

**MINISTERIO DE TRANSPORTE
SUPERINTENDENCIA DE TRANSPORTE**

RESOLUCIÓN NÚMERO _____ DE _____

"Por medio de la cual se modifican las Resoluciones 5790 y 60832 de 2016 de la Superintendencia de Transporte y se introducen mejoras y medidas para fortalecer las capacidades de inspección, Vigilancia y Control a través de su Sistema de Control y Vigilancia para CEA, CIA y OTT"

LA SUPERINTENDENTE DE TRANSPORTE

En ejercicio de las facultades constitucionales, legales y en especial las previstas en la Ley 105 de 1993, Ley 769 de 2002, modificada por la Ley 1383 de 2010, la ley 1702 de 2013, la Ley 2050 de 2020, el Decreto Unico Reglamentario 1079 de 2015, el Decreto 2409 de 2018 y las demás normas concordantes y,

CONSIDERANDO

Que el artículo 2º de la Constitución Política dispuso que las autoridades de la República están instituidas para proteger a todas las personas residentes del país en su vida, honra, bienes, creencias y demás derechos y libertades, y para asegurar el cumplimiento de los deberes sociales del Estado y de los particulares.

Que el artículo 24 de la Constitución Política estableció que todo colombiano tiene derecho a circular libremente por el territorio nacional, siempre sujeto a la intervención y reglamentación de las autoridades competentes para garantía de la seguridad de los habitantes y preservación de un ambiente sano.

Que el artículo 365 de la Constitución Política y el literal b del artículo 2 de la Ley 105 de 1993, establecen que le corresponde al Estado ejercer las funciones de planeación, regulación, control y vigilancia del servicio público de transporte y de las actividades a él vinculadas para asegurar la prestación eficiente a todos los habitantes del territorio nacional del servicio público de transporte, por lo cual están sometidos al régimen jurídico que fije la ley y podrá ser prestados por el Estado, directa o indirectamente, por comunidades organizadas, o por particulares.

Que la Ley 769 de 2002, en su artículo 3, parágrafo 1, dispuso que determinadas funciones de tránsito pueden asignarse, mediante delegación o convenio, para su realización, a entidades públicas o privadas, las que asumen una responsabilidad en calidad de organismos de apoyo a las autoridades de tránsito.

RESOLUCIÓN NÚMERO _____ DE _____

"Por medio de la cual se modifican las Resoluciones 5790 y 60832 de 2016 de la Superintendencia de Transporte y se introducen mejoras y medidas para fortalecer las capacidades de inspección, Vigilancia y Control a través de su Sistema de Control y Vigilancia para CEA, CIA y OTT"

Que el parágrafo 3 de la misma norma legal dispuso que la Superintendencia de Transporte tiene la función de vigilar y controlar a las autoridades, los organismos de tránsito y las entidades públicas o privadas que constituyan organismos de apoyo a las autoridades de tránsito.

Que, el artículo 1 de la Ley 769 de 2002, establece como principios rectores del tránsito terrestre a nivel nacional "la seguridad de los usuarios, la calidad, la oportunidad, el cubrimiento, la libertad de acceso, la plena identificación, la libre circulación, la educación y la descentralización", preceptos conforme a los cuales deben desarrollarse las actividades a cargo de los organismos de apoyo a las autoridades de tránsito.

Por lo anterior, y en aras de mayor claridad acerca de la definición y naturaleza de los CEA, CIA y OTT:

Que, la Ley 1682 de 2013, en su artículo 12, clasificó la actividad desarrollada por los Centros de Enseñanza Automovilística como un servicio conexo al transporte; categoría de la que hacen parte, según se precisó "[t]odos los servicios y/o actividades que se desarrollan o prestan en la infraestructura de transporte y complementan el transporte (...). Entre estos (...) los peritajes y evaluación de vehículos, las terminales de pasajeros y carga, las escuelas de enseñanza [CEA], (...) entre otros."

Que los Centros de Enseñanza Automovilística para Conductores (CEA), son establecimientos docentes de naturaleza pública, privada o mixta que tenga como actividad permanente la capacitación de personas que aspiran a conducir vehículos automotores y motocicletas. Los requisitos para su funcionamiento se encuentran en el artículo 2.3.1.2.1 del Decreto 1079 de 2015, las condiciones de funcionamiento y registro fueron reglamentadas por las Resoluciones 3245 de 2009 y 20203040011355 del 21 de agosto de 2020 del Ministerio de Transporte.

Que, por su parte, los Centros Integrales de Atención (CIA), son establecimientos donde se prestará el servicio de escuela y casa cárcel para la rehabilitación de los infractores a las normas del Código de Tránsito. Este podrá ser operado por el Estado o por entes privados que, a través del cobro de las tarifas por los servicios allí prestados, garantizarán su autosostenibilidad. Reglamentados mediante las Resoluciones 3204 de 2010, 4203 de 2010, (anuladas por el Consejo de Estado), actualmente las reglas para su registro y funcionamiento se encuentra en la Resolución 20203040011355 del 21 de agosto de 2020.

RESOLUCIÓN NÚMERO _____ DE _____

"Por medio de la cual se modifican las Resoluciones 5790 y 60832 de 2016 de la Superintendencia de Transporte y se introducen mejoras y medidas para fortalecer las capacidades de inspección, Vigilancia y Control a través de su Sistema de Control y Vigilancia para CEA, CIA y OTT"

Que, asimismo, al tenor de la definición general contenida en la Ley 769 de 2002, los organismos de tránsito y transporte constituyen organismos de apoyo al tránsito cuando cumplen con los requisitos y son autorizados para impartir cursos a infractores de las normas de tránsito, para los mismos efectos que la norma prevé para los Centros Integrales de Atención.

Ahora bien, la función de vigilancia, inspección y control tiene como propósito establecer el orden en las actividades del sector transporte, incluyendo aquellas relacionadas con el apoyo al tránsito. Esta labor busca mejorar los mecanismos de supervisión y control mediante el uso de medios tecnológicos que faciliten su desarrollo.

Que, mediante el Decreto 2409 de 2018, por el cual se modificó y renovó la estructura de la Superintendencia de Transporte, se estableció la necesidad de modernizar los sistemas de inspección, vigilancia y control. Asimismo, se asignó a la Superintendencia la función de dirigir, supervisar y coordinar el desarrollo de estas actividades, velando por el cumplimiento de las normas relacionadas con la adecuada prestación del servicio público de transporte, la operación portuaria, las concesiones e infraestructura, los servicios conexos y la protección de los usuarios del sector transporte.

Que existen razones suficientes por las cuales, ante situaciones que pueden constituir un riesgo para la prestación de los servicios de apoyo al tránsito, que hacen imperioso que la Superintendencia de Transporte adopte medidas que le permitan actuar preventiva y correctivamente, con base en las normativas que rigen estas actividades, para minimizar el riesgo o impacto de las conductas que atentan contra el interés general y los derechos de todos los actores del sistema de transporte.

Que, el ejercicio de tales atribuciones públicas por parte del Estado procura el mantenimiento del orden y la legalidad en las actividades que se desarrollan en el sector transporte, incluidas aquellas que realizan los organismos de apoyo al tránsito, para lo cual resulta oportuna la adaptación y uso de los avances tecnológicos y científicos que posibilitan el fortalecimiento de las capacidades institucionales de supervisión.

Que, a través del Decreto 2409 de 2018, el Presidente de la República como suprema autoridad administrativa en materia de tránsito, transporte y su infraestructura, facultó a la Superintendencia de Transporte para ejercer las funciones de vigilancia, inspección y control de la debida prestación del servicio de transporte, servicios conexos y la protección de los usuarios del sector.

RESOLUCIÓN NÚMERO _____ DE _____

"Por medio de la cual se modifican las Resoluciones 5790 y 60832 de 2016 de la Superintendencia de Transporte y se introducen mejoras y medidas para fortalecer las capacidades de inspección, Vigilancia y Control a través de su Sistema de Control y Vigilancia para CEA, CIA y OTT"

Que, la Superintendencia de Transporte, en el marco de las funciones de que tratan los numerales 2 y 15 del artículo 7 del Decreto 2409 de 2018, puede adoptar las políticas, metodologías y procedimientos y expedir los reglamentos, manuales e instructivos que sean necesarios para ejercer la vigilancia, inspección y control.

Que, asimismo, el numeral 6 del artículo 5 del Decreto 2409 de 2018, con fundamento en lo dispuesto en el artículo 15 párrafo 4 de la Constitución Política, dispone que la Superintendencia de Transporte está facultada para solicitar a las autoridades y particulares el suministro y entrega de documentos públicos, privados, reservados, garantizando la cadena de custodia, y cualquier otra información que se requiera para el correcto ejercicio de sus funciones.

Que, en el marco de tales funciones, es deber de la Superintendencia verificar el cumplimiento de las condiciones, requisitos y procedimientos establecidos en las normas legales y reglamentarias expedidas por el Congreso de la República, el Ministerio de Transporte y la misma Superintendencia.

Que, para tales menesteres, la Superintendencia ha enfocado sus esfuerzos en la implementación de mecanismos que promuevan el cumplimiento de su misión, desarrollando estrategias enfocadas en una supervisión preventiva, que no solamente reactiva, y que propenda, además de hacer seguimiento a la prestación del servicio de transporte, su infraestructura y los servicios complementarios, por la protección de los derechos de los usuarios del sector.

Que, desde el año 2018, la Superintendencia ha venido en un proceso de renovación con el propósito de tener una mayor capacidad técnica y tecnológica para fortalecer la función de vigilancia preventiva e implementar estrategias encaminadas a la protección de los usuarios del sector, con el fin de incrementar su confianza en la prestación de los diferentes servicios que en este confluyen.

Que, el Congreso de la República, con la aprobación de la Ley 1450 de 2011, por medio de la cual se aprobó el "Plan Nacional de Desarrollo 2010-2014", definió la Seguridad Vial como una política de Estado, razón que lo llevó a otorgarle a la Superintendencia de Transporte, como una de las estrategias orientadas a lograr el fortalecimiento de las capacidades de la administración, una facultad para expedir la reglamentación referente a las características técnicas mínimas que debían tener los sistemas de seguridad documental que debían implementarse por parte de los organismos de apoyo a las autoridades de tránsito.

RESOLUCIÓN NÚMERO _____ DE _____

"Por medio de la cual se modifican las Resoluciones 5790 y 60832 de 2016 de la Superintendencia de Transporte y se introducen mejoras y medidas para fortalecer las capacidades de inspección, Vigilancia y Control a través de su Sistema de Control y Vigilancia para CEA, CIA y OTT"

Que, para la época, los servicios ofertados por los organismos de apoyo a las autoridades de tránsito eran señalados y vistos con desconfianza, dado el auge de conductas reprochables que se enquistaron en la actividad, con las que se vulneraban sistemáticamente las disposiciones reglamentarias vigentes. Esta situación despertó en las instituciones del Estado el interés por crear mecanismos que permitieran a la Administración intervenir en la actividad de estos entes, de tal manera que se pudiera dotar a la Superintendencia de los instrumentos necesarios para ejercer su función de control.

Que, consecuentemente, en uso de la atribución legal conferida y en la búsqueda de crear un mecanismo de seguridad documental que permitiera ejercer la función de vigilancia preventiva y reactiva con mayor eficiencia y eficacia, con miras a impactar positivamente los servicios ofrecidos por los organismos de apoyo a las autoridades de tránsito, tanto en transparencia como en calidad, la Superintendencia de Transporte advirtió la necesidad de disponer de herramientas que le permitieran capturar y acceder a información precisa sobre los procedimientos que se adelantan al interior de estos sujetos de vigilancia, pues sólo a partir del recaudo de información de la operación era posible determinar si la expedición de los certificados que estos expiden se ajustaba y honraba las obligaciones y exigencias previstas en las normas vigentes.

Que, para tal propósito, la Superintendencia de Transporte reglamentó las características y componentes de un sistema de control, soportado en las tecnologías de la información, que ocupaba la instalación de un conjunto de dispositivos de hardware y soluciones de software que le permitieran lograr en primera medida un enteramiento, con información precisa y detallada, de la operación al interior de los organismos de apoyo, en las distintas fases de la prestación de sus servicios. A este sistema se denominó Sistema de Control y Vigilancia y con su creación se establecieron parámetros técnicos para lograr una manera eficiente y eficaz de vigilar y ejercer control.

Que, además de ofrecer una vista continua de la operación de los organismos de apoyo que permite verificar que el proceso de certificación a su cargo se realiza de conformidad con lo dictado por las normas del caso, el Sistema se pensó como un mecanismo seguro de almacenamiento y transmisión de dicha información, de tal manera que no pudiera ser alterada por parte de los vigilados.

Que, en el ejercicio de las funciones de inspección, vigilancia y control que le corresponden a la Superintendencia de Transporte, el Sistema de Control y Vigilancia constituye una herramienta tecnológica esencial para el cumplimiento de un fin público, consistente en la supervisión de los organismos de apoyo al

RESOLUCIÓN NÚMERO _____ DE _____

"Por medio de la cual se modifican las Resoluciones 5790 y 60832 de 2016 de la Superintendencia de Transporte y se introducen mejoras y medidas para fortalecer las capacidades de inspección, Vigilancia y Control a través de su Sistema de Control y Vigilancia para CEA, CIA y OTT"

tránsito y de los usuarios. Por lo tanto, toda la información que se capta, registra, procesa, almacena y transmite a través del SICOV, incluyendo datos personales y sensibles, se genera y recauda en virtud y para el ejercicio de esta función pública delegada al Estado. En consecuencia, la determinación del uso, control y disposición final de dicha información recaen de manera exclusiva en la Superintendencia de Transporte, independientemente de quién opere o administre tecnológicamente el sistema. La facultad de los operadores homologados sobre dicha información se limita a su administración y custodia bajo las directrices y requerimientos de la Superintendencia, a título de encargados, garantizando su integridad, confidencialidad, disponibilidad y trazabilidad. Cualquier interrupción, retención indebida o disposición no autorizada de la información esencial para la continuidad de la función de vigilancia y control acarreará las consecuencias legales pertinentes.

Que, en ese contexto fueron definidas y reglamentadas las características principales y componentes generales del Sistema de Control y Vigilancia para de los Centros de Enseñanza Automovilística (CEA) y Centros Integrales de Atención (CIA) a través de las Resoluciones No. 5790 de 2016 y 60832 de 2016; esta última a través de la cual se expidió el anexo técnico contentivo de sus características y funcionalidades, así como los requisitos de carácter financiero, jurídico y administrativo que deben cumplir los interesados en ser homologados como proveedores del Sistema.

Que, mediante las Resoluciones 25778 del 7 de junio de 2018 y 28349 de junio 22 del mismo año, la Superintendencia de Transporte autorizó, luego de haber corroborado el cumplimiento de las condiciones exigidas en los mentados actos administrativos, al CONSORCIO INTEGRADO DE SEGURIDAD CEAS-CIAS y a OLIMPIA MANAGEMENT S.A., respectivamente, como operadores homologados del Sistema de Control y Vigilancia para CEA, CIA y OTT. No obstante, el Sistema de Control y Vigilancia para Centros Integrales de Atención y Organismos de Tránsito y Transporte nunca fue implementado.

Que, la Ley 2050 de 2020, en su artículo 22, modificó el esquema de provisión de los Sistemas de Control y Vigilancia, al establecer que la Superintendencia de Transporte debe realizar, para el ejercicio de sus funciones, directamente o indirectamente a través de dicho Sistema, visitas periódicas a los organismos de apoyo a las autoridades de tránsito con el fin de verificar el cumplimiento de los mandatos legales y reglamentarios.

Que, el artículo 23 de la misma Ley adicionó un párrafo al artículo 136 de la Ley 769 de 2002, determinando que los cursos a los infractores de las normas

RESOLUCIÓN NÚMERO _____ DE _____

"Por medio de la cual se modifican las Resoluciones 5790 y 60832 de 2016 de la Superintendencia de Transporte y se introducen mejoras y medidas para fortalecer las capacidades de inspección, Vigilancia y Control a través de su Sistema de Control y Vigilancia para CEA, CIA y OTT"

de tránsito podrán dictarse también virtualmente, para lo cual quien lo dicta deberá garantizar la autenticación biométrica del ciudadano en la forma en que determine el Ministerio de Transporte, a través del Sistema de Control y Vigilancia de la Superintendencia de Transporte, a fin de lograr la identificación del infractor de forma segura, su registro y permanencia en el curso.

Que, a través de la Ley 2283 de 2023, el Congreso de la República estableció un plazo de seis (6) meses para que la Superintendencia de Transporte implementara el Sistema de Control y Vigilancia para los Centros Integrales de Atención.

Que, en el mismo sentido, la Ley 2294 de 2023 (Plan Nacional de Desarrollo 2022-2026) "Colombia Potencia Mundial de la Vida", artículo 180, Parágrafo 1, determinó la obligación para la Superintendencia de Transporte de vincular al Sistema de Control y Vigilancia (SICOV), en un plazo máximo de seis (6) meses, a todas las entidades que dictan cursos para obtener descuentos en las sanciones aplicables por la infracción de las normas de tránsito, es decir, a Centros integrales de Atención y Organismos de Tránsito y Transporte autorizados para ello.

Que, teniendo en cuenta lo anterior, resulta imperativo que la Superintendencia de Transporte, en el ejercicio de su función de IVC, ordene a los proveedores tecnológicos dar prioridad al despliegue y puesta en operación de la nueva versión del SICOV en los CIA y OTT.

Que, por lo tanto, la Superintendencia de Transporte debe continuar ejerciendo las funciones de inspección, vigilancia y control a su cargo sobre las actividades desplegadas por los organismos de apoyo a las autoridades de tránsito, por lo que debe continuar empeñando esfuerzos dirigidos a mejorar la eficiencia y eficacia de sus mecanismos y herramientas de control, lo cual pasa por el fortalecimiento de los Sistemas de Control y Vigilancia creados para los distintos actores sujetos de la vigilancia.

Que, la Superintendencia de Transporte reconoce que el fortalecimiento de sus capacidades de inspección, vigilancia y control sobre los organismos de apoyo y la prestación de sus servicios es determinante para impactar de manera positiva el tránsito y transporte del país, en beneficio de la población en su conjunto.

Que, en ese sentido, el Plan Nacional de Seguridad Vial adoptado por el Estado colombiano para el decenio 2022-2031, a través del Decreto 1430 del 29 de julio de 2022, fijó como objetivo general de la reducción del 50% en el número de

RESOLUCIÓN NÚMERO _____ DE _____

"Por medio de la cual se modifican las Resoluciones 5790 y 60832 de 2016 de la Superintendencia de Transporte y se introducen mejoras y medidas para fortalecer las capacidades de inspección, Vigilancia y Control a través de su Sistema de Control y Vigilancia para CEA, CIA y OTT"

muertes y lesiones graves para 2031. Para lograrlo, resulta fundamental contar con servicios de capacitación de conductores y de reeducación de infractores más rigurosos y legalmente impartidos, pues esta es la base para tener conductores más competentes, conscientes del riesgo y respetuosos de las normas.

Que, en línea con lo anterior, el mejoramiento de capacidades de la Superintendencia para la vigilancia de estos actores impacta potencialmente de manera positiva en dos de las Áreas de Acción de seguridad vial, a saber, el Comportamiento seguro de los actores viales (Área No. 4), y el Cumplimiento de las normas de tránsito en materia de seguridad vial (Área No. 5).

Que, el mejoramiento de estas capacidades institucionales también es sustancial dado el universo de vigilados que hacen parte de la categoría de organismos de apoyo a las autoridades de tránsito, que ronda actualmente aproximadamente los 2640.

Que la labor de vigilar a los más de 1290 CEA y 441 CIA y OTT que dictan cursos a infractores en el país, sólo se posibilita en la medida que el Estado apalanque sus capacidades en el aprovechamiento de las soluciones que ofrece la implementación y uso de la tecnología.

Que, ante esa necesidad, la Superintendencia de Transporte emprendió en 2022 una estrategia de transformación digital que sigue en curso, que apuesta, precisamente, por el fortalecimiento de las capacidades institucionales a partir del uso de sistemas y herramientas de TI, la innovación en procesos y la implementación de estrategias de co-creación para el cumplimiento de los objetivos de la entidad.

Que, dado que el Sistema que se encuentra en operación es objeto de importantes actualizaciones y ajustes para fortalecer el control de la actividad; se vuelve necesario revisar, mejorar y redefinir algunas de sus características técnicas, funciones y condiciones de operación.

Que, la presente transformación del Sistema de Control y Vigilancia se enmarca en la política pública de gobierno digital y en el fomento de las Tecnologías de la Información y las Comunicaciones (TIC) como herramienta fundamental para la modernización y eficiencia del Estado colombiano.

Que, tal y como se establece en el artículo 11 del Decreto 2409 de 2018, se asignan funciones a la Oficina de Tecnologías de Información y las

RESOLUCIÓN NÚMERO _____ DE _____

"Por medio de la cual se modifican las Resoluciones 5790 y 60832 de 2016 de la Superintendencia de Transporte y se introducen mejoras y medidas para fortalecer las capacidades de inspección, Vigilancia y Control a través de su Sistema de Control y Vigilancia para CEA, CIA y OTT"

Comunicaciones para dotar a la entidad de una dependencia responsable de las tecnologías de información, que permita modernizar los sistemas de inspección, vigilancia y control y así generar importantes eficiencias y mejores resultados.

Que, la Ley 1341 de 2009, la cual define los principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones, establece en su artículo 2, entre otras disposiciones, que el fomento, la promoción y el desarrollo de las Tecnologías de la Información y las Comunicaciones son una política de Estado que involucra a todos los sectores y niveles de la administración pública y de la sociedad, para contribuir al desarrollo educativo, cultural, económico, social y político e incrementar la productividad, la competitividad, el respeto a los Derechos Humanos inherentes y la inclusión social.

Que, a través del Decreto 767 de 2022 se actualizó la Política de Gobierno Digital, con el propósito de fortalecer los procesos de transformación e innovación digital en el sector público, promoviendo el uso y aprovechamiento de las tecnologías de la información y las comunicaciones (TIC) como herramienta fundamental para mejorar la calidad de vida de los ciudadanos y habitantes del territorio nacional, siendo una política que busca lograr un Estado más eficiente y transparente para el ciudadano.

Que, la interoperabilidad, en el marco de la Política de Gobierno Digital del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC), permite a las entidades públicas intercambiar información y coordinar procesos de manera ágil y eficiente, lo cual facilita la prestación de servicios integrados y evita la duplicación de esfuerzos en la administración pública, además de optimizar los recursos públicos, permitiendo una mejor respuesta a las necesidades de los usuarios.

Que, asimismo, la interoperabilidad promueve la conectividad y el flujo seguro de datos entre los diferentes sistemas y plataformas del Estado, asegurando que la información sea accesible y compartida de manera confiable, preservando la calidad, integridad y privacidad de los datos de los ciudadanos.

Que, el intercambio de información entre la Entidad, los usuarios y los vigilados se hará a través de mensajes de datos, de conformidad con lo establecido en la Ley 527 de 1999, los cuales son admisibles y tienen fuerza probatoria.

Que, la Ley 2294 de 2023, establece en el artículo 143 que el Ministerio de Tecnologías de la Información y las Comunicaciones debe diseñar e implementar

RESOLUCIÓN NÚMERO _____ DE _____

"Por medio de la cual se modifican las Resoluciones 5790 y 60832 de 2016 de la Superintendencia de Transporte y se introducen mejoras y medidas para fortalecer las capacidades de inspección, Vigilancia y Control a través de su Sistema de Control y Vigilancia para CEA, CIA y OTT"
estrategias para democratizar las TIC y desarrollar la sociedad del conocimiento y la tecnología en el país, a través de medidas como:

"[...] 5. Implementar iniciativas de transformación digital como herramienta para la productividad, la generación de empleo, la dinamización de la economía en las regiones y la potencialización de la economía popular.

6. Fortalecer el Gobierno Digital para tener una relación eficiente entre el Estado y el ciudadano, que lo acerque y le solucione sus necesidades, a través del uso de datos y de tecnologías digitales para mejorar la calidad de vida.

7. Promover un entorno digital seguro para generar confianza en el uso y apropiación de las TIC. [...]"

Que, en este contexto de avance tecnológico y compromiso con la modernización del Estado, el Sistema de Control y Vigilancia para CEA, CIA y OTT se integra como un componente esencial de la visión de los Sistemas Inteligentes de Transporte y de la propia estrategia de transformación digital de la Superintendencia de Transporte.

Que, la Ley 1450 de 2011 en su artículo 84 definió los Sistemas Inteligentes de Transporte (SIT) como el conjunto de soluciones tecnológicas, informáticas y de telecomunicaciones que recolectan, almacenan, procesan y distribuyen información, los cuales deben diseñarse para mejorar la operación, la gestión y la seguridad del transporte y el tránsito en el país.

Que, en línea con lo anterior, el Decreto 1079 de 2015, en el Título 1 de la Parte 5, artículos 2.5.1.3. y siguientes, establece que el Sistema Inteligente Nacional para la Infraestructura, el Tránsito y el Transporte (SINITT), que será administrado por el Ministerio de Transporte, tendrá por objetivo consolidar y proveer la información que suministren a su vez los subsistemas de gestión que lo integren, así como también la interoperabilidad de los SIT implementados a nivel nacional, bajo los principios de "excelencia en el servicio al ciudadano, apertura y reutilización de datos públicos, estandarización, interoperabilidad, neutralidad tecnológica, innovación y colaboración (...)".

