspectos relevantes conforme a la Ley 1581 de 2012 y las políticas que defina la Superintendencia. La autorización expresa de la política de tratamiento de datos deberá darse a través del software del SICOV.

Adhesión a estándares del servicio y uso de funcionalidades SICOV

20. **Cumplimiento de parámetros de servicio verificados por SICOV:** Asegurar que la prestación de los servicios se realice en estricto cumplimiento de la normatividad aplicable y los parámetros verificables a través del SICOV, garantizando que solo se preste el servicio desde la ubicación geográfica autorizada para el Centro, con los equipos de cómputo controlados y autorizados para el proceso y bajo los parámetros definidos en el presente Anexo.

21. **Gestión de exámenes y valoración precisa:** Garantizar la idoneidad en la realización de las evaluaciones prácticas y el correcto registro de sus resultados en SICOV, cuando aplique. Asegurar que las restricciones aplicables para los aspirantes a conducir, cuando así aplique, queden debidamente registradas y se vean reflejadas en el software SICOV.

22. **Expedición de certificados conforme a SICOV:** Asegurar que únicamente el personal debidamente autorizado y con identidad validada biométricamente en SICOV expida los Certificados de aptitud física, mental y de coordinación motriz, y solo cuando el SICOV haya habilitado dicha expedición por el cumplimiento verificado de todos los requisitos. El personal certificador del organismo de apoyo será el único responsable de la decisión de certificación.

23. **Gestión de auditorías de conformidad:** Cargar oportunamente en el SICOV los informes de auditoría del ONAC y registrar los planes de mejora y evidencias de cierre de no conformidades resultantes, en los plazos y formatos que determine la Superintendencia de Transporte.

24. **Cumplimiento de medidas de suspensión:** El CRC deberá acatar de manera inmediata las medidas de suspensión o desconexión del RUNT ordenadas por la Superintendencia de Transporte, a partir del momento en que se haga efectiva la medida en dicho Registro. El CRC podrá hacer seguimiento al tiempo de la suspensión a través del módulo de consulta del SICOV, que a su vez se nutre de la información del RUNT.

25. **Registro de tarifas:** Registrar y mantener actualizadas en SICOV las tarifas de sus servicios, de forma veraz y transparente, asegurando que el SICOV controle el pago de la capacitación.

Hasta aquí el Anexo Técnico

Tabla de control de cambios			
Versión	**Fecha**	**Detalle**	**Responsables**
1.0	30-03-26	Nuevo Anexo Técnico de requisitos de operación del SICOV para CRC	**Elaboró:** Carlos Daniel González Cervera, Asesor de Despacho. **Revisó:** Ángela Paola Galindo Nieto, Directora de Promoción y Prevención de Tránsito y Transporte. Alberto José Daza Sagbini, Superintendente Delegado de Tránsito y Transporte. Gunther Gabriel Ortíz, Jefe Oficina Asesora TIC