Que, asimismo, el artículo 2.5.1.4. del Decreto 1079 de 2015 estableció que todos los actores estratégicos deberán interpretar y aplicar las disposiciones que regulan los Sistemas Inteligentes para la Infraestructura, el Tránsito y el

RESOLUCIÓN NÚMERO _____ DE _____

"Por medio de la cual se modifican las Resoluciones 5790 y 60832 de 2016 de la Superintendencia de Transporte y se introducen mejoras y medidas para fortalecer las capacidades de inspección, Vigilancia y Control a través de su Sistema de Control y Vigilancia para CEA, CIA y OTT"

Transporte (SIT) al poner en marcha cualquier subsistema de gestión que vaya a componer el SINITT, conforme a los principios allí mencionados.

Que, ante esa necesidad, la Superintendencia de Transporte emprendió en 2023 una estrategia de transformación digital que apuesta precisamente por el fortalecimiento de las capacidades institucionales a partir del uso de sistemas y herramientas de TI, la innovación en procesos y la implementación de estrategias de co-creación para el cumplimiento de los objetivos de la entidad.

Que, la Superintendencia de Transporte está adoptando lineamientos de la Gestión de TI y se encuentra impulsando iniciativas de TI que buscan transformar las capacidades de la Entidad, para lo cual tiene en marcha tres proyectos con los que busca: 1) Unificar los sistemas de información misionales de la Entidad; 2) Transformar digitalmente a la Superintendencia de Transporte con fundamento en la política de gobierno digital; y 3) Estructurar, analizar, procesar, definir y divulgar información relevante para todos los interesados en las funciones a cargo de la Superintendencia de Transporte.

Que, adicionalmente, la Oficina de Tecnologías de la Información y las Comunicaciones de la Superintendencia de Transporte, en cumplimiento de los proyectos de su Plan Estratégico de Tecnologías de la Información (PETI), incluyó herramientas fundamentales para la implementación de nuevas tecnologías bajo los lineamientos del Ministerio de Tecnologías de la Información y las Comunicaciones (MinTIC).

Que, a través de la Resolución 12173 de 2024, la Superintendencia de Transporte apropió una estrategia de transformación digital, denominada "SuperTransporte digital", la cual fue diseñada principalmente para: 1) facilitar el acceso y gestión de trámites de forma electrónica, garantizando la eficiencia, transparencia y accesibilidad a los usuarios y para 2) modernizar y actualizar los sistemas de información de la entidad, en aras de fortalecer y mejorar sus procesos tecnológicos, con el fin de lograr mayor seguridad y eficiencia en la atención de los trámites, procesos misionales y operativos de la entidad.

Que, por medio de la Resolución 14305 de 2024, la Superintendencia adicionó un capítulo al Título V de la Circular Única de Infraestructura, a través de la cual definió y adoptó los lineamientos y condiciones técnicas, tecnológicas y operativas de funcionamiento de la plataforma tecnológica denominada "Sistema Inteligente Nacional de Supervisión al Transporte (SINST – VIGIA 2)", por medio de la cual la entidad busca gestionar de manera integral los reportes de información y documentos por parte de los obligados a utilizar el Sistema,

RESOLUCIÓN NÚMERO _____ DE _____

"Por medio de la cual se modifican las Resoluciones 5790 y 60832 de 2016 de la Superintendencia de Transporte y se introducen mejoras y medidas para fortalecer las capacidades de inspección, Vigilancia y Control a través de su Sistema de Control y Vigilancia para CEA, CIA y OTT"

atender requerimientos, realizar trámites y consultas en línea, además de facilitar la comunicación directa con la Superintendencia de Transporte.

Que, el Sistema de Control y Vigilancia implementado en los CEA, CIA y OTT es una solución tecnológica de vigilancia activa e integral de la Superintendencia de Transporte, compuesta por infraestructura de hardware, software, despliegue de dispositivos y servicios tecnológicos, que le permite a la entidad ejercer funciones de inspección, vigilancia y control sobre la operación de los CEA, CIA y OTT. Así mismo, el sistema facilita la verificación del cumplimiento de las condiciones y obligaciones establecidas en la normativa vigente, y actúa como un mecanismo integral para captar, registrar, almacenar, procesar, analizar y reportar, en tiempo real, información relacionada con la prestación del servicio por parte de estos sujetos vigilados.

Que, en el marco de la estrategia de transformación digital de la Superintendencia de Transporte y de conformidad con los lineamientos de la Política de Gobierno Digital, resulta esencial contar con una adecuada gobernanza de datos y servicios para el funcionamiento del Sistema de Control y Vigilancia de CEA, CIA y OTT. Dicha gobernanza permite asegurar la integridad, calidad, interoperabilidad, trazabilidad y seguridad de la información recolectada por el sistema, garantizando así procesos más eficaces de inspección, vigilancia y control. Además, fortalece la toma de decisiones basadas en datos, promueve la transparencia institucional, optimiza los recursos públicos y mejora la atención y confianza de los ciudadanos y sujetos vigilados en el ejercicio de la función pública.

Que, el Sistema de Control y Vigilancia de CEA, CIA y OTT hace parte del Sistema Inteligente Nacional de Supervisión al Transporte (SINST – VIGIA 2), el cual a su vez se integrará al Sistema Inteligente Nacional para la Infraestructura, el Tránsito y el Transporte (SINITT) del Ministerio de Transporte una vez este inicie su operación, conforme a lo dispuesto en el Decreto 1079 de 2015.

Que, en el marco del proceso de transformación digital que adelanta la Superintendencia de Transporte, se hace necesario actualizar las condiciones técnicas, tecnológicas y operativas del Sistema de Control y Vigilancia de los CEA, CIA y OTT, con el fin de garantizar mayor eficiencia, seguridad y calidad en los procesos de inspección, vigilancia y control.

Que, la introducción de mejoras al Sistema existente, gracias a nuevos avances de tecnología que están disponibles y/o a capacidades que pueden ser desarrolladas por parte de los operadores homologados, debe permitir a la

RESOLUCIÓN NÚMERO _____ DE _____

"Por medio de la cual se modifican las Resoluciones 5790 y 60832 de 2016 de la Superintendencia de Transporte y se introducen mejoras y medidas para fortalecer las capacidades de inspección, Vigilancia y Control a través de su Sistema de Control y Vigilancia para CEA, CIA y OTT"

Superintendencia dar un salto cualitativo en su capacidad para prevenir, detectar, controlar y monitorear conductas ilegales y prácticas reprochables evidenciadas en la prestación de los servicios de tránsito que se prestan en CEA, CIA y OTT.

Que, en línea de lo dicho, el fortalecimiento de capacidades de la Superintendencia pasa necesariamente por un reforzamiento de las funciones de carácter preventivo del Sistema, a través del afinamiento de mecanismos de alerta y el desarrollo y puesta en productivo de funciones automáticas de activación automática frente a la evidencia de conductas que puedan contravenir el ordenamiento jurídico. Estas herramientas deben contribuir a evitar que se mantengan en el tiempo actividades u operaciones sospechosas, generando también reportes inmediatos.

Que con estas actualizaciones se pretende, en últimas, implementar mecanismos efectivos para responder a las amenazas, debilidades y retos y que desafían actualmente la legalidad de los servicios a cargo de este grupo de vigilados, lo que conduce invariablemente a volver sobre los fines y las bases sobre los cuales fue concebido y puesto en marcha el SICOV.

Que, para esos efectos, se han identificado y analizado al interior de la Superintendencia de Transporte varias mejoras requeridas por el Sistema de Control y Vigilancia que deben perdurar y mejorarse en el transcurso del tiempo.

Que, en dicho proceso, se han considerado insumos de diferentes fuentes de información, entre las que se destacan, por su importancia: (i) la experiencia y conocimiento acumulados por la Superintendencia durante el ejercicio de sus atribuciones; (ii) los resultados del Contrato de consultoría No. 287 de 2021 celebrado por la Superintendencia con el mismo objetivo con Grow Data S.A.S.; (iii) las reuniones y conversaciones sostenidas con los proveedores del Sistema de Control y Vigilancia de 2022 a 2025; (iv) los resultados del Convenio de Asociación No. 217 de 2020 celebrado por la Superintendencia de Transporte con la Confederación Nacional de Organismos de Apoyo al Tránsito, con el propósito, entre otros, de identificar y analizar mejoras que podían introducirse al Sistema de Control y Vigilancia de organismos de apoyo al tránsito de la Superintendencia para fortalecer la legalidad en la actividad a cargo de los organismos de apoyo; y (v) en el sentir expresado por voceros de los CEA, CIA, OTT y sus agremiaciones, quienes han reiterado en distintos escenarios y oportunidades su preocupación por las que consideran vulnerabilidades de la herramienta.

RESOLUCIÓN NÚMERO _____ DE _____

"Por medio de la cual se modifican las Resoluciones 5790 y 60832 de 2016 de la Superintendencia de Transporte y se introducen mejoras y medidas para fortalecer las capacidades de inspección, Vigilancia y Control a través de su Sistema de Control y Vigilancia para CEA, CIA y OTT"

Que, como parte de los compromisos de la consultoría especializada realizada por Growdata S.A.S., el consulto (i) elaboró un diagnóstico con las características actuales del Sistema de Control y Vigilancia para CEA, en el que se consideraron y analizaron en detalle las soluciones tecnológicas de los actuales proveedores homologados por la Superintendencia de Transporte; y (ii) presentó una propuesta de mejora del Sistema, construida desde un enfoque especializado que empleó metodologías y marcos de trabajo robustos con base en los cuales se desarrolló una arquitectura objetivo del SICOV y con base en esta, se consideró un modelo de gobierno y operación de este.

Que, corolario de lo anterior, con fundamento en las fuentes de información aludidas, especialmente la que resultó del Contrato de consultoría celebrado con Grow Data S.A.S., esta autoridad ha advertido con claridad la necesidad de aplicar mejoras específicas al Sistema, identificando principalmente un refuerzo de las capacidades de:

- i) Verificación del cumplimiento ininterrumpido de los requisitos de registro en el RUNT y de operación por parte de los vigilados, los cuales constituyen estándares y condiciones mínimos exigidos de forma permanente. El Sistema, no puede perderse de vista, es el medio principal del que dispone la Superintendencia para enterarse del cumplimiento de estas obligaciones por parte de los vigilados;
- ii) Supervisión minuciosa del desarrollo de distintas etapas de la operación de estos actores al prestar el servicio, especialmente en lo que atañe a la validación de identidad de los usuarios e instructores, y el reporte de información precisa sobre las distintas etapas de la capacitación;
- iii) La actualización permanente de información de operación;
- iv) La seguridad en la transmisión de la información para evitar su manipulación;
- v) La obtención y procesamiento continuo de información sobre la operación de estos entes a fin de corroborar el cumplimiento o incumplimiento de las normas que reglamentan la función de tránsito a su cargo;
- vi) Reacción oportuna frente a incumplimientos de las reglas y términos de uso del Sistema y/o incumplimientos de la normatividad vigente; y
- vii) Transmisión de la información y acceso de la Superintendencia al reporte de novedades especiales sobre la operación del Sistema.

Que, para tales efectos, se han definido diferentes mecanismos que permiten lograr las mejoras identificadas del Sistema, por lo que es necesario hacer una

RESOLUCIÓN NÚMERO _____ DE _____

"Por medio de la cual se modifican las Resoluciones 5790 y 60832 de 2016 de la Superintendencia de Transporte y se introducen mejoras y medidas para fortalecer las capacidades de inspección, Vigilancia y Control a través de su Sistema de Control y Vigilancia para CEA, CIA y OTT"

modificación y/o creación de nuevas funciones, la parametrización de algunas existentes, lo cual se posibilita principalmente con el desarrollo de software, la adquisición e implementación de dispositivos y tecnología de reconocimiento facial para validar la identidad de los usuarios y el personal vinculado a los CEA, CIA y OTT y la gestión del conocimiento sobre los cambios directamente con estos actores.

Que, la modificación y creación de nuevas funciones y parámetros en el Sistema conlleva a definir y repensar los requisitos para permitir la expedición de certificados por parte de los organismos de apoyo al tránsito. A modo de ejemplo, el cumplimiento de los requisitos mínimos exigidos para el registro y la operación de los CEA, CIA y OTT durante toda la prestación del servicio, constituye condición sine qua non para que estos puedan utilizar las funciones del Sistema y especialmente expedir certificados.

Que, para tal menester, se debe optar por una parametrización en el Sistema que, ante la falta de evidencia vigente sobre el cumplimiento de obligaciones, genere una alerta y una marcación de irregularidad sobre el uso de aquellos recursos que no cumplan con las exigencias reglamentarias.

Que lo anterior debe acompañarse de una parametrización del Sistema que, ante la evidencia de incumplimientos de obligaciones o condiciones expresamente exigidas en la normatividad vigente, active alertas tempranas y automáticas. Dichas alertas generarán una marcación de irregularidad sobre todos los servicios que se presten bajo esa condición, dejando una trazabilidad completa a disposición de la Superintendencia de Transporte para el ejercicio de sus funciones de inspección, vigilancia y control.

Que, asimismo, se priorizó la inclusión de tecnología de reconocimiento facial para los procesos de validación de identidad de los usuarios del servicio y personal vinculado al CEA, CIA y OTT, gracias a los avances en las capacidades de procesamiento de información y a la precisión permitida por esa tecnología, que se consolida como una herramienta confiable y de alta eficacia en diversas aplicaciones a nivel mundial, convirtiéndose en una alternativa competitiva frente a otros métodos biométricos, lo cual le permite al Estado y particularmente a la Superintendencia mantenerse a la vanguardia con el mecanismo de gestión de validación de identidad de personas.

Que, la tecnología de reconocimiento facial ofrece un alto nivel de precisión en la identificación de personas en situaciones en las que el uso de huellas dactilares puede verse limitado, como en el caso de individuos con huellas dactilares

RESOLUCIÓN NÚMERO _____ DE _____

"Por medio de la cual se modifican las Resoluciones 5790 y 60832 de 2016 de la Superintendencia de Transporte y se introducen mejoras y medidas para fortalecer las capacidades de inspección, Vigilancia y Control a través de su Sistema de Control y Vigilancia para CEA, CIA y OTT" deterioradas o alteradas por condiciones de salud, lo que garantiza una mayor inclusión en los procesos de validación de identidad.

Que, la implementación del reconocimiento facial no solo mejora la seguridad en la validación de identidad, sino que también optimiza el tiempo y los recursos dedicados a la realización del trámite, contribuyendo a una administración pública más eficiente y moderna, acorde con las expectativas de los ciudadanos en un entorno digitalizado.

Que, sin perjuicio de lo anterior, en el marco del propósito de garantizar un sistema robusto y accesible de validación de identidad para los usuarios, es fundamental contar con un mecanismo alternativo que permita validar la identidad en caso de que el sistema de reconocimiento facial falle, no esté disponible o no sea viable debido a problemas técnicos o situaciones particulares de los usuarios, pues de esta manera se puede asegurar la continuidad de los servicios sin interrupciones y con altos estándares de seguridad.

Que, en consideración de las diversas condiciones fisiológicas de los ciudadanos, como el deterioro de las huellas dactilares o problemas dermatológicos, entre otros, es imperativo que los nuevos dispositivos lectores de huellas dactilares cuenten con tecnología avanzada en lectura de las capas de la piel humana, para garantizar que incluso personas con huellas deterioradas o condiciones similares puedan ser correctamente identificadas.

Que, la actualización de los dispositivos lectores de huella dactilar a tecnología especializada, con capacidades mejoradas, permitirá reducir significativamente los fallos en el proceso de validación de identidad, incluso en casos de huellas deterioradas o afectadas por afecciones dermatológicas. No obstante, en aquellos casos en los que persistan dificultades para una validación exitosa mediante el cotejo dactilar, se procederá con una verificación adicional a través de la comparación entre la selfie y el template, tanto del aspirante como del personal del CEA, CIA u OTT con que se presenten inconvenientes. En caso de que esta verificación tampoco sea satisfactoria, se aplicará un procedimiento claro y seguro de excepción biométrica. De esta manera, se garantiza la continuidad del proceso y la integridad en la verificación de identidad.

Que, con la incorporación de lectores de huella especializados, se da respuesta a una necesidad urgente de actualización tecnológica que no solo mejora la capacidad de los sistemas biométricos, sino que también refleja el compromiso del Estado con el acceso igualitario y la prestación de servicios públicos sin

RESOLUCIÓN NÚMERO _____ DE _____

"Por medio de la cual se modifican las Resoluciones 5790 y 60832 de 2016 de la Superintendencia de Transporte y se introducen mejoras y medidas para fortalecer las capacidades de inspección, Vigilancia y Control a través de su Sistema de Control y Vigilancia para CEA, CIA y OTT" exclusiones, asegurando que todos los ciudadanos puedan validar su identidad de forma adecuada.

Que, la naturaleza dinámica y la rápida evolución de las Tecnologías de la Información y las Comunicaciones (TIC), especialmente en áreas como la biometría, la inteligencia artificial y la seguridad de la información, hacen imperativo que el Sistema de Control y Vigilancia para los Centros de Enseñanza Automovilística, Centros Integrales de Atención y Organismos de Tránsito y Transporte no solo incorpore las soluciones más avanzadas disponibles a la fecha de la presente resolución, sino que también cuente con mecanismos y la obligación permanente de sus operadores homologados de vigilar el mercado tecnológico e incorporar proactivamente las mejoras y actualizaciones que surjan, a fin de evitar la obsolescencia tecnológica y asegurar la continua robustez, eficiencia y eficacia del SICOV en la prevención y detección de fraudes.

Que, como se advierte, la actualización tecnológica del Sistema de validación de identidad tiene como objetivo fortalecer el control y la seguridad en los servicios que los Organismos de Apoyo al Tránsito ofrecen a la población, asegurando que los usuarios sean correctamente identificados en todo momento, para evitar la suplantación de identidad y garantizar la integridad de los trámites.

Que, adicionalmente, un ajuste en la parametrización para exigir la validación de identidad en tres momentos distintos —antes, durante y después de la realización de la clase o curso— es una medida clave para prevenir cualquier intento de fraude, asegurando que solo aquellos usuarios que hayan completado satisfactoriamente los tres procesos de validación sean considerados como presentes en el servicio.

Que, la modernización del Sistema pretendida permitirá automatizar la clasificación de las clases agendadas por los usuarios en función de su cumplimiento con los tres momentos de validación de identidad, lo que contribuirá a una mayor transparencia, eficiencia y confiabilidad en los procesos de prestación de servicios públicos, limitando la posibilidad de intervenciones humanas que puedan generar errores o manipulación.

Que, la nueva parametrización del sistema debe garantizar que los prestadores de servicios no puedan modificar ni alterar la información sobre la presencia física de los usuarios en el establecimiento, evitando así cualquier posible manipulación de los datos y asegurando que los certificados de aptitud en conducción o de asistencia a los cursos solo sean emitidos a quienes hayan cumplido con el proceso de validación de identidad de manera completa y correcta.

RESOLUCIÓN NÚMERO _____ DE _____

"Por medio de la cual se modifican las Resoluciones 5790 y 60832 de 2016 de la Superintendencia de Transporte y se introducen mejoras y medidas para fortalecer las capacidades de inspección, Vigilancia y Control a través de su Sistema de Control y Vigilancia para CEA, CIA y OTT"

Que, por otra parte, el control adecuado de los recursos y capacidades instaladas en los establecimientos en que se prestan los servicios de manera presencial es esencial para garantizar la correcta prestación del servicio y evitar que se reporten cifras erróneas o infladas que no corresponden con la verdadera capacidad operativa o de recursos disponibles, lo que afecta la transparencia y la eficiencia del sistema.

Que, por lo tanto, se propone una modificación del Sistema que permita, una vez detectada una inconsistencia entre la información reportada por el prestador de servicios y la evidencia obtenida durante las visitas de verificación, la activación de protocolos preventivos para evitar que los prestadores puedan reportar información con recursos con los que no cuentan, a través de una parametrización del sistema que permita verificar reportes sospechosos y frenar las irregularidades, evitando que las infracciones de la normatividad se prolonguen indefinidamente y garantizando una mayor transparencia en la prestación de los servicios.

Que, la realización de ajustes a nivel del desarrollo de software, de hardware y a nivel de infraestructura física deben ser garantizados por parte de los proveedores que deseen mantener la homologación para operar el Sistema de Control y Vigilancia, es decir para operar deben contar con una infraestructura técnica y financiera sólida.

Que, comoquiera que existen a la fecha dos homologados autorizados para operar el Sistema de Control y Vigilancia de Centros de Enseñanza Automovilística y Centros Integrales de Atención, y que dichas autorizaciones se encuentran vigentes, comoquiera que subsisten las condiciones jurídicas que dieron lugar a la expedición de los actos administrativos por medio de los cuales se les otorgó la homologación; la incorporación e implementación de las mejoras del Sistema previstas en la presente resolución constituye requisito para que los operadores homologados del Sistema puedan continuar fungiendo como tal.

Que, el operador homologado que voluntariamente opte por dar cumplimiento a las nuevas condiciones del Sistema de Control, con el propósito de continuar en la operación, se registrará por las reglas y condiciones definidas por la Superintendencia de Transporte en las Resoluciones 5790 y 60832 de 2016 que a través del presente acto se modifican, manteniéndose por lo tanto este como el marco jurídico aplicable a la relación surgida con anterioridad entre este y la Superintendencia.

RESOLUCIÓN NÚMERO _____ DE _____

"Por medio de la cual se modifican las Resoluciones 5790 y 60832 de 2016 de la Superintendencia de Transporte y se introducen mejoras y medidas para fortalecer las capacidades de inspección, Vigilancia y Control a través de su Sistema de Control y Vigilancia para CEA, CIA y OTT"

Que la implementación de las mejoras implica que se realicen inversiones económicas y se dediquen capacidades y esfuerzos importantes con el objeto de lograr el cumplimiento del fin perseguido, que no es otro que el fortalecimiento de capacidades de la Superintendencia de Transporte.

Que, asimismo, la apuesta por continuar la operación del Sistema del Control y Vigilancia para CEA, CIA y OTT implica garantizar el funcionamiento adecuado, la máxima disponibilidad según los acuerdos de niveles de servicio (ANS) definidos, el mantenimiento constante del Sistema y la adopción de mejoras cuando así lo determine la Superintendencia; por lo que resulta indispensable que los homologados aseguren la sostenibilidad del mismo en el tiempo.

Que, en línea con lo anterior, dados los cambios que sufrirá el Sistema, el actual operador homologado que con posterioridad a la expedición del presente acto administrativo manifieste su interés por continuar la operación, demuestre y se compruebe que haya implementado la totalidad de las mejoras introducidas, se entenderá autorizado para continuar operando el Sistema.

Que, en reuniones sostenidas con los actuales homologados del Sistema para CEA y CIA en los años 2024 y 2025, la Superintendencia de Transporte expuso las debilidades y vulnerabilidades del Sistema que eran objeto de mejora y recibió retroalimentación por parte de estos actores, quienes hicieron observaciones y plantearon su percepción sobre el estado actual del Sistema, aportaron a la discusión ideas de mejora y precisaron aspectos de carácter técnico que consideraban debían ser tenidos en cuenta para lograr el objetivo de fortalecimiento de la inspección, vigilancia y control por parte de la entidad.

Que, en relación con la operación de los Centros Integrales de Atención y Organismos de Tránsito y Transporte que dictan cursos a infractores, la Sección 4 de la Resolución 20223040045295 del 2022 "Por medio del cual se expide la Resolución Única Compilatoria en materia de Tránsito del Ministerio de Transporte", artículos 3.6.4.2.4. y siguientes, estableció las condiciones de su conectividad con el Registro Único Nacional de Tránsito para todos los efectos de registro de los cursos presenciales y fijó las reglas generales del curso, su agendamiento y registro de usuarios e instructores.

Que, por consiguiente, hasta tanto se defina e implemente un mecanismo de integración o de comunicación efectivo entre el RUNT y el Sistema de Control y Vigilancia, los Centros Integrales de Atención y los Organismos de Tránsito y Transporte deberán prestar sus servicios empleando el Sistema de Control y

RESOLUCIÓN NÚMERO _____ DE _____

"Por medio de la cual se modifican las Resoluciones 5790 y 60832 de 2016 de la Superintendencia de Transporte y se introducen mejoras y medidas para fortalecer las capacidades de inspección, Vigilancia y Control a través de su Sistema de Control y Vigilancia para CEA, CIA y OTT"

Vigilancia, respetando sus condiciones de uso y operación las cuales se basarán en lo descrito en el presente acto administrativo.

Que, sin perjuicio de que exista el mecanismo de integración o comunicación entre el SICOV y el RUNT, la Superintendencia de Transporte supervisará la actividad de los CEA, CIA y Organismos de Tránsito y Transporte a partir de la información registrada en ambas fuentes, especialmente a partir de los reportes que reciba por la operación de la primera.

Que el artículo 8 de la Ley 2251 de 2022, que adicionó el artículo 136A de la Ley 769 de 2002, estableció algunas condiciones mínimas de validez de los cursos sobre normas de tránsito impartidos en Centros Integrales de Atención y Organismos de Tránsito y creó una sanción aplicable a los infractores a los que se les compruebe haber hecho fraude para obtener la certificación de asistencia al curso.

Que, a través de las Resoluciones 355 de 2023 y 1164 de 2023, la Superintendencia de Transporte modificó los anexos técnicos del Sistema de Control y Vigilancia de los organismos de apoyo a las autoridades de tránsito y estableció medidas para su mejoramiento y fortalecimiento.

Que, en línea de lo dicho, con el ánimo de mejorar el SICOV para CEA, CIA y OTT, la Superintendencia modificará las Resoluciones 5790 y 60832 de 2016.

Que, de conformidad con lo dispuesto en el artículo 7 de la Ley 1340 de 2009, modificado por el artículo 146 de la Ley 1955 de 2019, la Superintendencia de Transporte solicitó a la Superintendencia de Industria y Comercio que rindiera concepto de abogacía de la competencia sobre la presente Resolución y mediante oficio radicado No. XXXXXX del XX de XXX de 202X, dicha entidad, recomendó:

Que, en cumplimiento de lo dispuesto en el numeral 8 del artículo 8 Ley 1437 de 2011, el proyecto de acto administrativo fue publicado del 12 de septiembre al 02 de octubre de 2025 en la página web de la Superintendencia de Transporte, con el fin de garantizar la participación de los interesados. Durante el periodo de publicación se recibieron comentarios y sugerencias por parte de la ciudadanía y los interesados, los cuales fueron evaluados en cuanto a su pertinencia y relevancia. Como resultado de dicho análisis, se acogieron aquellas observaciones que aportaban al mejoramiento del proyecto de acto administrativo, conciliando así el contenido inicialmente propuesto con los

RESOLUCIÓN NÚMERO _____ DE _____

"Por medio de la cual se modifican las Resoluciones 5790 y 60832 de 2016 de la Superintendencia de Transporte y se introducen mejoras y medidas para fortalecer las capacidades de inspección, Vigilancia y Control a través de su Sistema de Control y Vigilancia para CEA, CIA y OTT" aportes recibidos, lo que permitió fortalecer la versión final del acto administrativo.

En mérito de lo expuesto,

RESUELVE,

TÍTULO I

ACTUALIZACIÓN DE LAS CONDICIONES GENERALES DE FUNCIONAMIENTO Y CARACTERÍSTICAS DEL SICOV PARA CENTROS DE ENSEÑANZA AUTOMOVILÍSTICA, CENTROS INTEGRALES DE ATENCIÓN Y ORGANISMOS DE TRÁNSITO Y TRANSPORTE

Artículo 1. Modifíquese el artículo 1 de la Resolución 5790 de 2016, el cual quedará así:

Artículo 1. Objeto y ámbito de aplicación. La presente Resolución tiene por objeto definir y reglamentar las condiciones de funcionamiento, funciones mínimas y características técnicas, tecnológicas y operativas con que debe contar el Sistema de Control y Vigilancia de la Superintendencia de Transporte para inspeccionar, vigilar y controlar la actividad de los Centros de Enseñanza Automovilística (CEA), Centros Integrales de Atención (CIA) y Organismos de Tránsito y Transporte (OTT) que dictan cursos a infractores de las normas de tránsito registrados en el RUNT, y para asegurar que la expedición de los certificados a cargo de estos centros se realice en cumplimiento de lo dispuesto por las normas de carácter legal y reglamentarias vigentes.

Artículo 2. Modifíquese el artículo 2 de la Resolución 5790 de 2016, el cual quedará así:

Artículo 2. Definición, características y obligatoriedad del Sistema de Control y Vigilancia. El Sistema de Control y Vigilancia es una solución tecnológica de vigilancia intrusiva de la Superintendencia de Transporte, compuesta por infraestructura de hardware, software, despliegue de dispositivos y servicios tecnológicos, que permite a la Superintendencia de Transporte ejercer funciones de inspección, vigilancia y control sobre la operación de los organismos de apoyo a las autoridades de tránsito, incluidos los Centros de Enseñanza Automovilística, Centros Integrales de Atención y Organismos de Tránsito y Transporte.

RESOLUCIÓN NÚMERO _____ DE _____

"Por medio de la cual se modifican las Resoluciones 5790 y 60832 de 2016 de la Superintendencia de Transporte y se introducen mejoras y medidas para fortalecer las capacidades de inspección, Vigilancia y Control a través de su Sistema de Control y Vigilancia para CEA, CIA y OTT"

El Sistema de Control y Vigilancia implementado en los CEA, CIA y OTT permite a la Superintendencia verificar el cumplimiento de las condiciones y obligaciones exigidas en la ley y el reglamento para el registro y operación de estos organismos de apoyo a las autoridades de tránsito. Asimismo, constituye un mecanismo integral para la captación, registro, almacenamiento, procesamiento, análisis y reporte en tiempo real de la información generada durante las distintas etapas del proceso de prestación de servicios por parte de estos organismos.

A través de la implementación del SICOV, se establecen mecanismos de control precisos que buscan garantizar seguridad y legalidad en los trámites y que permiten recopilar información sobre la operación durante las diferentes etapas de la prestación del servicio por parte del vigilado; esto es, desde el momento de llegada y registro de un usuario hasta el de la expedición a su nombre de una certificación, ante el cumplimiento de una serie de obligaciones y responsabilidades.

El SICOV para CEA, CIA y OTT garantiza a la Superintendencia las siguientes funciones a nivel tecnológico:

- 1. Verificación continua del cumplimiento normativo:** Asegura la verificación continua de los requisitos de registro en el RUNT y de operación vigentes por parte de los CEA, CIA y OTT, los cuales constituyen estándares y condiciones mínimos exigidos de forma permanente. El Sistema es el medio principal del que dispone la Superintendencia para enterarse del cumplimiento de estas obligaciones.
- 2. Supervisión minuciosa de la operación:** Permite la supervisión detallada del desarrollo de las distintas etapas de la prestación del servicio por parte de los CEA, CIA y OTT, especialmente en lo que atañe a la validación de identidad de los usuarios, instructores y certificadores, y el reporte de información precisa sobre las distintas etapas de la evaluación.
- 3. Expedición segura de certificados:** Garantiza la emisión de certificados de aptitud y/o de asistencia a un curso, sujeta al cumplimiento de la totalidad de requisitos del servicio, y desde los lugares autorizados.
- 4. Gestión integral de la información:** Provee disponibilidad, correlación, trazabilidad, almacenamiento, procesamiento y cruce de información de la prestación del servicio, permitiendo la actualización permanente y segura de la información de operación, así como la obtención y procesamiento continuo de datos para corroborar el cumplimiento normativo.

RESOLUCIÓN NÚMERO _____ DE _____

"Por medio de la cual se modifican las Resoluciones 5790 y 60832 de 2016 de la Superintendencia de Transporte y se introducen mejoras y medidas para fortalecer las capacidades de inspección, Vigilancia y Control a través de su Sistema de Control y Vigilancia para CEA, CIA y OTT"

- 5. Detección y reacción oportuna ante incumplimientos:** Facilita la reacción oportuna y automatizada frente a incumplimientos de las reglas del sistema o la normatividad vigente. Esto incluye la generación de alertas tempranas y automáticas ante la evidencia de incumplimientos a las obligaciones o condiciones exigidas por la normativa vigente. Todo servicio que se preste o expida mientras una alerta se encuentre activa, será objeto de una "marcación de irregularidad" visible y auditable en el sistema, la cual será reportada en tiempo real a la Superintendencia de Transporte.
- 6. Seguridad en la transmisión y acceso a la información:** Asegura la seguridad en la transmisión de la información para evitar su manipulación, y garantiza el acceso de la Superintendencia al reporte de novedades especiales sobre la operación del Sistema.
- 7. Validación de identidad avanzada:** Implementa tecnologías más seguras para fortalecer la validación de identidad de los usuarios y el personal, contribuyendo a prevenir la suplantación de identidad y garantizar la integridad de los trámites.
- 8. Gestión y trazabilidad de personal de capacitación y certificación:** El SICOV deberá implementar mecanismos para gestionar de manera integral el ciclo de vida laboral del personal que participa en las capacitaciones y la expedición de certificados (instructores y personal administrativo). Esto incluye el registro de vinculaciones y desvinculaciones, y la correlación de esta información con otros proveedores homologados del SICOV para detectar y analizar patrones de alta rotación que puedan ser indicativos de anomalías o irregularidades. Se implementarán alertas automáticas para la Superintendencia de Transporte ante movimientos inusuales de personal entre CEA, CIA y OTT.
- 9. Automatización y parametrización de controles:** Permite la modificación y/o creación de nuevas funciones y la parametrización de algunas existentes, lo cual se posibilita principalmente con el desarrollo de software, la adquisición e implementación de dispositivos y tecnología de reconocimiento facial, y la parametrización del sistema para verificar reportes sospechosos y frenar irregularidades.
- 10. Gestión de sanciones y medidas cautelares de suspensión:** El SICOV deberá contar con un módulo para la gestión y seguimiento de las medidas de suspensión de la operación de los CEA, CIA y OTT, ordenadas por la Superintendencia de Transporte, tanto de manera preventiva, como por fallo sancionatorio. Dicho módulo deberá contar llevar control de la fecha de ejecución y cumplimiento de las medidas por parte del RUNT.

RESOLUCIÓN NÚMERO _____ DE _____

"Por medio de la cual se modifican las Resoluciones 5790 y 60832 de 2016 de la Superintendencia de Transporte y se introducen mejoras y medidas para fortalecer las capacidades de inspección, Vigilancia y Control a través de su Sistema de Control y Vigilancia para CEA, CIA y OTT"

Estas funciones deben garantizarse en la prestación de servicios presenciales y virtuales.

El Sistema de Control y Vigilancia, como herramienta de inspección, vigilancia y control, es de uso obligatorio por parte de los Centros de Enseñanza Automovilística, Centros Integrales de Atención y Organismos de Tránsito y Transporte que dicten cursos a infractores de las normas de tránsito conforme lo previsto en el artículo 136 del Código Nacional de Tránsito.

Artículo 3. Modifíquese el Artículo 3 de la Resolución No. 005790 de 2016, el cual quedará así:

Artículo 3. Operación del Sistema de Control y Vigilancia para CEA, CIA y OTT. La operación del Sistema de Control y Vigilancia en los Centros de Enseñanza Automovilística, Centros Integrales de Atención y Organismos de Tránsito y Transporte será garantizada por parte de los proveedores tecnológicos homologados por la Superintendencia de Transporte.

Los procesos relacionados con la expedición de los certificados de aptitud se gestionarán y monitorearán a través de un conjunto de componentes interdependientes que aseguren la disponibilidad, continuidad y funcionalidad de un software especializado de gestión y control. Este software contará con las funcionalidades descritas en el Anexo Técnico del SICOV para CEA, CIA y OTT, el cual hace parte integral del presente acto administrativo.

Parágrafo. La Superintendencia de Transporte, publicará y mantendrá actualizada la información del listado de proveedores tecnológicos homologados para operar el SICOV para CEA, CIA y OTT.

Artículo 4. Modifíquese el artículo 5 de la Resolución 5790 de 2016, el cual quedará así:

Artículo 5. Características generales del Sistema de Control y Vigilancia para los CEA, CIA y OTT. Además de los protocolos establecidos en los artículos anteriores, el Sistema de Control y Vigilancia adoptado en el presente acto administrativo, deberá contar con los componentes y características funcionales y no funcionales que se detallan en el Anexo Técnico de la presente Resolución, los cuales son esenciales para garantizar la operación, seguridad, gestión y calidad del servicio.

RESOLUCIÓN NÚMERO _____ DE _____

"Por medio de la cual se modifican las Resoluciones 5790 y 60832 de 2016 de la Superintendencia de Transporte y se introducen mejoras y medidas para fortalecer las capacidades de inspección, Vigilancia y Control a través de su Sistema de Control y Vigilancia para CEA, CIA y OTT"

Artículo 5. Modifíquese el Artículo 8° de la Resolución No. 005790 de 2016, el cual quedará así:

Artículo 8. Conectividad y acceso al Sistema de Control y Vigilancia. Los proveedores tecnológicos homologados por la Superintendencia de Transporte para operar el Sistema de Control y Vigilancia en CEA, CIA y OTT deberán garantizar a la Superintendencia de Transporte la conectividad y el acceso permanente, seguro y en tiempo real a información de la operación registrada en el Sistema, así como a los eventos y alertas de la operación, incluyendo los registros (logs) detallados de las transacciones, consultas y las operaciones de interoperabilidad de datos realizadas entre los distintos proveedores homologados del SICOV.

La Superintendencia definirá los criterios de auditoría, búsqueda y estructura de la información, así como los requisitos para la generación de informes, gráficos y otras herramientas de visualización necesarias para el ejercicio de sus funciones de inspección, vigilancia y control.

Las especificaciones técnicas detalladas de la información que debe poder consultar la entidad y las condiciones de conectividad se establecerán en el Anexo Técnico del SICOV para CEA, CIA y OTT y serán actualizados por parte del Comité Técnico Operativo para el Fortalecimiento del SICOV.

Parágrafo 1. El proveedor tecnológico deberá garantizar la alta disponibilidad en todas las capas y componentes del Sistema de Control y Vigilancia para asegurar la continuidad del servicio y la funcionalidad de IVC. Las especificaciones técnicas para el diseño redundante y resiliente de cada capa se establecerán en el Anexo Técnico de la presente Resolución.

Artículo 6. Modifíquese el Artículo 10 de la Resolución No. 5790 de 2016, el cual quedará así:

Artículo 10. Obligaciones del proveedor del Sistema de Control y Vigilancia. La empresa, entidad, o persona que sea o hubiese sido autorizada por la Superintendencia de Transporte para operar el Sistema de Control y Vigilancia, deberá cumplir con las condiciones y requisitos técnicos exigidos para la operación del sistema, según lo dispuesto en el Anexo Técnico y demás actos administrativos que lo complementen.

Tendrá el deber de permitirle acceso, consulta y de suministrarle a la Superintendencia de Transporte toda la información que esta le requiera sobre

RESOLUCIÓN NÚMERO _____ DE _____

"Por medio de la cual se modifican las Resoluciones 5790 y 60832 de 2016 de la Superintendencia de Transporte y se introducen mejoras y medidas para fortalecer las capacidades de inspección, Vigilancia y Control a través de su Sistema de Control y Vigilancia para CEA, CIA y OTT" la actividad de los organismos de apoyo al tránsito y organismos de tránsito y transporte, y también de su propia actividad como operador autorizado.

Adicionalmente, deberá cumplir con las obligaciones específicas a cargo de los proveedores homologados del SICOV que se definan en el Anexo Técnico del SICOV para CEA, CIA y OTT.

Artículo 7. Modifíquese el Artículo 12 de la Resolución No. 5790 de 2016, el cual quedará así:

Artículo 12. Garantía de niveles de servicio y auditorías. Los proveedores homologados del Sistema de Control y Vigilancia deberán suscribir Acuerdos de Niveles de Servicio (ANS) con los CEA, CIA y OTT a los que presten el servicio, de acuerdo con los parámetros establecidos en el Anexo técnico.

Los proveedores homologados se someterán a las auditorías que la Superintendencia determine, conforme a las directrices, periodicidad, alcance y metodología que defina, para verificar que los niveles de servicio, seguridad de la información y confidencialidad y el adecuado funcionamiento del sistema, se ajustan a los requisitos previstos en la presente Resolución, en su Anexo Técnico y en las demás normas que la modifiquen, adicionen o complementen.

Artículo 8. Adiciónese un nuevo artículo a la Resolución No. 5790 de 2016, el cual quedará así:

Artículo 17. Responsabilidad por la operación y la información del Sistema de Control y Vigilancia.

La información generada, captada, registrada, procesada, almacenada y transmitida a través del Sistema de Control y Vigilancia es de uso exclusivo de la Superintendencia de Transporte para el ejercicio de su función pública de inspección, vigilancia y control sobre los CEA, CIA y OTT. En cualquier caso, se deberá dar cumplimiento a lo estipulado en la Ley 1581 de 2012 y sus decretos reglamentarios.

En este marco, la operación del SICOV y la veracidad, integridad, confidencialidad y disponibilidad de dicha información generará responsabilidad para los diferentes actores de la cadena, así:

- 1. Responsabilidad de los proveedores homologados del SICOV:** Los proveedores homologados por la Superintendencia de Transporte para la

RESOLUCIÓN NÚMERO _____ DE _____

"Por medio de la cual se modifican las Resoluciones 5790 y 60832 de 2016 de la Superintendencia de Transporte y se introducen mejoras y medidas para fortalecer las capacidades de inspección, Vigilancia y Control a través de su Sistema de Control y Vigilancia para CEA, CIA y OTT"

operación del SICOV de CEA, CIA y OTT serán responsables del cabal y oportuno cumplimiento de las obligaciones de operación, seguridad, calidad, Acuerdos de Niveles de Servicio y fines del tratamiento de datos establecidos en esta Resolución y su Anexo Técnico.

En materia de información, la determinación de su finalidad, uso, control y disposición final recaen de manera exclusiva en la Superintendencia de Transporte, independientemente de quién opere o administre tecnológicamente el sistema. La facultad de los operadores homologados sobre dicha información se limita por lo tanto a su administración y custodia bajo las directrices y lineamientos de la Superintendencia, a título de encargados, garantizando su integridad, confidencialidad, disponibilidad y trazabilidad.

Está prohibido el uso de los datos e información personales registrados en el SICOV, como toda aquella relacionada con la operación del Sistema, para fines comerciales.

Los operadores velarán por la seguridad de la información, la prevención de fraudes y la atención oportuna de incidentes relacionados con su operación. Serán directamente responsables por las afectaciones que se generen por fallas o vulnerabilidades directamente imputables a su sistema o su operación.

La Superintendencia definirá el procedimiento aplicable para determinar responsabilidades asociadas al cumplimiento e incumplimiento de obligaciones de operación del SICOV y la adopción de medidas de respuesta en los casos en que se presenten estas eventualidades.

Adicionalmente, los proveedores homologados deberán dar cumplimiento al listado de obligaciones específicas respecto de la implementación y operación del SICOV, contenido en el Anexo Técnico del SICOV para CEA, CIA y OTT.

- 2. Responsabilidad de los CEA, CIA y OTT:** Los CEA, CIA y OTT, como usuarios obligatorios del SICOV y generadores primarios de la información, serán responsables por el uso adecuado del sistema en sus instalaciones, la veracidad de los datos registrados, la correcta aplicación de los protocolos operativos y el cumplimiento de todas las obligaciones legales y reglamentarias inherentes a la prestación de sus servicios. Su responsabilidad incluye la salvaguarda de los dispositivos y componentes

RESOLUCIÓN NÚMERO _____ DE _____

"Por medio de la cual se modifican las Resoluciones 5790 y 60832 de 2016 de la Superintendencia de Transporte y se introducen mejoras y medidas para fortalecer las capacidades de inspección, Vigilancia y Control a través de su Sistema de Control y Vigilancia para CEA, CIA y OTT" del SICOV ubicados en sus centros y la diligencia para evitar manipulaciones o daños al sistema que puedan afectar la calidad o integridad de la información.

Adicionalmente, los CEA, CIA y OTT deberán dar cumplimiento al listado de obligaciones específicas respecto de la implementación y uso del SICOV, contenido en el Anexo Técnico de esta Resolución.

- 3. Responsabilidad de personal del CEA, CIA y OTT.** Sin perjuicio de la responsabilidad que recae en los CEA, CIA y OTT, el personal que interactúa con el SICOV en estos organismos de apoyo será igualmente responsable del cumplimiento de todas las obligaciones legales y reglamentarias inherentes a la prestación de los servicios en cada uno prestados. Esa responsabilidad incluye el uso responsable del Sistema de Control y Vigilancia puesto a disposición para su uso, la salvaguarda de los dispositivos y componentes del Sistema ubicados en los centros y la diligencia para evitar manipulaciones o daños al sistema que puedan afectar la calidad o integridad de la información.

Cualquier omisión del cumplimiento de estas responsabilidades por parte del personal vinculado a los organismos de apoyo derivará en la remisión de la información con el detalle de las circunstancias de tiempo, modo y lugar de las conductas evidenciadas, a las autoridades competentes según lo dispuesto en el ordenamiento jurídico nacional y la índole de la conducta desplegada, sea penal, disciplinaria, fiscal y/o disciplinaria, y cualquier otra.

- 4. Responsabilidad de los aliados de recaudo.** Todos los aliados de recaudo involucrados en la operación del Sistema de Control y Vigilancia de los CEA, CIA y OTT son responsables de registrar, validar, llevar trazabilidad de los datos de cada operación de recaudo, y en general, de cumplir con lo establecido en el Anexo Técnico del SICOV para CEA, CIA y OTT.

- 5. Responsabilidad de los operadores tecnológicos de autenticación biométrica ante la Registraduría Nacional del Estado Civil.** Todos los operadores de autenticación biométrica involucrados en la operación del Sistema de Control y Vigilancia en los CEA, CIA, OTT son responsables de cumplir con las obligaciones establecidas por la RNEC para prestar el servicio de validación de identidad contra las bases de datos de identificación ciudadana (Biometría) y de atender las obligaciones

RESOLUCIÓN NÚMERO _____ DE _____

"Por medio de la cual se modifican las Resoluciones 5790 y 60832 de 2016 de la Superintendencia de Transporte y se introducen mejoras y medidas para fortalecer las capacidades de inspección, Vigilancia y Control a través de su Sistema de Control y Vigilancia para CEA, CIA y OTT" específicas de operación conforme a lo previsto en lo establecido en el Anexo Técnico del SICOV para CEA, CIA y OTT.

6. Responsabilidad por el tratamiento de datos personales: Todos los actores involucrados en la operación del SICOV son responsables del tratamiento de datos personales y sensibles conforme a la Ley 1581 de 2012 y sus normas reglamentarias, y deberán garantizar por tanto la protección de los derechos de los titulares de la información.

Parágrafo. No será atribuible responsabilidad al proveedor autorizado del SICOV por eventos que deriven de caso fortuito o fuerza mayor, debidamente demostrados y documentados, ni por fallas o vulnerabilidades atribuibles a la indisponibilidad o deficiencias de las plataformas tecnológicas de terceros con los que el SICOV deba interoperar, siempre que el proveedor haya agotado los protocolos de reporte y mitigación establecidos en el Anexo Técnico.

Artículo 9. Adiciónese un nuevo artículo a la Resolución No. 5790 de 2016, el cual quedará así:

Artículo 18. Procedimiento para la delimitación de responsabilidad operativa. La Superintendencia de Transporte, a través del Comité Técnico Operativo, expedirá un procedimiento para la delimitación de responsabilidades operativas por fallas, cuellos de botella, inconsistencias y en general afectaciones disponibilidad que se presenten con el SICOV, con el objetivo de establecer los criterios técnicos, procedimentales y de evidencia para diferenciar las fallas imputables a la operación del proveedor autorizado, de aquellas atribuibles a terceros y las provocadas por caso fortuito o circunstancias de fuerza mayor.

Este procedimiento detallará los aspectos necesarios para el ejercicio del derecho de defensa y contradicción de los homologados ante un presunto incumplimiento de las obligaciones de operación, incluyendo la oportunidad de presentar justificaciones técnicas y pruebas en su defensa, las cuales serán objeto de una evaluación técnica objetiva por parte de la Superintendencia de Transporte antes de la imposición de cualquier medida definitiva.

Artículo 10. Adiciónese un nuevo artículo a la Resolución No. 5790 de 2016, el cual quedará así:

Artículo 19. Continuidad y sostenibilidad del Sistema. La operación del Sistema de Control y Vigilancia para CEA, CIA y OTT implica garantizar su funcionamiento adecuado, la máxima disponibilidad según los acuerdos de

RESOLUCIÓN NÚMERO _____ DE _____

"Por medio de la cual se modifican las Resoluciones 5790 y 60832 de 2016 de la Superintendencia de Transporte y se introducen mejoras y medidas para fortalecer las capacidades de inspección, Vigilancia y Control a través de su Sistema de Control y Vigilancia para CEA, CIA y OTT"

niveles de servicio (ANS) definidos, el mantenimiento constante del Sistema, el cumplimiento estricto de todas las condiciones y funcionalidades descritas en el Anexo Técnico de esta Resolución y en la adopción de mejoras cuando así lo determine la Superintendencia, asegurando la sostenibilidad del mismo en el tiempo.

Artículo 11. Adiciónese un nuevo artículo a la Resolución No. 5790 de 2016, el cual quedará así:

Artículo 20. Incumplimiento de los requisitos de operación del Sistema.

El incumplimiento de las obligaciones establecidas para la operación del SICOV de CEA, CIA y OTT por parte de los proveedores tecnológicos homologados por la Superintendencia de Transporte, la reincidencia de incumplimientos o la omisión de subsanación oportuna de fallas presentadas, dará lugar al inicio de un procedimiento de asignación de las responsabilidades, podrá derivar en la adopción de las medidas administrativas que resulten necesarias, incluyendo la suspensión o cancelación de la homologación, sin perjuicio de las demás acciones a que haya lugar.

El procedimiento a seguir para determinar la responsabilidad por el incumplimiento o desconocimiento de requisitos de operación del SICOV será determinado por la Superintendencia de Transporte.

En caso de suspensión o pérdida de la homologación, el proveedor homologado deberá garantizar, bajo la supervisión de la Superintendencia de Transporte, la activación del Plan de salida y reversión tecnológica, para asegurar la transferencia inmediata, segura e íntegra de la totalidad de la información de la operación.

Para estos efectos, la Superintendencia de Transporte utilizará la evidencia disponible en el Módulo de Consulta alojado en el CPD Analítico.

TÍTULO II

ACTUALIZACIÓN DEL ANEXO TÉCNICO DEL SICOV PARA CENTROS DE ENSEÑANZA AUTOMOVILISTICA, CENTROS INTEGRALES DE ATENCIÓN Y ORGANISMOS DE TRÁNSITO Y TRANSPORTE

Artículo 12. Sustitúyase el Anexo Técnico del Sistema de Control y Vigilancia adoptado a través de la Resolución No. 60832 de 2016, el cual quedará así:

RESOLUCIÓN NÚMERO _____ DE _____

"Por medio de la cual se modifican las Resoluciones 5790 y 60832 de 2016 de la Superintendencia de Transporte y se introducen mejoras y medidas para fortalecer las capacidades de inspección, Vigilancia y Control a través de su Sistema de Control y Vigilancia para CEA, CIA y OTT"

ANEXO TÉCNICO DEL SISTEMA DE CONTROL Y VIGILANCIA DE CEA, CIA Y OTT

TÍTULO 1

INFORMACIÓN GENERAL DEL SISTEMA DE CONTROL Y VIGILANCIA

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 Enseñanza Automovilística, Centros Integrales de Atención y Organismos de Tránsito y Transporte. Su objetivo primordial es garantizar la implementación, operación y mejora continua de un SICOV modernizado, robusto y eficiente, fundamental para fortalecer las capacidades de inspección, vigilancia y control de la Superintendencia de Transporte y asegurar la transparencia, calidad y seguridad en la prestación de los servicios a cargo de estos organismos de apoyo de tránsito y la protección de los usuarios.

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 y Comité Técnico Operativo para el Fortalecimiento del SICOV: Establece las directrices para las auditorías al Sistema y a sus operadores homologados, así como la conformación y funciones del comité encargado de su mejora continua.

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 CEA, CIA y OTT frente al funcionamiento del Sistema.

RESOLUCIÓN NÚMERO _____ DE _____

"Por medio de la cual se modifican las Resoluciones 5790 y 60832 de 2016 de la Superintendencia de Transporte y se introducen mejoras y medidas para fortalecer las capacidades de inspección, Vigilancia y Control a través de su Sistema de Control y Vigilancia para CEA, CIA y OTT"

1.2. Objetivo del documento

El presente Anexo Técnico tiene como objetivo principal establecer los requerimientos técnicos y operativos que deben cumplir los sistemas, componentes y servicios que conforman el Sistema de Control y Vigilancia, así como las condiciones exigidas para el mantenimiento y actualización de la homologación de los actuales proveedores homologados. Se busca garantizar la implementación y operación de un SICOV modernizado, robusto y eficiente que permita a la Superintendencia de Transporte fortalecer sus capacidades de inspección, vigilancia y control preventivo y correctivo sobre los organismos de apoyo a las autoridades de tránsito, incluyendo los Centros de Enseñanza Automovilística (CEA), los Centros Integrales de Atención (CIA) y los Organismos de Tránsito y Transporte (OTT) que imparten cursos a infractores. Este mejoramiento es determinante para impactar positivamente el tránsito y transporte del país, en beneficio de la población en su conjunto.

1.3. El Sistema de Control y Vigilancia: definición y capacidades

El Sistema de Control y Vigilancia es una solución tecnológica de vigilancia intrusiva de la Superintendencia de Transporte, compuesta por infraestructura de hardware, software, despliegue de dispositivos y servicios tecnológicos, que permite a la Superintendencia de Transporte ejercer funciones de inspección, vigilancia y control sobre la operación de los organismos de apoyo a las autoridades de tránsito, incluidos los Centros de Enseñanza Automovilística, Centros Integrales de Atención y Organismos de Tránsito y Transporte.

El Sistema de Control y Vigilancia implementado en los CEA, CIA y OTT permite a la Superintendencia verificar el cumplimiento de las condiciones y obligaciones exigidas en la ley y el reglamento para el registro y operación de estos organismos de apoyo a las autoridades de tránsito. Asimismo, constituye un mecanismo integral para la captación, registro, almacenamiento, procesamiento, análisis y reporte en tiempo real de la información generada durante las distintas etapas del proceso de prestación de servicios por parte de estos organismos.

A través de la implementación del SICOV, se establecen mecanismos de control precisos que buscan garantizar seguridad y legalidad en los trámites y que permiten recopilar información sobre la operación durante las diferentes etapas de la prestación del servicio por parte del vigilado; esto es, desde el momento de llegada y registro de un usuario hasta el de la expedición a su nombre de una

RESOLUCIÓN NÚMERO _____ DE _____

"Por medio de la cual se modifican las Resoluciones 5790 y 60832 de 2016 de la Superintendencia de Transporte y se introducen mejoras y medidas para fortalecer las capacidades de inspección, Vigilancia y Control a través de su Sistema de Control y Vigilancia para CEA, CIA y OTT" certificación, ante el cumplimiento de una serie de obligaciones y responsabilidades.

El SICOV para CEA, CIA y OTT garantiza a la Superintendencia las siguientes funciones a nivel tecnológico:

- 1. Verificación continua del cumplimiento normativo:** Asegura la verificación continua del cumplimiento de los requisitos de registro en el RUNT y de operación vigentes por parte de los CEA, CIA y OTT, los cuales constituyen estándares y condiciones mínimos exigidos de forma permanente. El Sistema es el medio principal del que dispone la Superintendencia para enterarse del cumplimiento de estas obligaciones.
- 2. Supervisión minuciosa de la operación:** Permite la supervisión detallada del desarrollo de las distintas etapas de la prestación del servicio por parte de los CEA, CIA y OTT, especialmente en lo que atañe a la validación de identidad de los usuarios, instructores y certificadores, y el reporte de información precisa sobre las distintas etapas de la evaluación.
- 3. Expedición segura de certificados:** Garantiza la emisión de certificados de aptitud y/o de asistencia a un curso, sujeta al cumplimiento de la totalidad de requisitos del servicio, y desde los lugares autorizados.
- 4. Gestión integral de la información:** Provee disponibilidad, correlación, trazabilidad, almacenamiento, procesamiento y cruce de información de la prestación del servicio, permitiendo la actualización permanente y segura de la información de operación, así como la obtención y procesamiento continuo de datos para corroborar el cumplimiento normativo.
- 5. Detección y reacción oportuna ante incumplimientos:** Facilita la reacción oportuna y automatizada frente a incumplimientos de las reglas del sistema o la normatividad vigente. Esto incluye la generación de alertas tempranas y automáticas ante la evidencia de incumplimientos a las obligaciones o condiciones exigidas por la normativa vigente. Todo servicio que se preste o expida mientras una alerta se encuentre activa, será objeto de una "marcación de irregularidad" visible y auditable en el sistema, la cual será reportada en tiempo real a la Superintendencia de Transporte.
- 6. Seguridad en la transmisión y acceso a la información:** Asegura la seguridad en la transmisión de la información para evitar su manipulación, y garantiza el acceso de la Superintendencia al reporte de novedades especiales sobre la operación del Sistema.
- 7. Validación de identidad avanzada:** Implementa tecnologías más seguras para fortalecer la validación de identidad de los usuarios y el

RESOLUCIÓN NÚMERO _____ DE _____

"Por medio de la cual se modifican las Resoluciones 5790 y 60832 de 2016 de la Superintendencia de Transporte y se introducen mejoras y medidas para fortalecer las capacidades de inspección, Vigilancia y Control a través de su Sistema de Control y Vigilancia para CEA, CIA y OTT"

personal, contribuyendo a prevenir la suplantación de identidad y garantizar la integridad de los trámites.

8. Gestión y trazabilidad de personal de capacitación y certificación:

El SICOV deberá implementar mecanismos para gestionar de manera integral el ciclo de vida laboral del personal que participa en las capacitaciones y la expedición de certificados (instructores y personal administrativo). Esto incluye el registro de vinculaciones y desvinculaciones, y la correlación de esta información con otros proveedores homologados del SICOV para detectar y analizar patrones de alta rotación que puedan ser indicativos de anomalías o irregularidades. Se implementarán alertas automáticas para la Superintendencia de Transporte ante movimientos inusuales de personal entre CEA, CIA y OTT.

9. Automatización y parametrización de controles: Permite la modificación y/o creación de nuevas funciones y la parametrización de algunas existentes, lo cual se posibilita principalmente con el desarrollo de software, la adquisición e implementación de dispositivos y tecnología de reconocimiento facial, y la parametrización del sistema para verificar reportes sospechosos y frenar irregularidades.

10. Gestión de sanciones y medidas cautelares de suspensión: El SICOV deberá implementar un módulo para la gestión y seguimiento de las medidas de suspensión, tanto preventivas como definitivas, ordenadas por la Superintendencia de Transporte y ejecutadas por el RUNT. Este módulo tendrá la capacidad de recibir y registrar, a través de la interoperabilidad o el mecanismo de transmisión de información vigente entre la Superintendencia de Transporte y el RUNT, la información del momento (fecha y hora) exacto en que se haga efectiva la medida. El SICOV llevará un control automático y preciso del tiempo transcurrido desde su ejecución, garantizando así la plena trazabilidad de la medida. El sistema generará 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.

El SICOV, al garantizar servicios de capacitación de conductores y reeducación de infractores más rigurosos y legalmente impartidos, es fundamental para tener conductores más competentes, conscientes del riesgo y respetuosos de las normas, impactando positivamente la seguridad vial.

1.4. Marco normativo

RESOLUCIÓN NÚMERO _____ DE _____

"Por medio de la cual se modifican las Resoluciones 5790 y 60832 de 2016 de la Superintendencia de Transporte y se introducen mejoras y medidas para fortalecer las capacidades de inspección, Vigilancia y Control a través de su Sistema de Control y Vigilancia para CEA, CIA y OTT"

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

- La Constitución Política, en su artículo 2, 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.
- La Constitución Política en su artículo 24, que consagra el derecho a la libre circulación, sujeto a la reglamentación de las autoridades para garantía de la seguridad.
- La Constitución Política en su artículo 365 y la Ley 105 de 1993 artículo 2 literal b, 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), artículo 3, parágrafo 3, modificado por la Ley 1383 de 2010, que le 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. Asimismo, el parágrafo 1 del artículo 14 de esa misma norma le otorgó la competencia de vigilar y supervisar los centros de enseñanza automovilística.
- La Ley 1682 de 2013, que clasificó la actividad de los Centros de Enseñanza Automovilística como un servicio conexo al transporte.
- 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.
- La Ley 2283 de 2023, que estableció un plazo para la implementación del SICOV para los Centros Integrales de Atención.
- La Ley 2294 de 2023 (Plan Nacional de Desarrollo 2022-2026), artículo 180, Parágrafo 1, que determinó la obligación de vincular al SICOV a todas las entidades que dictan cursos para descuentos en sanciones por infracciones de tránsito.

RESOLUCIÓN NÚMERO _____ DE _____

"Por medio de la cual se modifican las Resoluciones 5790 y 60832 de 2016 de la Superintendencia de Transporte y se introducen mejoras y medidas para fortalecer las capacidades de inspección, Vigilancia y Control a través de su Sistema de Control y Vigilancia para CEA, CIA y OTT"

- 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, pues el SICOV es un subsistema o se integrará en este marco.
- Resolución 3245 de 2009 del Ministerio de Transporte, por la cual se reglamenta el Decreto 1500 de 2009 y se establecen requisitos para la habilitación de los Centros de Enseñanza Automovilística
- 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.

RESOLUCIÓN NÚMERO _____ DE _____

"Por medio de la cual se modifican las Resoluciones 5790 y 60832 de 2016 de la Superintendencia de Transporte y se introducen mejoras y medidas para fortalecer las capacidades de inspección, Vigilancia y Control a través de su Sistema de Control y Vigilancia para CEA, CIA y OTT"

1.5. Alcance del documento

El presente Anexo Técnico define los requerimientos a nivel técnico y operativo que deben cumplir los proveedores actualmente homologados para continuar operando el Sistema de Control y Vigilancia para los Centros de Enseñanza Automovilística, Centros Integrales de Atención y Organismos de Tránsito y Transporte.

1.6. Glosario de términos

Para efectos de la interpretación, implementación y cumplimiento de las obligaciones dispuestas en el presente Anexo Técnico y en la Resolución que lo adopta, se adoptan las siguientes definiciones:

Alerta temprana: Notificación automatizada generada por el SICOV en tiempo real, dirigida a los actores del sistema (Organismos de Apoyo y Superintendencia), que advierte sobre la inminencia de un incumplimiento normativo (ej. vencimiento de pólizas) o la detección de un comportamiento anómalo en la operación, con el fin de activar acciones preventivas o correctivas inmediatas.

Alta disponibilidad (High Availability - HA): Característica de diseño del SICOV que garantiza un nivel absoluto de continuidad operacional durante un período de tiempo determinado. Se logra mediante la eliminación de puntos únicos de fallo (redundancia) en servidores, almacenamiento y redes, asegurando que el servicio perdure incluso si uno de sus componentes falla.

Ancho de banda dedicado: Capacidad de transmisión de datos de un canal de comunicación que se asigna de manera exclusiva para el tráfico del SICOV, garantizando una velocidad constante y sin fluctuaciones derivadas del uso compartido con otros servicios externos.

API (Interfaz de Programación de Aplicaciones): Conjunto de protocolos y definiciones informáticas que permiten la integración e intercambio seguro de datos entre sistemas de información distintos (ej. entre el SICOV y el RUNT, o entre diferentes operadores del SICOV), garantizando la interoperabilidad sin intervención humana directa.

Autenticación biométrica: Proceso técnico mediante el cual se verifica la identidad de una persona comparando sus rasgos físicos (huella dactilar o rostro) contra un registro previamente almacenado y validado (template o base de datos)

RESOLUCIÓN NÚMERO _____ DE _____

"Por medio de la cual se modifican las Resoluciones 5790 y 60832 de 2016 de la Superintendencia de Transporte y se introducen mejoras y medidas para fortalecer las capacidades de inspección, Vigilancia y Control a través de su Sistema de Control y Vigilancia para CEA, CIA y OTT" de la RNEC), garantizando que quien recibe o presta el servicio es quien dice ser.

CAPD (Centro Alternativo de Procesamiento de Datos): Infraestructura tecnológica de respaldo (espejo), ubicada en una localización geográfica distinta al CPD principal, diseñada para asumir la operación del SICOV de manera automática o manual en caso de desastre, fallo crítico o indisponibilidad del centro principal, garantizando la continuidad del negocio (BCP).

CPD (Centro de Procesamiento de Datos): Instalación física segura y acondicionada (Datacenter) que aloja centralizadamente los sistemas informáticos críticos (servidores, almacenamiento, redes) del SICOV. Es el núcleo donde se procesa, almacena y custodia la información del Sistema bajo los estándares de certificación exigidos.

Disponibilidad: Medida del tiempo en que el SICOV y sus componentes están operativos, accesibles y funcionando correctamente para los usuarios. Se expresa en porcentaje y es la base para la medición de los Acuerdos de Niveles de Servicio (ANS).

Enrolamiento: Proceso inicial de registro de un usuario o funcionario en el SICOV, mediante el cual se capturan sus datos biográficos y biométricos, se valida su identidad contra la Registraduría Nacional del Estado Civil (RNEC) y se crea su perfil digital para permitirle interactuar con el Sistema.

Gestión de trazabilidad: Capacidad del Sistema para registrar, almacenar y recuperar el historial completo de cada transacción o evento ocurrido (quién, cuándo, dónde y qué hizo), permitiendo reconstruir cronológicamente la prestación del servicio para fines de auditoría, control y vigilancia.

Hash (Huella Digital de Datos): Algoritmo matemático que transforma cualquier bloque de datos en una cadena de caracteres de longitud fija. En el SICOV, se utiliza para asegurar la integridad de la información, garantizando que un registro (ej. un certificado o un log) no ha sido alterado después de su creación.

Infraestructura descentralizada (Edge): Conjunto de dispositivos de hardware (Workstations, servidores locales NAS, sensores, cámaras) ubicados físicamente en las sedes de los organismos de apoyo (CEA, CIA, OTT), encargados de realizar el procesamiento inmediato de datos (como la captura biométrica) antes de su transmisión al sistema central.

RESOLUCIÓN NÚMERO _____ DE _____

"Por medio de la cual se modifican las Resoluciones 5790 y 60832 de 2016 de la Superintendencia de Transporte y se introducen mejoras y medidas para fortalecer las capacidades de inspección, Vigilancia y Control a través de su Sistema de Control y Vigilancia para CEA, CIA y OTT"

Interoperabilidad: Capacidad del SICOV para intercambiar datos e información con otros sistemas (RUNT, SIMIT, otros Operadores SICOV) de manera precisa, efectiva y segura, permitiendo que la información fluya entre distintas plataformas sin restricciones de tecnología base.

Liveness Detection (Prueba de Vida): Tecnología de seguridad biométrica diseñada para determinar si la muestra biométrica (rostro o huella) está siendo presentada por una persona viva presente en el punto de captura, evitando fraudes mediante el uso de fotos, videos, máscaras o huellas sintéticas.

Logs (Registros de Auditoría): Archivos digitales inalterables generados automáticamente por el sistema, que registran eventos operativos, errores, accesos y transacciones. Constituyen la evidencia digital forense de la operación del SICOV.

Marcación de irregularidad: Estado lógico aplicado por el SICOV a un registro de servicio (clase, curso, certificado) cuando se detecta que fue prestado o expedido mientras existía una Alerta Temprana activa o un incumplimiento de requisitos críticos. Esta marca es indeleble y alerta a la Superintendencia para su revisión posterior.

NAS (Network Attached Storage): Dispositivo de almacenamiento conectado a la red que permite guardar y recuperar datos (como archivos de video, imágenes o logs) desde una ubicación centralizada para usuarios de red autorizados. En el SICOV, se utiliza primordialmente para el almacenamiento local seguro de evidencias en las sedes.

NOC (Network Operations Center): Centro de Operaciones de Red. Unidad especializada responsable de monitorear, supervisar y mantener la salud de la infraestructura de telecomunicaciones, servidores y servicios del SICOV, asegurando su disponibilidad y rendimiento las 24 horas del día.

Parametrización: Configuración de las reglas de negocio, variables y límites operativos dentro del código del software del SICOV (ej. horarios permitidos, capacidad máxima de alumnos, tiempos de clase), con el fin de traducir las normas legales y reglamentarias en restricciones técnicas de obligatorio cumplimiento por el sistema.

Redundancia: Estrategia de diseño que consiste en la duplicación de componentes críticos (fuentes de poder, enlaces de internet, discos duros, servidores) con la intención de aumentar la confiabilidad del sistema,

RESOLUCIÓN NÚMERO _____ DE _____

"Por medio de la cual se modifican las Resoluciones 5790 y 60832 de 2016 de la Superintendencia de Transporte y se introducen mejoras y medidas para fortalecer las capacidades de inspección, Vigilancia y Control a través de su Sistema de Control y Vigilancia para CEA, CIA y OTT" asegurando que si un componente falla, el duplicado asuma su función inmediatamente.

SAN (Storage Area Network): Red de área de almacenamiento de alta velocidad que conecta grupos de dispositivos de almacenamiento con servidores. En el SICOV, se utiliza en el CPD para garantizar que las bases de datos tengan un acceso a disco rápido, dedicado y seguro, separado de la red de área local.

SOC (Security Operations Center): Centro de Operaciones de Seguridad. Unidad centralizada que se ocupa de problemas de seguridad a nivel organizacional y técnico. Su función en el SICOV es monitorear, detectar, analizar y responder a incidentes de ciberseguridad (ataques, intrusiones, fraudes tecnológicos) en tiempo real.

Template biométrico: Representación matemática digital de las características únicas extraídas de una muestra biométrica (huella o rostro). Por razones de seguridad y privacidad, el SICOV almacena y compara templates, no necesariamente las imágenes originales en todos los procesos.

Tiempo de latencia: Tiempo que tarda un paquete de datos en transmitirse desde el punto de origen (ej. un CEA) hasta el servidor central del SICOV y regresar. Es un indicador crítico para la experiencia de usuario en procesos de validación en tiempo real.

TIER III: Nivel de certificación internacional para Centros de Datos (según estándar Uptime Institute o TIA-942) que garantiza una disponibilidad del 99.982%. Exige "Mantenimiento Concurrente", lo que significa que cualquier componente (servidor, aire acondicionado, electricidad) puede ser mantenido o reemplazado sin necesidad de apagar el sistema o interrumpir el servicio.

PIN: Código numérico o alfanumérico único, generado por el sistema de recaudo, que sirve como comprobante digital del pago de los servicios y habilita la prestación de los mismos en el SICOV.

VPN (Virtual Private Network): Tecnología de red que crea una conexión segura y cifrada (túnel) sobre una red menos segura (como Internet). El SICOV utiliza VPNs para asegurar que los datos transmitidos entre los organismos de apoyo y el CPD no puedan ser interceptados o leídos por terceros no autorizados.

WAF (Web Application Firewall): Cortafuegos específico para aplicaciones web que filtra, monitorea y bloquea el tráfico HTTP/HTTPS malicioso hacia y desde el

RESOLUCIÓN NÚMERO _____ DE _____

"Por medio de la cual se modifican las Resoluciones 5790 y 60832 de 2016 de la Superintendencia de Transporte y se introducen mejoras y medidas para fortalecer las capacidades de inspección, Vigilancia y Control a través de su Sistema de Control y Vigilancia para CEA, CIA y OTT"
SICOV, protegiendo el sistema contra ataques como inyección SQL, Cross-Site Scripting (XSS) y otros riesgos de seguridad web.

TÍTULO 2

REQUERIMIENTOS PARA LA PROVISIÓN DEL SICOV PARA CEA, CIA y OTT

2.1. PRESENTACIÓN DE SOLICITUD

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 CEA, CIA y OTT.

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 acápite 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 de 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 CEA, CIA y OTT.

En el *Anexo de formatos e instrucciones de presentación de la solicitud*, 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, además validar la capacidad jurídica y la facultad que debe tener una persona para adelantar cualquier tipo de proceso con una Entidad Estatal, a

RESOLUCIÓN NÚMERO _____ DE _____

"Por medio de la cual se modifican las Resoluciones 5790 y 60832 de 2016 de la Superintendencia de Transporte y se introducen mejoras y medidas para fortalecer las capacidades de inspección, Vigilancia y Control a través de su Sistema de Control y Vigilancia para CEA, CIA y OTT"

saber: (i) Obligarse a cumplir el objeto que motivó la creación e implementación del SICOV; y (ii) no estar incurso 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

RESOLUCIÓN NÚMERO _____ DE _____

"Por medio de la cual se modifican las Resoluciones 5790 y 60832 de 2016 de la Superintendencia de Transporte y se introducen mejoras y medidas para fortalecer las capacidades de inspección, Vigilancia y Control a través de su Sistema de Control y Vigilancia para CEA, CIA y OTT"

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.

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.).

De acuerdo con la ley, un certificado de esta naturaleza deberá contener el número, la fecha y la notaría de la escritura de constitución y de las reformas del contrato, el nombre de los representantes legales de la sociedad, las facultades conferidas en los estatutos y las limitaciones a dichas facultades, y en el evento que la sociedad tenga sucursales o agencias en otras ciudades del país, el documento y la fecha mediante el cual se decretó su apertura, si las mismas se encuentran en jurisdicción diferente a la Cámara.

2.2.2. Autorización del órgano social

RESOLUCIÓN NÚMERO _____ DE _____

"Por medio de la cual se modifican las Resoluciones 5790 y 60832 de 2016 de la Superintendencia de Transporte y se introducen mejoras y medidas para fortalecer las capacidades de inspección, Vigilancia y Control a través de su Sistema de Control y Vigilancia para CEA, CIA y OTT"

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 RUT tiene vigencia indefinida y solo debe ser actualizado cuando haya cambios en el lugar de residencia, número telefónico, correo electrónico, actividad económica, responsabilidades o algún otro atributo o característica que se encuentre dentro del registro del contribuyente, esto, de acuerdo con lo establecido en los artículos 555-1 y 658-3 numeral 3 del Estatuto Tributario y el artículo 1.6.1.2.7 de Decreto 1625 del 2016.

La CIIU (Sistema de Clasificación Industrial Internacional Uniforme) es una clasificación uniforme de todas las actividades económicas por procesos productivos. Su objetivo principal es proporcionar un conjunto de categorías de actividades que se pueda utilizar al elaborar estadísticas sobre ellas o escoger un segmento del mercado, permitiendo que las compañías puedan ser clasificadas por sectores o categorías comparables al estándar internacionalmente en diferentes tipos específicos de actividades económicas. Las actividades de los proveedores homologados del Sistema de Control y Vigilancia están enmarcadas en sectores del mercado que son resumidas a través de los códigos que reporten como su actividad de negocio ya sea principal o secundaria.

RESOLUCIÓN NÚMERO _____ DE _____

"Por medio de la cual se modifican las Resoluciones 5790 y 60832 de 2016 de la Superintendencia de Transporte y se introducen mejoras y medidas para fortalecer las capacidades de inspección, Vigilancia y Control a través de su Sistema de Control y Vigilancia para CEA, CIA y OTT"

El Sistema de Control y Vigilancia para los CEA, CIA y OTT requiere para su operación 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 homologados 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. Este es el único documento de identificación válido para todos los actos civiles, políticos, administrativos y judiciales según la Ley 39 de 1961. Se expide para los ciudadanos colombianos al cumplir los 18 años (mayoría de edad en Colombia). El organismo encargado para realizar las tareas de expedición de cédulas es la Registraduría Nacional del Estado Civil de Colombia. En el caso de los extranjeros, existe 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, de conformidad con la Ley 757 de 2002, modificada por la Ley 999 de 2005, reglamentada por el Decreto 4969 de 2009 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.

RESOLUCIÓN NÚMERO _____ DE _____

"Por medio de la cual se modifican las Resoluciones 5790 y 60832 de 2016 de la Superintendencia de Transporte y se introducen mejoras y medidas para fortalecer las capacidades de inspección, Vigilancia y Control a través de su Sistema de Control y Vigilancia para CEA, CIA y OTT"

En el Anexo de formatos e instrucciones de presentación de la solicitud, 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 Anexo de formatos e instrucciones de presentación de la solicitud desarrolla el 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. Cuando esta información no conste en el certificado de existencia o representación expedido por la Cámara de Comercio. 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%.

RESOLUCIÓN NÚMERO _____ DE _____

"Por medio de la cual se modifican las Resoluciones 5790 y 60832 de 2016 de la Superintendencia de Transporte y se introducen mejoras y medidas para fortalecer las capacidades de inspección, Vigilancia y Control a través de su Sistema de Control y Vigilancia para CEA, CIA y OTT"

En el Anexo de formatos e instrucciones de presentación de la solicitud, 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 técnica del operador homologado, adquiridos a través su participación previa en actividades iguales o similares a las previstas para la implementación del servicio del SICOV. Esta experiencia constituye un criterio fundamental para evaluar su idoneidad para satisfacer las necesidades descritas.

Los operadores homologados 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 homologado 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 de sus integrantes. Cuando la experiencia haya sido adquirida como parte de un contratista plural,

RESOLUCIÓN NÚMERO _____ DE _____

"Por medio de la cual se modifican las Resoluciones 5790 y 60832 de 2016 de la Superintendencia de Transporte y se introducen mejoras y medidas para fortalecer las capacidades de inspección, Vigilancia y Control a través de su Sistema de Control y Vigilancia para CEA, CIA y OTT" 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 Enseñanza Automovilística y los Centros Integrales de Atención.

La Superintendencia considera que el cumplimiento de los requisitos que se exponen a continuación permitirá verificar la idoneidad técnica de los operadores homologados del SICOV, asegurando una prestación del servicio eficaz y conforme a los estándares requeridos. 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 establecido en una moneda diferente al peso colombiano 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 homologados 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

RESOLUCIÓN NÚMERO _____ DE _____

"Por medio de la cual se modifican las Resoluciones 5790 y 60832 de 2016 de la Superintendencia de Transporte y se introducen mejoras y medidas para fortalecer las capacidades de inspección, Vigilancia y Control a través de su Sistema de Control y Vigilancia para CEA, CIA y OTT" 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 Anexo de formatos e instrucciones de presentación de la solicitud, se encuentra un modelo de presentación de la certificación de experiencia del homologado 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, ISO 27001 y Certificación SOC 2 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.

RESOLUCIÓN NÚMERO _____ DE _____

"Por medio de la cual se modifican las Resoluciones 5790 y 60832 de 2016 de la Superintendencia de Transporte y se introducen mejoras y medidas para fortalecer las capacidades de inspección, Vigilancia y Control a través de su Sistema de Control y Vigilancia para CEA, CIA y OTT"

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:

RESOLUCIÓN NÚMERO _____ DE _____

"Por medio de la cual se modifican las Resoluciones 5790 y 60832 de 2016 de la Superintendencia de Transporte y se introducen mejoras y medidas para fortalecer las capacidades de inspección, Vigilancia y Control a través de su Sistema de Control y Vigilancia para CEA, CIA y OTT"

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.

- 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 redundará 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 Infrastructure 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

RESOLUCIÓN NÚMERO _____ DE _____

"Por medio de la cual se modifican las Resoluciones 5790 y 60832 de 2016 de la Superintendencia de Transporte y se introducen mejoras y medidas para fortalecer las capacidades de inspección, Vigilancia y Control a través de su Sistema de Control y Vigilancia para CEA, CIA y OTT"

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.

En caso de Unión Temporal o Consorcio, **cada una** de las sociedades debe contar con la certificación en sistema de gestión de la calidad ISO 9001 e ISO 27001 y **al menos** una de los debe contar con alguna de las otras certificaciones aquí listadas. La certificación deberá estar vigente a la fecha de evaluación y será aplicable a los operadores homologados que constituyan dicha figura plural.

En el Anexo de formatos e instrucciones de presentación de la solicitud, 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 Anexo de formatos e instrucciones de presentación de la solicitud, se encuentra un modelo de certificado de cumplimiento de las exigencias mínimas

RESOLUCIÓN NÚMERO _____ DE _____

"Por medio de la cual se modifican las Resoluciones 5790 y 60832 de 2016 de la Superintendencia de Transporte y se introducen mejoras y medidas para fortalecer las capacidades de inspección, Vigilancia y Control a través de su Sistema de Control y Vigilancia para CEA, CIA y OTT" 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.

RESOLUCIÓN NÚMERO _____ DE _____

"Por medio de la cual se modifican las Resoluciones 5790 y 60832 de 2016 de la Superintendencia de Transporte y se introducen mejoras y medidas para fortalecer las capacidades de inspección, Vigilancia y Control a través de su Sistema de Control y Vigilancia para CEA, CIA y OTT"

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 de experiencia 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.

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

RESOLUCIÓN NÚMERO _____ DE _____

"Por medio de la cual se modifican las Resoluciones 5790 y 60832 de 2016 de la Superintendencia de Transporte y se introducen mejoras y medidas para fortalecer las capacidades de inspección, Vigilancia y Control a través de su Sistema de Control y Vigilancia para CEA, CIA y OTT"

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 o desarrollo de software y experiencia laboral certificada como arquitecto, líder, coordinador, desarrollador 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 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 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

RESOLUCIÓN NÚMERO _____ DE _____

"Por medio de la cual se modifican las Resoluciones 5790 y 60832 de 2016 de la Superintendencia de Transporte y se introducen mejoras y medidas para fortalecer las capacidades de inspección, Vigilancia y Control a través de su Sistema de Control y Vigilancia para CEA, CIA y OTT" (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 Infrastructure 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 implementación 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 horarios 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 CEA, CIA y OTT 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.

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:

RESOLUCIÓN NÚMERO _____ DE _____

"Por medio de la cual se modifican las Resoluciones 5790 y 60832 de 2016 de la Superintendencia de Transporte y se introducen mejoras y medidas para fortalecer las capacidades de inspección, Vigilancia y Control a través de su Sistema de Control y Vigilancia para CEA, CIA y OTT"

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:

- Encriptación de los datos que viajan a través de la red.
- Actualización en línea de lo recaudado.
- Debe estar constituido un esquema de replicación en línea de los datos.
- Deberá emitir o generar comprobantes de recaudo, con posibilidades de emitir las copias necesarias.
- Contar con redundancia de un CPD principal y un CAPD, que garantice la continuidad del servicio.
- Deberá contar con dispositivos de seguridad perimetral en la red.
- Disponer de un canal de atención inmediata para los usuarios y/o clientes.
- Deberá tener restricción en la manipulación técnica de los equipos de cómputo o terminales en los puntos de recaudo.
- 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, tipo y número de identidad del usuario del servicio. Con estos últimos datos deberá generar un algoritmo hash cuyo resultado debe ser

RESOLUCIÓN NÚMERO _____ DE _____

"Por medio de la cual se modifican las Resoluciones 5790 y 60832 de 2016 de la Superintendencia de Transporte y se introducen mejoras y medidas para fortalecer las capacidades de inspección, Vigilancia y Control a través de su Sistema de Control y Vigilancia para CEA, CIA y OTT"

un número que permita realizar verificaciones de información y prevenir cualquier intento de violación o cambio de información.

- Debe 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.
 - Deberá presentar procedimiento que evite que traten de falsificar comprobantes de recaudo.
 - Deberá suministrar al operador del SICOV, la información requerida de la trazabilidad de cada operación de recaudo.
 - 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.
4. 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 actual proveedor SICOV preste el servicio, independientemente del municipio del país en el que se encuentren.

La atención debe ser garantizada a través de los siguientes canales o medios de atención: línea telefónica, Whatsapp y correo electrónico.

5. 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.
6. 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.
7. 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 artículo 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.
8. 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.

RESOLUCIÓN NÚMERO _____ DE _____

"Por medio de la cual se modifican las Resoluciones 5790 y 60832 de 2016 de la Superintendencia de Transporte y se introducen mejoras y medidas para fortalecer las capacidades de inspección, Vigilancia y Control a través de su Sistema de Control y Vigilancia para CEA, CIA y OTT"

9. Constituir una póliza de cumplimiento a favor de cada CEA, CIA, OTT a los que preste el servicio y del homologado, por el buen manejo del dinero recaudado.

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 por esta conforme a lo dispuesto en la Resolución 27145 de 2023 y las normas que la sustituyan, adicionen o modifiquen.

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. 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 cumplir de

RESOLUCIÓN NÚMERO _____ DE _____

"Por medio de la cual se modifican las Resoluciones 5790 y 60832 de 2016 de la Superintendencia de Transporte y se introducen mejoras y medidas para fortalecer las capacidades de inspección, Vigilancia y Control a través de su Sistema de Control y Vigilancia para CEA, CIA y OTT" manera oportuna y satisfactoria con las obligaciones a cargo de los proveedores homologados del SICOV.

La capacidad financiera exigida deberá ser adecuada y proporcional en relación con la naturaleza, el valor 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 homologado 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 operador 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 con el 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:

RESOLUCIÓN NÚMERO _____ DE _____

"Por medio de la cual se modifican las Resoluciones 5790 y 60832 de 2016 de la Superintendencia de Transporte y se introducen mejoras y medidas para fortalecer las capacidades de inspección, Vigilancia y Control a través de su Sistema de Control y Vigilancia para CEA, CIA y OTT"

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 homologado para el esclarecimiento de la información, tales como: estados financieros de años anteriores, anexos

RESOLUCIÓN NÚMERO _____ DE _____

"Por medio de la cual se modifican las Resoluciones 5790 y 60832 de 2016 de la Superintendencia de Transporte y se introducen mejoras y medidas para fortalecer las capacidades de inspección, Vigilancia y Control a través de su Sistema de Control y Vigilancia para CEA, CIA y OTT"

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 a la presentación de la solicitud.

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

RESOLUCIÓN NÚMERO _____ DE _____

"Por medio de la cual se modifican las Resoluciones 5790 y 60832 de 2016 de la Superintendencia de Transporte y se introducen mejoras y medidas para fortalecer las capacidades de inspección, Vigilancia y Control a través de su Sistema de Control y Vigilancia para CEA, CIA y OTT"

operador participe de una Unión Temporal o Consorcio, para los efectos de este Anexo, deberán 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 documento establece los requerimientos técnicos mínimos que deben ser cumplidos por parte de los operadores homologados del Sistema de Control y Vigilancia de la Superintendencia de Transporte para Centros de Enseñanza Automovilística, Centros Integrales de Atención y Organismos de Tránsito y Transporte que dicten cursos a infractores de las normas de tránsito, 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 5790 de 2016, 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 caso que alguna de estas normas técnicas internacionales quede en desuso, se debe utilizar cualquier otra norma que la reemplace.

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.

RESOLUCIÓN NÚMERO _____ DE _____

"Por medio de la cual se modifican las Resoluciones 5790 y 60832 de 2016 de la Superintendencia de Transporte y se introducen mejoras y medidas para fortalecer las capacidades de inspección, Vigilancia y Control a través de su Sistema de Control y Vigilancia para CEA, CIA y OTT"

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).

Este acápite desarrollará reglas básicas de operación de la Mesa de Ayuda.

- 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 Enseñanza Automovilística, los Centros Integrales de Atención, Organismos de Tránsito y Transporte y la Superintendencia de Transporte.

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 clases, gestión de recursos, certificaciones, etc.), pueda fluir en tiempo

RESOLUCIÓN NÚMERO _____ DE _____

"Por medio de la cual se modifican las Resoluciones 5790 y 60832 de 2016 de la Superintendencia de Transporte y se introducen mejoras y medidas para fortalecer las capacidades de inspección, Vigilancia y Control a través de su Sistema de Control y Vigilancia para CEA, CIA y OTT"

real desde los organismos de apoyo hacia los servidores centrales del SICOV, así como para la comunicación con sistemas externos de terceros involucrados con la operación, así como el RUNT, SIMIT, proveedores o entidades externas, entre otros. Permite la conectividad 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 Enseñanza Automovilística, Centros Integrales de Atención y Organismos de Tránsito y Transporte que dicten cursos a infractores de las normas de tránsito, 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 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 le debe garantizar a la Superintendencia 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, inspección, vigilancia y control 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 (CPD-A), conformado por un Centro de Procesamiento de Datos Analítico y un Centro Alternativo de Procesamiento de Datos Analítico (CPD Analítico), los cuales consolidarán en un único repositorio nacional los datos generados por los organismos de apoyo (CDA, CEA, CRC) a través del SICOV.

RESOLUCIÓN NÚMERO _____ DE _____

"Por medio de la cual se modifican las Resoluciones 5790 y 60832 de 2016 de la Superintendencia de Transporte y se introducen mejoras y medidas para fortalecer las capacidades de inspección, Vigilancia y Control a través de su Sistema de Control y Vigilancia para CEA, CIA y OTT"

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 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 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 compañía, 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 CAPD, 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 identificando

RESOLUCIÓN NÚMERO _____ DE _____

"Por medio de la cual se modifican las Resoluciones 5790 y 60832 de 2016 de la Superintendencia de Transporte y se introducen mejoras y medidas para fortalecer las capacidades de inspección, Vigilancia y Control a través de su Sistema de Control y Vigilancia para CEA, CIA y OTT"

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.

2.5.1.1. Plan de recuperación de desastres del Operador, indicando los objetivos de recuperación.

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 sitios seguros, 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.

RESOLUCIÓN NÚMERO _____ DE _____

"Por medio de la cual se modifican las Resoluciones 5790 y 60832 de 2016 de la Superintendencia de Transporte y se introducen mejoras y medidas para fortalecer las capacidades de inspección, Vigilancia y Control a través de su Sistema de Control y Vigilancia para CEA, CIA y OTT"

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.

RESOLUCIÓN NÚMERO _____ DE _____

"Por medio de la cual se modifican las Resoluciones 5790 y 60832 de 2016 de la Superintendencia de Transporte y se introducen mejoras y medidas para fortalecer las capacidades de inspección, Vigilancia y Control a través de su Sistema de Control y Vigilancia para CEA, CIA y OTT"

8. **Provisión de hardware:** El hardware necesario para el funcionamiento del Sistema de Control y Vigilancia en las sedes de los CEA, CIA y OTT, así como aquellos componentes que deban ser instalados en los vehículos de enseñanza, 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 organismos de apoyo y en sus vehículos de enseñanza.

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 cero punto de fallo único y la recuperación automática del servicio 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.

RESOLUCIÓN NÚMERO _____ DE _____

"Por medio de la cual se modifican las Resoluciones 5790 y 60832 de 2016 de la Superintendencia de Transporte y se introducen mejoras y medidas para fortalecer las capacidades de inspección, Vigilancia y Control a través de su Sistema de Control y Vigilancia para CEA, CIA y OTT"

El DRP deberá ser 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, su rol esencial para la función de inspección, vigilancia y control de la Superintendencia de Transporte, 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 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

RESOLUCIÓN NÚMERO _____ DE _____

"Por medio de la cual se modifican las Resoluciones 5790 y 60832 de 2016 de la Superintendencia de Transporte y se introducen mejoras y medidas para fortalecer las capacidades de inspección, Vigilancia y Control a través de su Sistema de Control y Vigilancia para CEA, CIA y OTT"

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 crítica 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 alternativo) 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 CEA, CIA y OTT, cuyas características se detallan a continuación, deben ser de uso exclusivo.

2.5.5.3. Recursos de cómputo y procesamiento

RESOLUCIÓN NÚMERO _____ DE _____

"Por medio de la cual se modifican las Resoluciones 5790 y 60832 de 2016 de la Superintendencia de Transporte y se introducen mejoras y medidas para fortalecer las capacidades de inspección, Vigilancia y Control a través de su Sistema de Control y Vigilancia para CEA, CIA y OTT"

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.

RESOLUCIÓN NÚMERO _____ DE _____

"Por medio de la cual se modifican las Resoluciones 5790 y 60832 de 2016 de la Superintendencia de Transporte y se introducen mejoras y medidas para fortalecer las capacidades de inspección, Vigilancia y Control a través de su Sistema de Control y Vigilancia para CEA, CIA y OTT"

- **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/asíncrona 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.

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.

RESOLUCIÓN NÚMERO _____ DE _____

"Por medio de la cual se modifican las Resoluciones 5790 y 60832 de 2016 de la Superintendencia de Transporte y se introducen mejoras y medidas para fortalecer las capacidades de inspección, Vigilancia y Control a través de su Sistema de Control y Vigilancia para CEA, CIA y OTT"

- **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 1.3 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

RESOLUCIÓN NÚMERO _____ DE _____

"Por medio de la cual se modifican las Resoluciones 5790 y 60832 de 2016 de la Superintendencia de Transporte y se introducen mejoras y medidas para fortalecer las capacidades de inspección, Vigilancia y Control a través de su Sistema de Control y Vigilancia para CEA, CIA y OTT"

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:** El CPD principal deberá estar ubicado en territorio nacional, y el CPAD redundante podrá estar ubicado 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 pararrayos, 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.

RESOLUCIÓN NÚMERO _____ DE _____

"Por medio de la cual se modifican las Resoluciones 5790 y 60832 de 2016 de la Superintendencia de Transporte y se introducen mejoras y medidas para fortalecer las capacidades de inspección, Vigilancia y Control a través de su Sistema de Control y Vigilancia para CEA, CIA y OTT"

- **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 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 por tipo de organismo de apoyo (uno para CEA, otro para CIA y OTT) que permita la interacción entre la infraestructura central del SICOV y estos organismos de apoyo.

Para la conectividad con los CEA, 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 2000 MB simétricas o dedicado 1:1, con conectividad redundante provista por diferentes proveedores de servicio de internet (ISP).

RESOLUCIÓN NÚMERO _____ DE _____

"Por medio de la cual se modifican las Resoluciones 5790 y 60832 de 2016 de la Superintendencia de Transporte y se introducen mejoras y medidas para fortalecer las capacidades de inspección, Vigilancia y Control a través de su Sistema de Control y Vigilancia para CEA, CIA y OTT"

Para la conectividad con los CIA y OTT, 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 500 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 CEA, CIA, OTT 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 CEA, CIA, y OTT deberá contar con:

Canal dedicado: 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.

La alta disponibilidad deberá garantizarse proveedor 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 CIA 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.

Conexión al NAP Colombia: 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.

RESOLUCIÓN NÚMERO _____ DE _____

"Por medio de la cual se modifican las Resoluciones 5790 y 60832 de 2016 de la Superintendencia de Transporte y se introducen mejoras y medidas para fortalecer las capacidades de inspección, Vigilancia y Control a través de su Sistema de Control y Vigilancia para CEA, CIA y OTT"

Dirección IP pública fija: 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 organismos de apoyo 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 CEA, CIA y OTT será supervisado por la Superintendencia de Transporte a través del SICOV.

El proveedor de comunicaciones contratado por cada OAT 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.

RESOLUCIÓN NÚMERO _____ DE _____

"Por medio de la cual se modifican las Resoluciones 5790 y 60832 de 2016 de la Superintendencia de Transporte y se introducen mejoras y medidas para fortalecer las capacidades de inspección, Vigilancia y Control a través de su Sistema de Control y Vigilancia para CEA, CIA y OTT"

- 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 pérdida 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 CIA hasta el NAP.

Soporte y mantenimiento

El proveedor de comunicaciones contratado por cada OAT deberá operar y mantener la solución instalada sin que el CIA 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:**
 - o Nivel 3 Administrable
 - o 24 puertos Fast Ethernet, velocidad 10/100/1000 Mbps

RESOLUCIÓN NÚMERO _____ DE _____

"Por medio de la cual se modifican las Resoluciones 5790 y 60832 de 2016 de la Superintendencia de Transporte y se introducen mejoras y medidas para fortalecer las capacidades de inspección, Vigilancia y Control a través de su Sistema de Control y Vigilancia para CEA, CIA y OTT"

- 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

RESOLUCIÓN NÚMERO _____ DE _____

"Por medio de la cual se modifican las Resoluciones 5790 y 60832 de 2016 de la Superintendencia de Transporte y se introducen mejoras y medidas para fortalecer las capacidades de inspección, Vigilancia y Control a través de su Sistema de Control y Vigilancia para CEA, CIA y OTT"

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 del Sistema de Control y Vigilancia para CEA, CIA y OTT

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 CEA, CIA y OTT, permita capturar, procesar, gestionar y analizar la información, y llevar trazabilidad integral de su operación, en cada una de las etapas los servicios por estos ofertados, 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.

2.5.8.1. Funcionalidades tecnológicas transversales del software del

RESOLUCIÓN NÚMERO _____ DE _____

"Por medio de la cual se modifican las Resoluciones 5790 y 60832 de 2016 de la Superintendencia de Transporte y se introducen mejoras y medidas para fortalecer las capacidades de inspección, Vigilancia y Control a través de su Sistema de Control y Vigilancia para CEA, CIA y OTT"

SICOV para los CEA, CIA y OTT:

Introducción

El presente capítulo describe las funcionalidades y capacidades tecnológicas generales que el Sistema de Control y Vigilancia deberá proveer de manera transversal para su operación con todos los Centros de Enseñanza Automovilística, los Centros Integrales de Atención y los Organismos de Tránsito y Transporte que imparten cursos a infractores.

La descripción de cada función se realiza en términos generales y comunes. Las particularidades, excepciones, o reglas de negocio específicas que apliquen de manera diferenciada a cada tipo de organismo de apoyo, en razón de la naturaleza y características de sus servicios, se detallarán en los capítulos subsiguientes.

2.5.8.1.1. Gestión del registro de información de los organismos de apoyo al tránsito 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 Organismo de Apoyo al Tránsito autorizado para operar.

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 la sede habilitada; números de teléfono de contacto actualizados; y direcciones de correo electrónico institucional designadas para notificaciones oficiales (deberá ser el mismo reportado al VIGIA).

RESOLUCIÓN NÚMERO _____ DE _____

"Por medio de la cual se modifican las Resoluciones 5790 y 60832 de 2016 de la Superintendencia de Transporte y se introducen mejoras y medidas para fortalecer las capacidades de inspección, Vigilancia y Control a través de su Sistema de Control y Vigilancia para CEA, CIA y OTT"

d) **Representación legal:** Información completa y vigente del representante legal principal y de los suplentes registrados (si los hubiere), incluyendo nombres y apellidos completos, tipo y número de documento de identidad.

e) **Detalles operativos y de habilitación:** Horarios de atención al público para cada sede; y la información detallada (número y fecha de expedición) del acto administrativo de habilitación o autorización expedido por el Ministerio de Transporte 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 operador del SICOV procederá con el registro y la gestión centralizada del número único de IDClient asignado por la Registraduría Nacional del Estado Civil a cada organismo de apoyo. Este IDClient es indispensable para que en el organismo de apoyo se puedan 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.

- i. El registro de toda la información sobre el IDClient de cada CEA, CIA y OTT en el SICOV, deberá estar respaldado por la constancia de asignación expedida por la RNEC, a través de correo electrónico o el medio del que disponga esa entidad.
- ii. La parametrización del Sistema validará que ningún CEA, CIA y OTT 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.
- iii. El proveedor del SICOV, a través de su operador biométrico, debe garantizar la prestación del servicio mientras el IDClient del CEA, CIA u OTT se mantenga activo.
- iv. 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 CEA, CIA y OTT, 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 CEA, CIA y OTT con el operador del SICOV con el que tenga vínculo.

RESOLUCIÓN NÚMERO _____ DE _____

"Por medio de la cual se modifican las Resoluciones 5790 y 60832 de 2016 de la Superintendencia de Transporte y se introducen mejoras y medidas para fortalecer las capacidades de inspección, Vigilancia y Control a través de su Sistema de Control y Vigilancia para CEA, CIA y OTT"

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) **Información adicional requerida:** Cualquier otro 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.

h) **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 aspirantes, instructores y certificadores, al inicio y al final de cada clase, curso, de cada examen cuando aplique, y del momento de certificación.
- Los resultados de las pruebas de los exámenes obtenidos.

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

Los CEA, CIA y OTT 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.

2.5.8.1.2. 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 alumnos (CEA) e infractores de normas de tránsito (CIA y OTT), 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 organismo de apoyo, el sistema realizará el enrolamiento mediante la captura de datos biográficos, la digitalización

RESOLUCIÓN NÚMERO _____ DE _____

"Por medio de la cual se modifican las Resoluciones 5790 y 60832 de 2016 de la Superintendencia de Transporte y se introducen mejoras y medidas para fortalecer las capacidades de inspección, Vigilancia y Control a través de su Sistema de Control y Vigilancia para CEA, CIA y OTT"

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 organismos de apoyo (CEA, CIA y OTT) 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 (template) 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 a la primera sesión académica o al curso, 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.

2.5.8.1.3. Gestión y registro de pagos de servicios de capacitación en conducción.

El Sistema de Control y Vigilancia deberá facilitar y garantizar el registro seguro del pago de la tarifa correspondiente a la prestación del servicio de capacitación en los CEA y de los cursos en CIA y OTT cuando estos se dicten de manera virtual. Este proceso 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.

RESOLUCIÓN NÚMERO _____ DE _____

"Por medio de la cual se modifican las Resoluciones 5790 y 60832 de 2016 de la Superintendencia de Transporte y se introducen mejoras y medidas para fortalecer las capacidades de inspección, Vigilancia y Control a través de su Sistema de Control y Vigilancia para CEA, CIA y OTT"

a) Condicionamiento para el pago: 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 prestado por el organismo de apoyo al tránsito, más los valores de terceros. De la constancia de pago efectivo deberá quedar trazabilidad en los registros (logs) del SICOV.

La habilitación de la generación del PIN estará condicionada a la verificación previa y automática por parte del SICOV del cumplimiento de los prerequisites que apliquen para cada tipo de servicio, según se especifica en los capítulos de funcionalidades particulares de este Anexo.

b) 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 del mecanismo de interoperabilidad o integración que se desarrolle, la información precisa del pago recibido hecho por parte del usuario del servicio o de quien lo realice en nombre suyo, discriminando los valores dispersados 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 o representante de la persona jurídica que realizó el 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.

c) Facilidades de pago: El SICOV deberá registrar la información detallada de la transacción de pago y la entidad que procesó el recaudo.

d) 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 un (1) día, correspondiente a la misma fecha de su generación. Finalizado el día de su generación, si el PIN no ha sido consumido para la prestación del servicio de capacitación, 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 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, y de acuerdo con el procedimiento que se defina y acepte el usuario al momento de adquirir el PIN.

RESOLUCIÓN NÚMERO _____ DE _____

"Por medio de la cual se modifican las Resoluciones 5790 y 60832 de 2016 de la Superintendencia de Transporte y se introducen mejoras y medidas para fortalecer las capacidades de inspección, Vigilancia y Control a través de su Sistema de Control y Vigilancia para CEA, CIA y OTT"

e) 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.

2.5.8.1.4. 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, instructores y personal certificador) que interactúen con el Sistema. Este registro, que se realizará al momento del enrolamiento inicial, requerirá, 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.

RESOLUCIÓN NÚMERO _____ DE _____

"Por medio de la cual se modifican las Resoluciones 5790 y 60832 de 2016 de la Superintendencia de Transporte y se introducen mejoras y medidas para fortalecer las capacidades de inspección, Vigilancia y Control a través de su Sistema de Control y Vigilancia para CEA, CIA y OTT"

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) descritas en este literal 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 que se desarrolla más adelante.

RESOLUCIÓN NÚMERO _____ DE _____

"Por medio de la cual se modifican las Resoluciones 5790 y 60832 de 2016 de la Superintendencia de Transporte y se introducen mejoras y medidas para fortalecer las capacidades de inspección, Vigilancia y Control a través de su Sistema de Control y Vigilancia para CEA, CIA y OTT"

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.
- **Consulta y reutilización en la red:** Cuando un organismo de apoyo (CEA, CIA, OTT) realice el escaneo del documento de identidad de un usuario, el SICOV consultará automáticamente al Subsistema ABIS central.

Si el usuario ya existe en el ABIS, el sistema confirmará la identidad haciendo una validación biométrica con la tecnología de reconocimiento facial y, de resultar exitosa, habilitará el uso del template existente para realizar todos los cotejos con reconocimiento facial posteriores (selfie vs template) requeridos durante el nuevo servicio.

En los casos que la validación de identidad con reconocimiento facial contra el ABIS sea exitosa no se requerirá un nuevo enrolamiento biométrico del usuario, ni volver a consultar a la RNEC (salvo criterio de actualización periódica), pero sí la validación del documento físico.

En los casos que la validación de identidad con reconocimiento facial contra el ABIS no sea exitosa, se realizará todo el procedimiento de enrolamiento y registro de datos aquí y validación contra la RNEC descrito y, si este resulta exitoso, se actualizará la información del ABIS.

Si el usuario no existe en el ABIS, se procederá con el flujo completo de enrolamiento, registro de datos y validación contra la RNEC y creación del nuevo template en el ABIS.

c) **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

RESOLUCIÓN NÚMERO _____ DE _____

"Por medio de la cual se modifican las Resoluciones 5790 y 60832 de 2016 de la Superintendencia de Transporte y se introducen mejoras y medidas para fortalecer las capacidades de inspección, Vigilancia y Control a través de su Sistema de Control y Vigilancia para CEA, CIA y OTT"

tratamiento de datos personales del SICOV, la RNEC y otros consentimientos requeridos.

f) 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.

2.5.8.1.5. 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 organismo de apoyo 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.

1. **Momentos de validación:** Este proceso fundamental de verificación se empleará:
 - Por parte de todos los usuarios del servicio y miembros del personal del CEA, CIA y OTT, al momento del primer acceso o enrolamiento formal en el Sistema.
 - Por parte de todos los usuarios y personal de instructores de los CEA, CIA y OTT, así:
 - o De manera aleatoria en 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:

Para los usuarios e instructores, en los momentos de validación inicial o final de la clase, curso, o examen.

RESOLUCIÓN NÚMERO _____ DE _____

"Por medio de la cual se modifican las Resoluciones 5790 y 60832 de 2016 de la Superintendencia de Transporte y se introducen mejoras y medidas para fortalecer las capacidades de inspección, Vigilancia y Control a través de su Sistema de Control y Vigilancia para CEA, CIA y OTT"

- 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 verificación de identidad contra la RNEC se efectuará utilizando los siguientes mecanismos, conforme a las directrices de dicha entidad 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 vida (liveness detection) de conformidad con lo establecido por la RNEC.

b) **Reconocimiento facial contra RNEC (mecanismo principal condicionado):** Se podrá emplear la tecnología de reconocimiento facial para la verificación contra la RNEC, una vez esta sea reglamentada y autorizada para este fin por esa entidad y provista a través de un operador biométrico 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 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.

RESOLUCIÓN NÚMERO _____ DE _____

"Por medio de la cual se modifican las Resoluciones 5790 y 60832 de 2016 de la Superintendencia de Transporte y se introducen mejoras y medidas para fortalecer las capacidades de inspección, Vigilancia y Control a través de su Sistema de Control y Vigilancia para CEA, CIA y OTT"

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) **Procedimiento de excepción biométrica:** En caso de que no sea posible validar la identidad del usuario mediante cotejo biométrico dactilar ni con comparación entre la selfie vs. su documento, se deberá seguir el siguiente procedimiento de excepción:

1. El usuario deberá acudir ante la RNEC para que dicha entidad certifique o haga constar la condición y/o afección individual que le impide al usuario validar su identidad biométrica dactilar.
2. Una vez obtenida la certificación, el usuario deberá dirigirse al CEA, CIA u OTT correspondiente y entregar el certificado.
3. El personal encargado del enrolamiento en el centro recibirá el certificado, lo escaneará y radicará de inmediato en el SICOV a través del mecanismo que este habilite.
4. El SICOV almacenará los registros (logs) del uso del mecanismo de excepción biométrica, con todos los detalles de información del usuario, intentos de validación y del servicio.
5. Los enrolamientos de todos los servicios que activen con el uso del mecanismo de excepción biométrica quedarán marcados por esa causa y serán objeto de posterior seguimiento y verificación por parte de la Superintendencia de Transporte.
6. A través del SICOV se capturará una fotografía del usuario en el momento de activación de la excepción biométrica, la cual será utilizada como template para las validaciones que se realicen durante y al finalizar las clases o el curso.
7. El operador homologado del SICOV validará la veracidad del certificado entregado por el usuario, expedido por la RNEC.

Parágrafo 1. El proveedor del SICOV deberá informar a la Superintendencia, a través de los tableros de datos del Módulo de consulta, IVC e inteligencia de negocio del CPD Analítico, la información detallada de aquellos servicios en los que se utilizó el mecanismo de excepción biométrica.

Parágrafo 2. Mientras el proveedor del SICOV valida la veracidad de la información contenida en el certificado expedido por la RNEC que aporte un usuario, el usuario podrá avanzar en el proceso de capacitación.

RESOLUCIÓN NÚMERO _____ DE _____

"Por medio de la cual se modifican las Resoluciones 5790 y 60832 de 2016 de la Superintendencia de Transporte y se introducen mejoras y medidas para fortalecer las capacidades de inspección, Vigilancia y Control a través de su Sistema de Control y Vigilancia para CEA, CIA y OTT"

De confirmar alguna presunta irregularidad en la certificación aportada por el usuario, el Sistema restringirá la funcionalidad que permite la expedición de certificaciones a favor de dicho usuario quedando restringido el reporte de certificación objeto de consulta por parte del RUNT.

2.5.8.1.6. Gestión del registro y control de información del personal vinculado a los organismos de apoyo.

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 organismos de apoyo, incluyendo instructores, personal administrativo y directivo que interactúe con el Sistema.

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 y estado del personal:

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 precedentes de este Anexo y 2) a la existencia del registro en el RUNT de los instructores, cuando aplique.

b) El SICOV registrará la fecha de vinculación y, cuando ocurra, la fecha de desvinculación efectiva del personal, información que deberá ser actualizada diligentemente por el organismo de apoyo, 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 por la Superintendencia para la consecución de funciones públicas de Inspección, Vigilancia y Control, la confidencialidad de la información y las consecuencias ante malas prácticas y el uso indebido del Sistema por acciones en las que puede incurrir el personal vinculado al organismo de apoyo.

RESOLUCIÓN NÚMERO _____ DE _____

"Por medio de la cual se modifican las Resoluciones 5790 y 60832 de 2016 de la Superintendencia de Transporte y se introducen mejoras y medidas para fortalecer las capacidades de inspección, Vigilancia y Control a través de su Sistema de Control y Vigilancia para CEA, CIA y OTT"

2. Control de actividad y vigencia del registro de instructores:

a) **Inactivación temporal por inactividad prolongada:** El SICOV identificará automáticamente a aquellos instructores para los cuales no se registre actividad de impartición de clases o cursos en el Sistema durante un periodo consecutivo de treinta (30) días calendario. En tal caso, el Sistema modificará el estado del instructor a "inactivo temporalmente" y generará una alerta dirigida al organismo de apoyo y, de ser posible, al instructor, 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 instructor 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 instructor en este estado pueda volver a impartir clases o cursos, el organismo de apoyo deberá realizar un nuevo proceso de registro inicial completo. El SICOV dejará traza de este procedimiento.

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:

- i. Tipo de vinculación contractual.
- ii. Cargo o rol desempeñado y, para los instructores, las categorías para las cuales está autorizado.
- iii. Número, categoría, fecha de expedición y vigencia de la licencia de conducción (cuando sea requisito para el cargo).
- iv. Para los instructores, información de su licencia o certificado de idoneidad, con su respectiva vigencia.
- v. Certificados de títulos académicos y de formación relevantes para el ejercicio de sus funciones.
- vi. Un historial de las verificaciones de identidad realizadas contra las bases de datos de la RNEC y a través de tecnología de reconocimiento facial.
- vii. Opcionalmente, y previa autorización explícita del titular, se podrá registrar información sobre comparendos por infracciones a las normas de tránsito que puedan ser relevantes para evaluar su idoneidad continua. Esta información se tratará con especial cuidado y su acceso será restringido.

RESOLUCIÓN NÚMERO _____ DE _____

"Por medio de la cual se modifican las Resoluciones 5790 y 60832 de 2016 de la Superintendencia de Transporte y se introducen mejoras y medidas para fortalecer las capacidades de inspección, Vigilancia y Control a través de su Sistema de Control y Vigilancia para CEA, CIA y OTT"

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 legales 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 de los instructores en diferentes CEA, CIA y OTT, permitiendo así a la Superintendencia de Transporte detectar y analizar patrones que puedan ser indicativos de anomalías o irregularidades.

La interoperabilidad entre sistemas y su parametrización restringirá automáticamente la posibilidad de que se agende más de una clase o curso a un mismo instructor en el mismo o en diferentes establecimientos u organismos de apoyo, en el mismo horario. El análisis de esta información servirá como insumo para focalizar y priorizar las acciones de inspección, vigilancia y control de la entidad.

2.5.8.1.7. Validación continua de identidad de los participantes en el proceso de capacitación o curso.

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 de los instructores, así como del personal certificador, durante todas las etapas del proceso de capacitación 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 a los momentos y reglas específicas que se detallarán en los capítulos de funcionalidades particulares para cada tipo de organismo de apoyo:

a) **Reconocimiento facial (selfie vs. template):** Como mecanismo ágil de verificación, comparando una imagen facial capturada en tiempo real

RESOLUCIÓN NÚMERO _____ DE _____

"Por medio de la cual se modifican las Resoluciones 5790 y 60832 de 2016 de la Superintendencia de Transporte y se introducen mejoras y medidas para fortalecer las capacidades de inspección, Vigilancia y Control a través de su Sistema de Control y Vigilancia para CEA, CIA y OTT" contra el patrón biométrico de referencia (template) previamente registrada 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 instructores, como mínimo, en los siguientes tres momentos clave de cada sesión de clase o curso: **al inicio, durante (para verificación de permanencia) y al finalizar.** Los mecanismos específicos a utilizar en cada uno de estos momentos, tanto para clases teóricas como prácticas, se detallarán en las secciones de funcionalidades particulares para CEA y para CIA/OTT.
3. **Validación de identidad del personal certificador:** La validación de la identidad de la persona designada y registrada en el SICOV por el organismo de apoyo para expedir los certificados (sea el representante legal o su delegado) 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

RESOLUCIÓN NÚMERO _____ DE _____

"Por medio de la cual se modifican las Resoluciones 5790 y 60832 de 2016 de la Superintendencia de Transporte y se introducen mejoras y medidas para fortalecer las capacidades de inspección, Vigilancia y Control a través de su Sistema de Control y Vigilancia para CEA, CIA y OTT" 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 el desarrollo del curso:** 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 el procedimiento de validación de identidad mediante tecnología de reconocimiento facial (comparación entre selfie y template) del aspirante y/o del instructor.

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 del mecanismo de excepción biométrica a lo largo de la prestación del servicio de todos aquellos usuarios que hayan validado satisfactoriamente su identidad al menos una vez a través de cotejo biométrico dactilar y/o del uso de tecnología de reconocimiento facial a lo largo de la prestación del servicio.

2.5.8.1.8. Procesamiento analítico de datos de validación para la integridad del proceso de capacitación.

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 e instructores. 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 e instructores. Este registro detallado deberá incluir, como mínimo: el mecanismo de validación empleado, el

RESOLUCIÓN NÚMERO _____ DE _____

"Por medio de la cual se modifican las Resoluciones 5790 y 60832 de 2016 de la Superintendencia de Transporte y se introducen mejoras y medidas para fortalecer las capacidades de inspección, Vigilancia y Control a través de su Sistema de Control y Vigilancia para CEA, CIA y OTT" resultado de cada validación, la fecha y hora exactas, la identificación del usuario e instructor involucrados, la información del organismo de apoyo, el aula o vehículo asociado, y la clase o curso específico.

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 las sesiones de capacitación:** El SICOV deberá contabilizar y llevar un registro preciso del tiempo de duración efectiva de cada sesión de clase o curso impartido, verificando que la duración de cada hora académica cumpla, como mínimo, con el tiempo establecido en la normatividad sectorial vigente que regule la materia.

2.5.8.1.9. Gestión de la programación académica y 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 las clases o cursos, así como la asignación y el control de los recursos académicos necesarios para su impartición (tales como instructores y aulas), a través de la plataforma SICOV.

1. **Programación y gestión centralizada:** El personal debidamente autorizado del organismo de apoyo será responsable de realizar la totalidad de la programación de los servicios de capacitación o cursos 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 académica interna deberá sincronizarse en tiempo real con el agendamiento web, conforme a lo señalado en el siguiente numeral, asegurando que los cupos reservados digitalmente por los ciudadanos queden automáticamente bloqueados y asignados en el cronograma de recursos del organismo de apoyo.

RESOLUCIÓN NÚMERO _____ DE _____

"Por medio de la cual se modifican las Resoluciones 5790 y 60832 de 2016 de la Superintendencia de Transporte y se introducen mejoras y medidas para fortalecer las capacidades de inspección, Vigilancia y Control a través de su Sistema de Control y Vigilancia para CEA, CIA y OTT"

2. **Registro y trazabilidad de contenidos curriculares:** El SICOV deberá permitir al organismo de apoyo registrar, para cada clase o curso programado, los módulos o temas específicos de las mallas curriculares definidas por la Agencia Nacional de Seguridad Vial (ANSV) o el Ministerio de Transporte. El Sistema facilitará la trazabilidad de los contenidos impartidos y generará reportes que permitan a la Superintendencia de Transporte supervisar la correspondencia entre lo programado y las mallas curriculares oficiales.

2.5.8.1.10. Gestión de agendamiento web.

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 servicios ofertados por los organismos de apoyo, 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 organismos de apoyo 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 con plataformas externas que cumplan los requisitos de seguridad de este anexo.
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 ley, 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: Consultar la disponibilidad real de cupos y realizar la reserva de la cita, la cual se sincronizará automáticamente con la agenda interna del organismo, reservando ese espacio de tiempo para evitar sobreventas.

RESOLUCIÓN NÚMERO _____ DE _____

"Por medio de la cual se modifican las Resoluciones 5790 y 60832 de 2016 de la Superintendencia de Transporte y se introducen mejoras y medidas para fortalecer las capacidades de inspección, Vigilancia y Control a través de su Sistema de Control y Vigilancia para CEA, CIA y OTT"

3. Para confirmar la reserva, el sistema exigirá el respaldo transaccional mediante la compra directa del PIN (pasarelas de pago con dispersión).
 - a. La reserva se sincronizará automáticamente con la agenda interna del organismo, bloqueando el recurso (instructor/vehículo/aula).
 - 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. El sistema permitirá reservar citas únicamente para horarios que inicien, como mínimo, dos (2) horas después del momento de la transacción.
 - 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).

2.5.8.1.11. Gestión del registro histórico detallado del proceso de capacitación.

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 las clases o cursos que componen su proceso de capacitación en un organismo de apoyo.

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

- a) **Identificación de la sesión:** Fecha, hora de inicio y finalización real de cada sesión, sede del organismo de apoyo, aula o vehículo utilizado (según aplique), e identificación del instructor o instructores responsables de impartirla.
- b) **Contenido formativo:** La temática o módulos específicos abordados durante la sesión, conforme a la malla curricular registrada y lo reportado por el instructor.

RESOLUCIÓN NÚMERO _____ DE _____

"Por medio de la cual se modifican las Resoluciones 5790 y 60832 de 2016 de la Superintendencia de Transporte y se introducen mejoras y medidas para fortalecer las capacidades de inspección, Vigilancia y Control a través de su Sistema de Control y Vigilancia para CEA, CIA y OTT"

c) **Constancia de asistencia y permanencia:** La clasificación final de la sesión como "Cursada" o "No Cursada", basada en los resultados de las validaciones de identidad y permanencia, conforme a lo establecido en los numerales correspondientes de este Anexo Técnico.

d) **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.

e) **Registro de incidentes de permanencia:** En caso de que se haya activado un procedimiento de re-validación individual por no haberse detectado la permanencia de un participante, el registro deberá incluir la alerta generada por el Sistema y el resultado del posterior intento de verificación.

f) **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.

g) **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.

2.5.8.1.12. Integración e interfaz de validación para el registro de información del servicio y 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 (RUNT) verificar, previo al registro de un certificado expedido por un organismo de apoyo, que el usuario cumplió con la totalidad de los requisitos del proceso de capacitación monitoreados y validados por el SICOV.

RESOLUCIÓN NÚMERO _____ DE _____

"Por medio de la cual se modifican las Resoluciones 5790 y 60832 de 2016 de la Superintendencia de Transporte y se introducen mejoras y medidas para fortalecer las capacidades de inspección, Vigilancia y Control a través de su Sistema de Control y Vigilancia para CEA, CIA y OTT"

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) al que se presta el servicio.
- b) El estado de la "Decisión de Certificación" del usuario dentro del SICOV, señalando si este ha cumplido satisfactoriamente con la totalidad de los requisitos del proceso, incluyendo las validaciones de identidad y permanencia requeridas.

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

2.5.8.1.13. Gestión de conformidad documental y continuidad operativa de los organismos de apoyo.

El Sistema de Control y Vigilancia implementará funcionalidades integrales para la gestión y verificación continua del cumplimiento, por parte de los organismos de apoyo, 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 organismo de apoyo 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 centralizado donde cada organismo de apoyo 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

RESOLUCIÓN NÚMERO _____ DE _____

"Por medio de la cual se modifican las Resoluciones 5790 y 60832 de 2016 de la Superintendencia de Transporte y se introducen mejoras y medidas para fortalecer las capacidades de inspección, Vigilancia y Control a través de su Sistema de Control y Vigilancia para CEA, CIA y OTT" originales, así como su renovación y actualización oportuna antes de su fecha de vencimiento.

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 organismo de apoyo 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 registrado por el organismo de apoyo, a través de correo electrónico certificado.
- c) El Sistema generará y enviará alertas en caso de encontrar inconsistencias entre la información registrada por el CEA, CIA y OTT 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.
- d) El SICOV deberá conservar un registro auditable del envío y de la entrega de estas notificaciones, así como del cargue y actualización de los documentos por parte del organismo de apoyo.

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 CEA, CIA y OTT, 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 administradoras 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.

RESOLUCIÓN NÚMERO _____ DE _____

"Por medio de la cual se modifican las Resoluciones 5790 y 60832 de 2016 de la Superintendencia de Transporte y se introducen mejoras y medidas para fortalecer las capacidades de inspección, Vigilancia y Control a través de su Sistema de Control y Vigilancia para CEA, CIA y OTT"

Sustenta la autenticación segura del personal enrolado y garantiza la consulta de información personal del individuo.

- **Organismos evaluadores de la conformidad:** Validación del estado de certificación de los organismos de apoyo asegurando la coherencia entre la certificación vigente, su contenido y la realidad de la operación de estos organismos.
- **Ministerio de Transporte – Registro Único Nacional de Tránsito:** Para la confirmación de que los CEA, CIA y OTT y su personal se encuentran registrados y cumplen con los requisitos para desarrollar la actividad.

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 organismo de apoyo 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 organismo de apoyo 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 organismo de apoyo 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.

RESOLUCIÓN NÚMERO _____ DE _____

"Por medio de la cual se modifican las Resoluciones 5790 y 60832 de 2016 de la Superintendencia de Transporte y se introducen mejoras y medidas para fortalecer las capacidades de inspección, Vigilancia y Control a través de su Sistema de Control y Vigilancia para CEA, CIA y OTT"

- d) **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 presuntas irregularidades de diferente tipo conforme a lo establecido en este Anexo Técnico.

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) instructor(es) involucrados y del usuario del servicio de capacitación.

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

e) **Procedimiento para el 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 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 CEA, CIA y OTT, se 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.

RESOLUCIÓN NÚMERO _____ DE _____

"Por medio de la cual se modifican las Resoluciones 5790 y 60832 de 2016 de la Superintendencia de Transporte y se introducen mejoras y medidas para fortalecer las capacidades de inspección, Vigilancia y Control a través de su Sistema de Control y Vigilancia para CEA, CIA y OTT"

2.5.8.1.14. 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 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 CEA, CIA u OTT, 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. 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 de ejecución de órdenes 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 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, a fin de coordinar de manera oportuna la reactivación del servicio y evitar la afectación injustificada de los derechos del administrado.

RESOLUCIÓN NÚMERO _____ DE _____

"Por medio de la cual se modifican las Resoluciones 5790 y 60832 de 2016 de la Superintendencia de Transporte y se introducen mejoras y medidas para fortalecer las capacidades de inspección, Vigilancia y Control a través de su Sistema de Control y Vigilancia para CEA, CIA y OTT"

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.

2.5.8.1.15. 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 o recertificación efectuadas a los organismos de apoyo por los Organismos Evaluadores de la Conformidad (OEC) acreditados.

El CEA, CIA y OTT deberá cargar en el Sistema y reportar el contenido del informe de seguimiento y evaluación con sus resultados, al cierre del mismo dentro de los tres (3) días hábiles siguientes al recibo de cada informe.

El Sistema deberá facilitar la extracción o el registro estructurado de los hallazgos, no conformidades y oportunidades 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 certificación 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 y acciones correctivas o de mejora, en lo que sea de su competencia.

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

RESOLUCIÓN NÚMERO _____ DE _____

"Por medio de la cual se modifican las Resoluciones 5790 y 60832 de 2016 de la Superintendencia de Transporte y se introducen mejoras y medidas para fortalecer las capacidades de inspección, Vigilancia y Control a través de su Sistema de Control y Vigilancia para CEA, CIA y OTT"

El Sistema de Control y Vigilancia deberá incorporar mecanismos y herramientas que permitan gestionar la geolocalización automática de los equipos y dispositivos empleados por el organismo de apoyo para prestar el servicio, para asegurar que el uso de dispositivos y cargue de información se realicen exclusivamente desde los sitios autorizadas y a través de canales seguros.

a) **Verificación del origen de las operaciones:** El Sistema deberá constatar, a través de medios técnicos como la geolocalización (GPS) de los dispositivos fijos y móviles, 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 organismo de apoyo y los servidores centrales del SICOV se realice a través de canales de comunicación seguros que preserven la integridad y confidencialidad de los datos, conforme a los estándares de seguridad definidos en este Anexo Técnico.

2.5.8.1.17. Verificación continua de la permanencia de los participantes.

El Sistema de Control y Vigilancia deberá implementar mecanismos tecnológicos para verificar la permanencia continua de los usuarios del servicio y los instructores durante el desarrollo completo de cada sesión de clase o curso, tanto en modalidad presencial como virtual. Esta función es crucial para asegurar la participación efectiva en el proceso de capacitación y prevenir el abandono de las sesiones una vez realizada la validación inicial de identidad.

1. **Mecanismo general de verificación:** El SICOV recabará y analizará en tiempo real la información de los participantes presentes en un aula o vehículo, realizando, como mínimo, un procedimiento de comprobación de permanencia por cada hora académica cursada. El mecanismo principal para esta verificación será la **tecnología de reconocimiento facial**, que procesará al menos una captura visual de los asistentes en cualquier momento, a horas aleatoriamente escogidas por el Sistema, para validar su identidad. Este procedimiento se realizará por cada hora de sesión.
2. **Procedimiento de revalidación por no detección:** Si como resultado del procedimiento automático de verificación de permanencia, el Sistema

RESOLUCIÓN NÚMERO _____ DE _____

"Por medio de la cual se modifican las Resoluciones 5790 y 60832 de 2016 de la Superintendencia de Transporte y se introducen mejoras y medidas para fortalecer las capacidades de inspección, Vigilancia y Control a través de su Sistema de Control y Vigilancia para CEA, CIA y OTT"

no logra identificar o detectar a un participante que se registró al inicio, se activará de inmediato un procedimiento de **revalidación individual** que seguirá las reglas contempladas en los numerales que desarrollan las funcionalidades específicas del SICOV en CEA y en CIA y OTT para la validación de identidad durante el servicio. Dicho procedimiento requerirá que la persona confirme su identidad a través del mecanismo biométrico de reconocimiento facial dentro de los cinco (5) minutos siguientes al intento fallido de validación dispuesto para el efecto.

3. **Infraestructura descentralizada y software requerido:** La implementación de esta funcionalidad requerirá la instalación de infraestructura y hardware en los organismos de apoyo (como cámaras en aulas, dispositivos móviles en vehículos e infraestructura descentralizada), así como el uso de software especializado.

2.5.8.1.18. 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 organismo de apoyo. Esta capacidad determinará el volumen máximo de servicios (clases, cursos 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 organismo de apoyo 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 (ej. número de aulas, aforo máximo, número de instructores, y vehículos por categoría cuando aplique) consignada en el certificado de conformidad vigente y en los informes de auditoría del Organismo Evaluador de la Conformidad (OEC).
 - b) La información detallada y actualizada que el organismo de apoyo registre directamente en el SICOV sobre sus recursos disponibles y habilitados, incluyendo instructores activos, vehículos de enseñanza operativos (para CEA), y aulas físicas con su dimensionamiento.
 - 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

RESOLUCIÓN NÚMERO _____ DE _____

"Por medio de la cual se modifican las Resoluciones 5790 y 60832 de 2016 de la Superintendencia de Transporte y se introducen mejoras y medidas para fortalecer las capacidades de inspección, Vigilancia y Control a través de su Sistema de Control y Vigilancia para CEA, CIA y OTT"

homologados conforme a las instrucciones y lineamientos de la Superintendencia.

En caso de discrepancia en la capacidad instalada u operativa de un CEA, CIA u OTT, se le dará prevalencia a la información obtenida en las visitas que se realicen a los establecimientos, sobre la información registrada por el organismo de apoyo en el SICOV.

2. **Control automático de agendamiento y asignación de recursos:** El SICOV estará parametrizado para impedir el agendamiento de clases o cursos y la asignación de recursos que excedan la capacidad instalada registrada y validada para el organismo de apoyo. Específicamente, el Sistema impedirá que se programe más de una actividad simultáneamente para una misma aula o vehículo, o que un mismo instructor sea asignado a más de una actividad en el mismo horario.
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, excediendo los límites previstos en la normatividad (p. ej. Horas de clase dictadas por un instructor u horas de clase práctica en un vehículo), se exige la implementación de mecanismos de integración o interoperabilidad para el intercambio seguro de información relevante entre los distintos software desarrollados por los proveedores homologados 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.

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

El Sistema de Control y Vigilancia facilitará a cada organismo de apoyo 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

RESOLUCIÓN NÚMERO _____ DE _____

"Por medio de la cual se modifican las Resoluciones 5790 y 60832 de 2016 de la Superintendencia de Transporte y se introducen mejoras y medidas para fortalecer las capacidades de inspección, Vigilancia y Control a través de su Sistema de Control y Vigilancia para CEA, CIA y OTT" 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 CEA, CIA y OTT, 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:

RESOLUCIÓN NÚMERO _____ DE _____

"Por medio de la cual se modifican las Resoluciones 5790 y 60832 de 2016 de la Superintendencia de Transporte y se introducen mejoras y medidas para fortalecer las capacidades de inspección, Vigilancia y Control a través de su Sistema de Control y Vigilancia para CEA, CIA y OTT"

a) El SICOV ofrecerá un conjunto de informes operativos predefinidos que reflejen los principales indicadores de gestión del CEA, CIA y OTT. 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 organismos de apoyo 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.

RESOLUCIÓN NÚMERO _____ DE _____

"Por medio de la cual se modifican las Resoluciones 5790 y 60832 de 2016 de la Superintendencia de Transporte y se introducen mejoras y medidas para fortalecer las capacidades de inspección, Vigilancia y Control a través de su Sistema de Control y Vigilancia para CEA, CIA y OTT"

2.5.8.1.20. Clasificación automática del estado de las sesiones del proceso de capacitación.

El Sistema de Control y Vigilancia deberá clasificar de manera automática cada sesión de clase o curso registrada para un usuario como **"Cursada"** o **"No Cursada"**. Esta clasificación se basará estrictamente en el cumplimiento de los requisitos de validación de identidad y de verificación de permanencia, tanto del usuario como del instructor, conforme a los procedimientos detallados en los numerales correspondientes de este Anexo Técnico.

1. **Criterios para clasificación como "Cursada"**: Una sesión se clasificará automáticamente como "Cursada" si, y solo si, el SICOV registra que se cumplieron de manera acumulativa y satisfactoria todos los puntos de control de identidad y permanencia establecidos para dicha sesión (ej. al inicio, durante y al finalizar). El SICOV registrará esta clasificación de forma inmediata y automatizada una vez se confirmen todas las validaciones requeridas.
2. **Criterios para clasificación como "No Cursada"**: Cualquier sesión que no cumpla con la totalidad de los criterios establecidos en el numeral anterior será clasificada automáticamente por el SICOV como "No Cursada". El Sistema habilitará un campo de diligenciamiento obligatorio para que el personal del CEA, CIA u OTT registre el motivo específico de dicha clasificación (ej. falla en la validación de identidad final del usuario, no detección de permanencia en la sesión, fallas en el Sistema con su descripción con evidencia, etc.) y esta información deberá estar disponible para consulta por parte del organismo de apoyo y, en lo posible, ser informada al usuario.

2.5.8.1.21. Habilitación para la expedición de certificados.

El Sistema de Control y Vigilancia deberá gestionar el proceso de generación de los certificados de culminación del proceso de capacitación 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

RESOLUCIÓN NÚMERO _____ DE _____

"Por medio de la cual se modifican las Resoluciones 5790 y 60832 de 2016 de la Superintendencia de Transporte y se introducen mejoras y medidas para fortalecer las capacidades de inspección, Vigilancia y Control a través de su Sistema de Control y Vigilancia para CEA, CIA y OTT" indispensable que el proceso de capacitación (clase o curso) haya sido clasificado como "**Cursado**" por el SICOV, 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.
- b) El Sistema deberá generar el certificado con toda la información del usuario y la categoría de la licencia a la que aspira, incluyendo un número único de identificación y los mecanismos para su posterior validación y registro en el RUNT. Además, el certificado deberá ser firmado digitalmente por el representante legal del organismo de apoyo y/o el personal autorizado para dicha expedición.
- 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.

2.5.8.1.22. 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 organismo de apoyo.

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.

RESOLUCIÓN NÚMERO _____ DE _____

"Por medio de la cual se modifican las Resoluciones 5790 y 60832 de 2016 de la Superintendencia de Transporte y se introducen mejoras y medidas para fortalecer las capacidades de inspección, Vigilancia y Control a través de su Sistema de Control y Vigilancia para CEA, CIA y OTT"

- e. Identificación de los instructores que impartieron las clases o el curso sobre normas de tránsito al usuario.
- f. Identificación del funcionario del organismo de apoyo (representante legal o su delegado) que autorizó y formalizó la expedición del certificado en el SICOV.

2.5.8.1.23. Registro y actualización de tarifas de servicios.

El Sistema de Control y Vigilancia deberá disponer de una funcionalidad para que cada organismo de apoyo registre y mantenga actualizada la información detallada de las tarifas que establece y ofrece al público por sus servicios de capacitación o cursos.

1. **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 totalidad de las tarifas vigentes 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.
2. **Finalidad del registro tarifario en SICOV:** La información sobre las tarifas registrada en el SICOV tendrá como finalidades principales:
 - a) Facilitar la transparencia informativa hacia los aspirantes y usuarios del servicio.
 - b) 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.
 - c) 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.
3. **Actualización automática de tarifas mínimas:** el Sistema estará configurado de 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 CEA, 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

RESOLUCIÓN NÚMERO _____ DE _____

"Por medio de la cual se modifican las Resoluciones 5790 y 60832 de 2016 de la Superintendencia de Transporte y se introducen mejoras y medidas para fortalecer las capacidades de inspección, Vigilancia y Control a través de su Sistema de Control y Vigilancia para CEA, CIA y OTT" el valor de la tarifa de aquellos CEA que la tuvieran configurada en el mínimo monto tarifario al cierre del año inmediatamente anterior.

2.5.8.1.24. Aplicación móvil del SICOV para usuarios e instructores.

El Sistema de Control y Vigilancia deberá incluir y soportar una aplicación móvil oficial, compatible con los sistemas operativos Android e iOS, destinada a facilitar la interacción y el acceso a información relevante por parte de los usuarios del servicio y los instructores vinculados a los organismos de apoyo.

El acceso a las funcionalidades de la aplicación móvil requerirá la autenticación segura de los usuarios e instructores mediante sus credenciales SICOV.

1. **Funcionalidades para usuarios del servicio:** La aplicación móvil deberá permitir al usuario, como mínimo, las siguientes funcionalidades generales:
 - a) Consultar su historial de clases o cursos, visualizando las sesiones clasificadas como "Cursadas", las pendientes y el estado general de su progreso en el proceso de capacitación.
 - b) Consultar las tarifas vigentes de los servicios ofrecidos por el organismo de apoyo al que se encuentre vinculado.
 - c) Visualizar el estado de los Números Únicos de Identificación de Pago (PIN) adquiridos y asociados a su proceso.
 - d) Recibir notificaciones y recordatorios automáticos sobre clases o cursos programados, así como alertas sobre los requerimientos de validación de identidad.
 - e) Gestionar sus clases o cursos (consultar, programar, confirmar, reprogramar o cancelar), sujeto a las políticas operativas que para ello haya establecido el respectivo organismo de apoyo.
 - f) Acceder a la funcionalidad de valoración de la calidad del servicio (instructores y contenidos), conforme a lo establecido en este Anexo Técnico.
2. **Funcionalidades para instructores:** La aplicación móvil deberá permitir al instructor, como mínimo, las siguientes funcionalidades generales:
 - a) Consultar su agenda personal de clases o cursos programados en el SICOV.

RESOLUCIÓN NÚMERO _____ DE _____

"Por medio de la cual se modifican las Resoluciones 5790 y 60832 de 2016 de la Superintendencia de Transporte y se introducen mejoras y medidas para fortalecer las capacidades de inspección, Vigilancia y Control a través de su Sistema de Control y Vigilancia para CEA, CIA y OTT"

b) Recibir notificaciones y recordatorios sobre sus actividades asignadas y cualquier cambio relevante en su programación.

c) Recibir información sobre los requerimientos y procedimientos de validación de identidad que se le aplicarán durante la impartición de las clases o cursos.

2.5.8.1.25. 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 presuntos 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 organismo de apoyo. La información para el CEA, CIA u OTT 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 y no críticos:** Se generará una alerta si el sistema detecta que un CEA, CIA u OTT no ha

RESOLUCIÓN NÚMERO _____ DE _____

"Por medio de la cual se modifican las Resoluciones 5790 y 60832 de 2016 de la Superintendencia de Transporte y se introducen mejoras y medidas para fortalecer las capacidades de inspección, Vigilancia y Control a través de su Sistema de Control y Vigilancia para CEA, CIA y OTT"

subsano 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 sin SOAT y/o RTMyEC:** Se generará una alerta de restricción automática si detecta, bien por cuenta de la información registrada por el CEA y disponible en el Sistema; o como resultado de la comparación de la información registrada y la consulta que realice el operador homologado del SICOV en el RUNT, o eventualmente por recepción directa de información gracias al funcionamiento de un mecanismo de interoperabilidad con la Superintendencia de Transporte que permita la transmisión de información del RUNT (una vez este sea implementado), que un vehículo de enseñanza no cuenta con SOAT o con el certificado de revisión técnico-mecánica y de emisiones contaminantes (RTMyEC) vigentes.

Alertas por posible manipulación de dispositivos y 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 o vehículos de los organismos de apoyo.
- **Duplicidad o inconsistencias en el IDClient:** El sistema generará una alerta si se detecta que un organismo de apoyo 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 de cualquier sesión o curso (inicio, durante, cierre). Para el caso del personal, la alerta se activará si estos fallos se presentan consecutivamente en tres o más sesiones seguidas (clases o cursos).

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.

RESOLUCIÓN NÚMERO _____ DE _____

"Por medio de la cual se modifican las Resoluciones 5790 y 60832 de 2016 de la Superintendencia de Transporte y se introducen mejoras y medidas para fortalecer las capacidades de inspección, Vigilancia y Control a través de su Sistema de Control y Vigilancia para CEA, CIA y OTT"

- **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.
- **Calificaciones consistentemente bajas:** El SICOV podrá generar alertas si se detectan patrones de calificaciones consistentemente bajas en los instructores o en los servicios prestados por un organismo de apoyo, a través del sistema de valoración de la calidad.

Otras alertas:

- El incumplimiento de los requisitos documentales críticos y no críticos, según se detalla en la función de gestión de conformidad documental.
- 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.
- Cualquier otra situación específica que el presente Anexo Técnico defina como susceptible de generar una alerta automática.

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 del servicio prestado con la especificación de la causal de activación, para efectos de supervisión, y dejará, para efectos de supervisión, un registro detallado con la trazabilidad histórica del servicio marcado.

Con estas evidencias, la Superintendencia de Transporte podrá solicitar, visualizar y descargar informes de los operadores homologados del SICOV, sobre capacitaciones y cursos específicos dictados por CEA, CIA y OTT de todo el país que hayan quedado marcados por irregularidad, para consultar todos los detalles de los mismos.

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

RESOLUCIÓN NÚMERO _____ DE _____

"Por medio de la cual se modifican las Resoluciones 5790 y 60832 de 2016 de la Superintendencia de Transporte y se introducen mejoras y medidas para fortalecer las capacidades de inspección, Vigilancia y Control a través de su Sistema de Control y Vigilancia para CEA, CIA y OTT" 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 CEA, CIA u OTT, 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:

a) Cualquier orden administrativa de la Superintendencia de Suspensión preventiva de actividades de un CEA, CIA u OTT, 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 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

RESOLUCIÓN NÚMERO _____ DE _____

"Por medio de la cual se modifican las Resoluciones 5790 y 60832 de 2016 de la Superintendencia de Transporte y se introducen mejoras y medidas para fortalecer las capacidades de inspección, Vigilancia y Control a través de su Sistema de Control y Vigilancia para CEA, CIA y OTT"

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:

a) 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).

b) 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 discriminando si su origen fue específico o estructural.

2.5.8.1.26. Sistema de valoración de la calidad de la capacitación por parte de los usuarios.

RESOLUCIÓN NÚMERO _____ DE _____

"Por medio de la cual se modifican las Resoluciones 5790 y 60832 de 2016 de la Superintendencia de Transporte y se introducen mejoras y medidas para fortalecer las capacidades de inspección, Vigilancia y Control a través de su Sistema de Control y Vigilancia para CEA, CIA y OTT"

El Sistema de Control y Vigilancia, a través de su aplicación móvil oficial, deberá ofrecer a los usuarios la funcionalidad para valorar la calidad del servicio de capacitación o curso recibido en un organismo de apoyo. Esta valoración incluirá, como mínimo, la posibilidad de calificar a los instructores que impartieron las sesiones y de puntuar aspectos relevantes del contenido y desarrollo de las mismas.

1. **Condiciones para habilitar la valoración:** La opción de calificar y puntuar se habilitará en la aplicación móvil exclusivamente para aquellos usuarios cuyo proceso de capacitación (clase o curso) haya sido clasificado como "Cursado" en el SICOV, conforme a los procedimientos establecidos en este Anexo Técnico. La funcionalidad de valoración estará disponible para el usuario por un tiempo limitado después de haber cursado la respectiva sesión o curso, según el parámetro que defina la Superintendencia de Transporte, dentro de los seis meses siguientes a la implementación del sistema.
2. **Componentes de la valoración:** El sistema de valoración deberá permitir al usuario, como mínimo:
 - a) Evaluar el desempeño del instructor o instructores que impartieron el servicio, utilizando una escala definida y considerando criterios como claridad en las explicaciones, pedagogía, dominio del tema y trato respetuoso.
 - b) Evaluar la pertinencia, calidad y utilidad del contenido temático del servicio recibido y la organización de la sesión. La Superintendencia de Transporte podrá definir los criterios específicos, las escalas de calificación y los aspectos detallados a valorar, buscando la objetividad y utilidad de la información recopilada.
3. **Gestión y uso de la información de valoraciones:**
 - a) El SICOV registrará y procesará de forma anónima o seudonimizada (respecto al instructor y al organismo de apoyo) las valoraciones individuales para generar estadísticas agregadas y tendencias sobre la calidad del servicio.
 - b) La Superintendencia de Transporte tendrá acceso a la información consolidada y a los análisis derivados de estas valoraciones como insumo para sus funciones de IVC, la identificación de áreas de mejora en el sector

RESOLUCIÓN NÚMERO _____ DE _____

"Por medio de la cual se modifican las Resoluciones 5790 y 60832 de 2016 de la Superintendencia de Transporte y se introducen mejoras y medidas para fortalecer las capacidades de inspección, Vigilancia y Control a través de su Sistema de Control y Vigilancia para CEA, CIA y OTT" y la evaluación del desempeño general de los organismos de apoyo. Se podrán generar alertas a la Superintendencia ante patrones de calificaciones consistentemente bajas para instructores u organismos específicos.

c) Los organismos de apoyo podrán tener acceso a informes agregados y anonimizados sobre las valoraciones de sus propios instructores y servicios, como herramienta para su gestión interna de calidad.

d) El tratamiento de esta información se regirá por los principios de la Ley 1581 de 2012, informando a los usuarios sobre el uso que se dará a sus valoraciones y a los instructores sobre la existencia de este mecanismo de evaluación.

2.5.8.1.27. 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: $[(\text{Tiempo Total del Periodo de Medición} - \text{Tiempo Total de Indisponibilidad No Justificada}) / \text{Tiempo Total del Periodo de Medición}] * 100$.

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

RESOLUCIÓN NÚMERO _____ DE _____

"Por medio de la cual se modifican las Resoluciones 5790 y 60832 de 2016 de la Superintendencia de Transporte y se introducen mejoras y medidas para fortalecer las capacidades de inspección, Vigilancia y Control a través de su Sistema de Control y Vigilancia para CEA, CIA y OTT"

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 CEA, CIA y OTT con una anticipación mínima de cinco (5) días hábiles, explicando las razones de su realización. En el caso de los CEA, CIA y OTT, 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 CEA, CIA y OTT 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.

2.5.8.2. Funcionalidades particulares del SICOV para Centros de Enseñanza Automovilística

Introducción

Las funcionalidades que se describen a continuación son específicas para la operación de los Centros de Enseñanza Automovilística (CEA) y complementan o detallan las capacidades transversales descritas en el Numeral 2.5.7.1. del presente Anexo Técnico.

RESOLUCIÓN NÚMERO _____ DE _____

"Por medio de la cual se modifican las Resoluciones 5790 y 60832 de 2016 de la Superintendencia de Transporte y se introducen mejoras y medidas para fortalecer las capacidades de inspección, Vigilancia y Control a través de su Sistema de Control y Vigilancia para CEA, CIA y OTT"

2.5.8.2.1. Verificación de prerequisites y gestión de pagos.

En adición a lo establecido en la función transversal sobre gestión de pagos, para los Centros de Enseñanza Automovilística, el SICOV implementará las siguientes reglas específicas:

a) **Aplicabilidad:** La funcionalidad de gestión y registro de pagos se aplicará para todos los servicios de capacitación y certificación que ofrezca el CEA.

b) **Condicionamiento para el pago:** El SICOV solo habilitará la generación del número único de identificación de pago (PIN) para un curso de capacitación en conducción después de haber verificado en tiempo real que el aspirante cuenta con un Certificado de Aptitud en el examen de aptitud física, mental y de coordinación motriz, expedido por un Centro de Reconocimiento de Conductores (CRC y que dicho certificado se encuentra vigente.

c) **Mecanismo de verificación:** Esta verificación se realizará mediante la integración y consulta que el SICOV para CEA efectuará con el Sistema de Control y Vigilancia para Centros de Reconocimiento de Conductores (SICOV-CRC).

2.5.8.2.2. Gestión integral de evaluaciones de conocimiento teórico y práctico.

En adición a las funciones transversales, el SICOV deberá incorporar funcionalidades específicas para la administración, aplicación y registro de las evaluaciones de conocimiento teórico y práctico que son requisito para la obtención del Certificado de Aptitud en Conducción (CAC) en los Centros de Enseñanza Automovilística (CEA).

1. Gestión de evaluaciones teóricas:

a) **Repositorio de preguntas:** El SICOV deberá gestionar un repositorio de preguntas para las evaluaciones teóricas. Estas preguntas serán elaboradas por cada CEA conforme a los módulos y temas de la malla curricular oficial para cada categoría de licencia de conducción, y deberán seguir estrictamente los lineamientos, estructura y criterios de calidad definidos por la Agencia Nacional de Seguridad Vial (ANSV) y el Ministerio de Transporte.

RESOLUCIÓN NÚMERO _____ DE _____

"Por medio de la cual se modifican las Resoluciones 5790 y 60832 de 2016 de la Superintendencia de Transporte y se introducen mejoras y medidas para fortalecer las capacidades de inspección, Vigilancia y Control a través de su Sistema de Control y Vigilancia para CEA, CIA y OTT"

b) **Generación de exámenes:** A partir del repositorio de preguntas, el SICOV generará automáticamente las evaluaciones teóricas para cada usuario, seleccionando aleatoriamente un número determinado de preguntas (ocho (8) por cada módulo o tema a evaluar). El Sistema garantizará que las evaluaciones generadas sean únicas para cada aspirante que las presente simultáneamente.

c) **Registro y análisis de resultados:** El SICOV registrará los resultados detallados de cada evaluación, incluyendo las respuestas del usuario y la calificación. Podrá generar estadísticas sobre el rendimiento de las preguntas (ej. ranking por grado de dificultad) como insumo para la mejora continua del banco de preguntas por parte de la autoridad competente.

El sistema deberá proveer al usuario la visualización de su resultado final y de las preguntas que fueron respondidas incorrectamente, sin revelar la respuesta correcta, para fines informativos y pedagógicos.

d) **Criterios de aprobación:** Los porcentajes o criterios de aprobación para las evaluaciones teóricas se configurarán en el SICOV de estricta conformidad con lo establecido en la normatividad vigente expedida por el Ministerio de Transporte o la autoridad competente en la materia.

e) **Control del proceso:** El SICOV controlará el tiempo máximo para la realización de cada evaluación, entregará los resultados de forma automática e inmediata al usuario, y conservará el historial de todos los intentos realizados por cada aspirante.

2. Gestión de evaluaciones prácticas:

a) **Registro estructurado de resultados:** El SICOV deberá permitir al instructor designado registrar de manera estructurada los resultados de la prueba de evaluación práctica. La funcionalidad facilitará que el instructor califique cada uno de los ítems o maniobras a evaluar conforme a los criterios definidos en la normatividad, indicando si el aspirante cumplió o no con el estándar requerido.

b) **Registro del recorrido (GPS):** El SICOV deberá registrar y asociar a cada evaluación práctica el trazado georreferenciado completo del recorrido realizado por el vehículo de enseñanza, utilizando la información

RESOLUCIÓN NÚMERO _____ DE _____

"Por medio de la cual se modifican las Resoluciones 5790 y 60832 de 2016 de la Superintendencia de Transporte y se introducen mejoras y medidas para fortalecer las capacidades de inspección, Vigilancia y Control a través de su Sistema de Control y Vigilancia para CEA, CIA y OTT" del dispositivo con GPS con el que cuente el vehículo, instalado y monitoreado por el operador homologado.

2.5.8.2.3. Gestión y control de vehículos de enseñanza.

El Sistema de Control y Vigilancia deberá gestionar y mantener un registro actualizado y detallado de cada vehículo vinculado por un Centro de Enseñanza Automovilística para la impartición de clases prácticas. Esta funcionalidad se basará primordialmente en la información disponible y actualizada en el Registro Único Nacional de Tránsito, la cual deberá ser consultada a través de la consulta manual por parte del operador homologado y/o de la implementación del mecanismo de interoperabilidad que establezca la Superintendencia.

La información que se debe registrar por parte del CEA incluye, como mínimo la siguiente, por vehículo:

a) **Identificación y características del vehículo:** Número de placa (matrícula), marca, clase, línea, tipo de servicio (enseñanza), color, modelo, número de chasis (VIN), número de motor y demás especificaciones técnicas relevantes registradas en el RUNT.

b) **Documentación legal y de operación:**

i. Información de la licencia de tránsito y de la tarjeta de servicio (o documento equivalente), incluyendo su vigencia y correspondencia con el CEA.

ii. Fecha de expedición y vigencia de la póliza del Seguro Obligatorio de Accidentes de Tránsito (SOAT).

iii. Fecha de expedición y vigencia del Certificado de Revisión Técnico-Mecánica y de Emisiones Contaminantes (RTMyEC), así como la identificación del Centro de Diagnóstico Automotor (CDA) que la expidió.

iv. Para vehículos adaptados para la enseñanza a personas con discapacidad, información del certificado de adaptación correspondiente.

1. **Registro de novedades por parte del CEA:** El SICOV permitirá al CEA registrar, de forma oportuna, las siguientes novedades asociadas a sus vehículos vinculados:

RESOLUCIÓN NÚMERO _____ DE _____

"Por medio de la cual se modifican las Resoluciones 5790 y 60832 de 2016 de la Superintendencia de Transporte y se introducen mejoras y medidas para fortalecer las capacidades de inspección, Vigilancia y Control a través de su Sistema de Control y Vigilancia para CEA, CIA y OTT"

- Cualquier situación o evento que genere la indisponibilidad temporal o permanente del vehículo para la impartición de clases prácticas (ej. mantenimiento, reparación, hurto, siniestro), o cualquier otra novedad relevante que deba ser conocida por la Superintendencia de Transporte, conforme a los lineamientos que esta expida.
- La fecha exacta de vinculación del vehículo al CEA y la fecha de su desvinculación definitiva.

2. **Control automatizado por vigencia documental:**

a) El SICOV deberá generar alertas automáticas dirigidas al CEA con antelación suficiente sobre el próximo vencimiento de la póliza SOAT y/o del certificado de RTMyEC de los vehículos registrados.

b) El vencimiento de la póliza SOAT o del certificado de RTMyEC de un vehículo vinculado al CEA dará lugar, de forma automática e inmediata, a la restricción del uso de dicho vehículo en el SICOV. En consecuencia, no se podrán programar ni impartir clases prácticas en ese vehículo hasta que el CEA cargue en el Sistema los documentos vigentes que acrediten el cumplimiento de estos requisitos legales, y dichos documentos sean validados conforme al procedimiento que se establezca.

La información precisa sobre el momento (fecha y hora) exacto en que la medida de suspensión del CEA, CIA u OTT se haga efectiva en el Registro Único Nacional de Tránsito, que comunique a la Superintendencia el Ministerio de Transporte o directamente el concesionario del RUNT, será transmitida a los operadores homologados a través del mecanismo de interoperabilidad o consulta y con la periodicidad que se determine para tal efecto. El SICOV llevará dicho registro de información actualizado

La Superintendencia informará al operador SICOV cada vez que adopte una medida de suspensión en contra de un CEA, CIA u OTT.

3. **Verificación de la vinculación legal del vehículo al CEA:** El SICOV deberá contar con campos específicos para registrar la información de la Tarjeta de Servicio del vehículo. El operador del SICOV, utilizando la información registrada y las consultas disponibles al RUNT, verificará que dicho documento haya sido expedido a nombre del CEA y se encuentre vigente.

RESOLUCIÓN NÚMERO _____ DE _____

"Por medio de la cual se modifican las Resoluciones 5790 y 60832 de 2016 de la Superintendencia de Transporte y se introducen mejoras y medidas para fortalecer las capacidades de inspección, Vigilancia y Control a través de su Sistema de Control y Vigilancia para CEA, CIA y OTT"

2.5.8.2.4. Monitoreo y validación en tiempo real de vehículos de enseñanza.

El Sistema de Control y Vigilancia deberá registrar, monitorear y validar en tiempo real la ubicación geográfica y el recorrido de los vehículos de enseñanza vinculados al CEA durante la impartición de cada clase práctica. Esta función tiene como objetivo verificar la realización efectiva de la instrucción práctica y el cumplimiento de los parámetros de la clase.

1. Dispositivo de geolocalización vehicular y transmisión de datos:

a) Para cumplir con esta función, cada vehículo de enseñanza deberá circular con un dispositivo con tecnología de geolocalización (GPS) y con capacidad de transmisión de datos, el cual será suministrado, instalado y configurado por el proveedor autorizado del SICOV.

b) El dispositivo deberá ser instalado o estar asociado al vehículo para asegurar su permanencia y operatividad continua, y contará con medidas de protección efectivas contra la manipulación no autorizada, intentos de alteración o desinstalación, incluyendo la generación de alertas al SICOV ante tales eventos.

c) El dispositivo será resistente a las condiciones ambientales propias de la operación vehicular y deberá permitir la obtención y transmisión de la geoposición del vehículo durante todo el desarrollo de las clases prácticas.

d) La ubicación del dispositivo en el vehículo deberá permitir su eventual inspección por la Superintendencia de Transporte y el mantenimiento por personal técnico autorizado del proveedor del SICOV, sin que ello comprometa su seguridad o facilite la manipulación indebida por parte de terceros.

2. Funcionalidades del SICOV con base en datos de geolocalización:

a) El SICOV registrará el historial completo de ubicación y recorrido de cada vehículo durante las horas de clase práctica programadas y en desarrollo.

b) El SICOV permitirá a la Superintendencia de Transporte, a través del operador homologado y, para fines operativos, al CEA (respecto a sus

RESOLUCIÓN NÚMERO _____ DE _____

"Por medio de la cual se modifican las Resoluciones 5790 y 60832 de 2016 de la Superintendencia de Transporte y se introducen mejoras y medidas para fortalecer las capacidades de inspección, Vigilancia y Control a través de su Sistema de Control y Vigilancia para CEA, CIA y OTT" propios vehículos), la visualización en tiempo real de la ubicación de los vehículos que se encuentren impartiendo clases prácticas.

c) La información de geolocalización y recorridos servirá como insumo para la generación de reportes, la atención de quejas o reclamos, y los procesos de auditoría e investigación que adelante la Superintendencia de Transporte.

2.5.8.2.5. Homologación de módulos formativos comunes.

En adición a la función transversal de gestión de la programación académica, el SICOV implementará una funcionalidad específica para la homologación de módulos formativos en los Centros de Enseñanza Automovilística (CEA):

a) Cuando un aspirante a conductor se inscriba en un mismo CEA para cursar simultáneamente dos o más programas de capacitación conducentes a la obtención de licencias de conducción de diferentes categorías, y dicha inscripción múltiple ocurra dentro de un periodo no superior a tres (3) meses contados desde la primera inscripción, el SICOV permitirá la homologación de la asistencia y aprobación de aquellos módulos, unidades temáticas o clases teóricas cuyo contenido sea certificadamente común o equivalente para los programas involucrados, conforme a las directrices que establezca el Ministerio de Transporte.

b) No serán objeto de homologación las clases prácticas de conducción ni aquellos módulos o contenidos teóricos que sean específicos y diferenciados para cada categoría de licencia de conducción.

c) La aplicación de esta funcionalidad de homologación no implicará, bajo ninguna circunstancia, una reducción en la intensidad horaria total mínima exigida por la normatividad vigente para cada categoría de licencia de conducción. El SICOV deberá asegurar que el plan de formación del aspirante, aun con homologaciones, cumpla con la totalidad de horas requeridas.

2.5.8.2.6. Momentos y mecanismos específicos de validación de identidad.

En complemento a la función transversal de validación continua de identidad descrito en esta sección, para la operación de los Centros de Enseñanza Automovilística, el SICOV exigirá y registrará la validación de identidad tanto de

RESOLUCIÓN NÚMERO _____ DE _____

"Por medio de la cual se modifican las Resoluciones 5790 y 60832 de 2016 de la Superintendencia de Transporte y se introducen mejoras y medidas para fortalecer las capacidades de inspección, Vigilancia y Control a través de su Sistema de Control y Vigilancia para CEA, CIA y OTT" aspirantes como de instructores en los siguientes momentos y con los siguientes mecanismos específicos:

- a) **Al inicio y al final de cada sesión de clase teórica:** La validación se realizará obligatoriamente a través del cotejo biométrico de minucias dactilares contra las bases de datos de la RNEC. Esta validación se hará en los puntos de validación de identidad ubicados en el interior o exterior de los salones de clase.
- b) **Al inicio y al final de cada sesión de clase práctica:** La validación se realizará obligatoriamente a través de la tecnología de reconocimiento facial (selfie vs. template almacenado en el Abis del SICOV).
- c) **Al inicio y al final de cada evaluación teórica y/o práctica:** La validación se realizará obligatoriamente a través del cotejo biométrico de minucias dactilares contra las bases de datos de la RNEC, cuando estas evaluaciones apliquen conforme a la normatividad vigente.
- d) **Durante el desarrollo de las clases teóricas y prácticas:** La verificación de permanencia se realizará a través de reconocimiento facial. El Sistema de Control y Vigilancia deberá implementar mecanismos tecnológicos para verificar la permanencia continua de los usuarios del servicio y los instructores durante el desarrollo completo de cada sesión de clase o curso, tanto en modalidad presencial como virtual. Esta función es crucial para asegurar la participación efectiva en el proceso formativo y prevenir el abandono de las sesiones una vez realizada la validación inicial de identidad. El SICOV recabará y analizará en tiempo real la información de los participantes presentes en un aula o vehículo, realizando, como mínimo, un procedimiento de comprobación de permanencia por cada hora académica cursada. En caso de poder verificar la permanencia, se procederá con el procedimiento del literal e.
- e) **Procedimiento de revalidación por no detección de permanencia:** Cuando, durante una clase teórica o práctica, el sistema de verificación de permanencia no logre detectar a un aspirante o instructor, el SICOV lo requerirá inmediatamente para que, dentro de un plazo perentorio (cinco (5) minutos), realice un nuevo proceso de validación de identidad a través de uno de los dispositivos fijos o móviles dispuestos en el CEA, utilizando el mecanismo biométrico que corresponda según el tipo de clase: si es teórica, a través de cotejo de minucias dactilares contra la RNEC y si es práctica, a través de reconocimiento facial.

RESOLUCIÓN NÚMERO _____ DE _____

"Por medio de la cual se modifican las Resoluciones 5790 y 60832 de 2016 de la Superintendencia de Transporte y se introducen mejoras y medidas para fortalecer las capacidades de inspección, Vigilancia y Control a través de su Sistema de Control y Vigilancia para CEA, CIA y OTT"

2.5.8.2.7. Condicionamiento para el avance a la fase de capacitación práctica.

En adición a las funciones transversales, el Sistema de Control y Vigilancia implementará la siguiente regla de negocio específica para el proceso de capacitación en los Centros de Enseñanza Automovilística (CEA):

El SICOV habilitará en el sistema la opción de programación y realización de clases prácticas para un aspirante a conductor únicamente cuando verifique de manera automática que dicho aspirante ha cumplido con los siguientes requisitos previos:

a) Haber acumulado la totalidad de las horas del ciclo de capacitación teórica requeridas para la categoría de licencia de conducción a la que aspira, debiendo todas las sesiones teóricas estar clasificadas como "Cursadas" por el SICOV.

b) Haber aprobado la evaluación o los exámenes de conocimiento teórico correspondientes, cuando estos sean un prerrequisito para iniciar la fase práctica, conforme a la normatividad vigente y a los registros del SICOV.

El cumplimiento de estas condiciones será verificado automáticamente por el Sistema antes de permitir la programación de cualquier clase práctica.

2.5.8.2.8. Integración e interfaz de validación para el registro de información del servicio y certificados en el RUNT.

En adición a la función transversal sobre la interfaz de validación con el RUNT, para los Centros de Enseñanza Automovilística, el SICOV implementará las siguientes reglas y contenidos específicos:

El SICOV deberá disponer de un servicio de integración seguro y eficiente con el RUNT que permita que la información asociada a la prestación del servicio en el CEA, que se encuentre registrada en el SICOV, y cuyo reporte sea obligatorio hacer también en el Registro Único Nacional de Tránsito, pueda transmitirse de manera segura del primero al segundo, evitando reprocesamientos en el reporte de información en ambos sistemas.

La integración permitirá verificar automáticamente que el cargue de cada dato e información del servicio prestado, incluyendo cada clase realizada y/o certificado expedido por el organismo de apoyo, sólo se dé en los casos que el

RESOLUCIÓN NÚMERO _____ DE _____

"Por medio de la cual se modifican las Resoluciones 5790 y 60832 de 2016 de la Superintendencia de Transporte y se introducen mejoras y medidas para fortalecer las capacidades de inspección, Vigilancia y Control a través de su Sistema de Control y Vigilancia para CEA, CIA y OTT" usuario haya cumplido con la totalidad de los requisitos del proceso de capacitación monitoreados y validados por el SICOV.

Para ello, el software SICOV del operador del Sistema deberá homologarse ante el RUNT, cumpliendo los con los requisitos y condiciones técnicas de homologación y recertificación definidos por el Ministerio de Transporte.

La integración deberá garantizar que el RUNT reciba del SICOV, la siguiente información, como mínimo:

- a) La confirmación de la identidad del usuario registrado en SICOV (nombre completo y número de documento) al que se prestó el servicio.
- b) La información de la clase calificada en el Sistema como "Cursada", respecto del cual se desea hacer el cargue.
- c) El estado de la "Decisión de Certificación" del usuario dentro del SICOV.

Esta funcionalidad es esencial para asegurar que solo la información de las clases, cursos y certificados correspondientes a procesos formativos debidamente verificados por el SICOV sean inscritos en el RUNT para los fines legales correspondientes.

2.5.8.2.9. Proceso y contenido específico para la expedición de Certificados de Aptitud en Conducción (CAC).

En adición a la función transversal sobre la expedición de certificados, para los Centros de Enseñanza Automovilística, el SICOV implementará las siguientes reglas y contenidos específicos para la generación del **Certificado de Aptitud en Conducción (CAC)**:

1. **Condiciones para la habilitación:** El SICOV habilitará la funcionalidad para la expedición de un CAC a un aspirante específico si, y solo si, se han cumplido las siguientes condiciones acumulativas, verificadas y registradas en el Sistema:
 - a) La totalidad de las horas y sesiones del ciclo de capacitación teórico-práctico requeridas para la categoría de licencia de conducción solicitada han sido clasificadas como "Cursadas".

RESOLUCIÓN NÚMERO _____ DE _____

"Por medio de la cual se modifican las Resoluciones 5790 y 60832 de 2016 de la Superintendencia de Transporte y se introducen mejoras y medidas para fortalecer las capacidades de inspección, Vigilancia y Control a través de su Sistema de Control y Vigilancia para CEA, CIA y OTT"

b) El aspirante ha aprobado la evaluación o las evaluaciones de conocimiento teórico y práctico que sean exigibles para la respectiva categoría de licencia de conducción.

2. **Proceso de expedición formal:** Una vez cumplidas las condiciones, el SICOV habilitará la opción para que el personal del CEA debidamente autorizado proceda con la expedición formal del certificado. El Sistema deberá generar el certificado con las características de seguridad y contenido que defina la Superintendencia de Transporte, incluyendo un número único de identificación para su posterior registro en el RUNT y, de manera obligatoria, deberá ser **firmado digitalmente** por el representante legal del CEA y/o el personal autorizado para dicha expedición.

2.5.8.2.10. Gestión de plazos y caducidad del proceso de capacitación.

En adición a las funciones transversales, y para la correcta gestión del ciclo de capacitación en los Centros de Enseñanza Automovilística, el SICOV implementará las siguientes funcionalidades de control de plazos:

a) **Monitoreo de la vigencia del proceso:** El SICOV deberá estar parametrizado para monitorear el progreso de los aspirantes en el ciclo de capacitación teórico-práctica, en relación con el término máximo para su culminación, según lo previsto en la normatividad aplicable o, en su defecto, en los parámetros que establezca el Ministerio de Transporte mediante acto administrativo.

b) **Alertas preventivas de vencimiento:** El Sistema deberá generar alertas automáticas dirigidas al CEA, con una antelación de por lo menos diez (10) días hábiles, informando sobre la proximidad del vencimiento del plazo para que un usuario culmine su ciclo de capacitación.

c) **Inactivación automática del curso:** En caso de que un aspirante no culmine satisfactoriamente la totalidad del ciclo de capacitación teórico-práctica dentro del término máximo establecido, y siempre que no medie una causal de justificación válida y documentada, el SICOV procederá a inactivar automáticamente el registro de dicho curso. Para retomar su proceso de capacitación, el aspirante deberá iniciar un nuevo registro, sujeto a las condiciones vigentes en ese momento.

RESOLUCIÓN NÚMERO _____ DE _____

"Por medio de la cual se modifican las Resoluciones 5790 y 60832 de 2016 de la Superintendencia de Transporte y se introducen mejoras y medidas para fortalecer las capacidades de inspección, Vigilancia y Control a través de su Sistema de Control y Vigilancia para CEA, CIA y OTT"

2.5.8.2.11. Documentación mínima requerida en el repositorio para los CEA.

En desarrollo de lo dispuesto en el numeral transversal 2.5.7.1.11. sobre la gestión de conformidad documental, y sin perjuicio de otros que pueda exigir el Ministerio de Transporte, los Centros de Enseñanza Automovilística deberán cargar y mantener vigentes en el repositorio del SICOV, como mínimo, los siguientes documentos para acreditar su operación legal y continua, los cuales, por su trascendencia, se consideran críticos:

- a) Certificado de existencia y representación legal expedido por la Cámara de Comercio, que acredite su actividad económica principal y complementarias. Este deberá ser actualizado en el Sistema por parte de los CEA cada vez que sea modificado.
- b) Certificado de conformidad de organismo de certificación de producto vigente, así como los informes de recertificación y de seguimiento anual, que acrediten la conformidad con la norma técnica sectorial aplicable.
- c) Licencia de funcionamiento del establecimiento o establecimientos, expedida por la autoridad competente, cuando aplique según la normativa municipal o distrital.
- d) Acto administrativo de registro de los programas de formación de conductores ante la Secretaría de Educación competente.
- e) Póliza vigente de responsabilidad civil extracontractual que ampare los riesgos inherentes a la actividad de enseñanza.
- f) Constancia de registro en el RUNT (ID RUNT).

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.

2.5.8.2.12. Contenido específico del registro histórico de Certificados de Aptitud en Conducción (CAC).

En adición a la información general requerida en el numeral transversal 2.5.7.1.20. sobre la gestión del registro histórico de certificados, para los

RESOLUCIÓN NÚMERO _____ DE _____

"Por medio de la cual se modifican las Resoluciones 5790 y 60832 de 2016 de la Superintendencia de Transporte y se introducen mejoras y medidas para fortalecer las capacidades de inspección, Vigilancia y Control a través de su Sistema de Control y Vigilancia para CEA, CIA y OTT"

Centros de Enseñanza Automovilística, el registro histórico de cada Certificado de Aptitud en Conducción (CAC) expedido deberá incluir de manera obligatoria:

La(s) categoría(s) de la licencia de conducción para la(s) cual(es) se expidió el certificado de aptitud.

Interoperabilidad en casos de migración de información entre operadores SICOV: Para garantizar la consistencia de la información que debe reposar en el SICOV sobre los certificados de capacitación expedidos por cada CEA y la trazabilidad de la información del servicio prestado al usuario, en los términos aquí señalados, con el propósito de evitar vacíos de información en caso de que un CEA cambie de operador homologado; se exige la implementación de mecanismos de integración o interoperabilidad del Sistema para el intercambio seguro de dicha información.

La Superintendencia de Transporte definirá, en coordinación con los operadores homologados, estándares técnicos, protocolos y la información mínima a intercambiar para dar cumplimiento a esta función, durante el periodo de implementación, a través de la realización de mesas técnicas.

2.5.8.2.13. Contenido específico del registro histórico del proceso de capacitación.

En adición a la información general requerida en el numeral transversal 2.5.7.1.9. sobre la gestión del registro histórico del proceso de capacitación, para los Centros de Enseñanza Automovilística, el registro histórico de cada **sesión de clase práctica** deberá incluir de manera obligatoria:

a) La identificación del vehículo de enseñanza utilizado, incluyendo, como mínimo, su número de placa y el recorrido realizado.

2.5.8.2.14. Contenido específico de los informes para CEA.

En desarrollo de lo dispuesto en el numeral transversal 2.5.7.1.17. sobre las herramientas de autoconsulta, y sin perjuicio de otros indicadores que pueda definir la Superintendencia de Transporte, los informes operativos que el SICOV genere para los Centros de Enseñanza Automovilística (CEA) deberán incluir, como mínimo, las siguientes estadísticas y datos:

a) Número de aspirantes inscritos, matriculados y retirados del proceso de capacitación.

RESOLUCIÓN NÚMERO _____ DE _____

"Por medio de la cual se modifican las Resoluciones 5790 y 60832 de 2016 de la Superintendencia de Transporte y se introducen mejoras y medidas para fortalecer las capacidades de inspección, Vigilancia y Control a través de su Sistema de Control y Vigilancia para CEA, CIA y OTT"

b) Detalle de clases teóricas y prácticas impartidas, con la posibilidad de ser filtradas por instructor, vehículo y módulo temático.

c) Resultados agregados de las evaluaciones teóricas y prácticas, incluyendo tasas de aprobación por cada tipo de evaluación y por categoría de licencia.

d) Número y tipo (categoría de licencia) de los Certificados de Aptitud en Conducción (CAC) expedidos.

e) Indicadores de utilización de la capacidad instalada, detallando el uso de aulas, vehículos e instructores.

f) Alertas generadas por el SICOV ante el vencimiento de la vigencia o inexistencia de documentos que soporten el cumplimiento de requisitos críticos de operación del CEA.

2.5.8.2.15. Funcionalidades específicas de la aplicación móvil para el entorno CEA.

En adición a las capacidades generales descritas en el numeral transversal 2.5.7.1.22. sobre la aplicación móvil, para los usuarios de los Centros de Enseñanza Automovilística, la aplicación deberá ofrecer vistas y funcionalidades específicas que reflejen la naturaleza de su proceso de capacitación:

a) **Progreso en el ciclo de capacitación:** El usuario deberá poder consultar de manera clara e intuitiva su estado de avance general, visualizando el historial detallado de clases teóricas y prácticas que han sido clasificadas como "Cursadas" y aquellas que se encuentren pendientes.

b) **Gestión de clases prácticas:** La aplicación deberá facilitar la programación de clases prácticas, permitiendo al usuario visualizar la agenda y disponibilidad de los vehículos e instructores del CEA.

2.5.8.3. Funcionalidades particulares del SICOV para Centros Integrales de Atención y Organismos de Tránsito y Transporte

Introducción

Las funcionalidades que se describen a continuación son específicas para la operación de los Centros Integrales de Atención y los Organismos de Tránsito y

RESOLUCIÓN NÚMERO _____ DE _____

"Por medio de la cual se modifican las Resoluciones 5790 y 60832 de 2016 de la Superintendencia de Transporte y se introducen mejoras y medidas para fortalecer las capacidades de inspección, Vigilancia y Control a través de su Sistema de Control y Vigilancia para CEA, CIA y OTT"

Transporte que imparten cursos a infractores de las normas de tránsito. Estas funciones complementan o detallan las capacidades transversales descritas en el presente Capítulo del Anexo Técnico.

2.5.8.3.1. Gestión de pagos por el uso del SICOV

En adición a lo establecido en la función transversal sobre la gestión de pagos, en el caso de los CIA y OTT, el SICOV implementará las siguientes reglas específicas:

Modalidad de recaudo y costo de operación del SICOV:

Para la operación del SICOV en los cursos sobre normas de tránsito que se impartan de manera presencial y/o virtual (una vez estos sean reglamentados por el Ministerio de Transporte), será necesario que los CIA y OTT aseguren el pago al operador del Sistema por el servicio, conforme al esquema y condiciones que para el efecto se establezcan con el operador.

Para los cursos virtuales, la validación exitosa del pago por el servicio será condición técnica indispensable para que el Sistema genere y envíe al usuario el enlace o credenciales de acceso a la sala virtual o plataforma de capacitación.

2.5.8.3.2. Enrolamiento digital y validación documental para cursos virtuales

Para el caso de los cursos impartidos en modalidad virtual por los CIA y OTT, el SICOV deberá disponer de una funcionalidad de enrolamiento en línea que permita el registro remoto del infractor. En estos casos, la validación de identidad para el enrolamiento se realizará exclusivamente mediante tecnología de reconocimiento facial y tecnología de validación de autenticidad y vida de documento de identidad.

Para garantizar la seguridad de este proceso, el software del SICOV deberá emplear las tecnologías de Reconocimiento Óptico de Caracteres (OCR) y lectura de Zona de Lectura Mecánica (MRZ) que permitan escanear y validar la información del documento de identidad original presentado por el usuario a través de la cámara de su dispositivo.

El operador homologado deberá garantizar que esta tecnología cuente con capacidad de detección de vida (liveness detection) tanto de la persona como

RESOLUCIÓN NÚMERO _____ DE _____

"Por medio de la cual se modifican las Resoluciones 5790 y 60832 de 2016 de la Superintendencia de Transporte y se introducen mejoras y medidas para fortalecer las capacidades de inspección, Vigilancia y Control a través de su Sistema de Control y Vigilancia para CEA, CIA y OTT" del documento, asegurando que se trata de un usuario real y de un documento físico original, y no de una imagen, video o reproducción digital.

2.5.8.3.3. Integración con SIMIT y gestión de información de comparendos.

El Sistema de Control y Vigilancia deberá disponer de funcionalidades para integrarse o interoperar de manera segura y eficiente con el Sistema Integrado de Información sobre Multas y Sanciones por Infracciones de Tránsito (SIMIT), o el sistema que haga sus veces. Esta integración tiene como finalidad principal obtener la información de los comparendos que habilitan la realización de los cursos para infractores, calcular los beneficios asociados a la realización del curso, y llevar un registro completo del proceso.

Para todos los efectos de lo aquí dispuesto, se tendrá en cuenta lo dispuesto por el Ministerio de Transporte sobre la notificación por conducta concluyente, en aquellos casos en que un usuario acuda directamente al CIA/OTT antes que a la autoridad de tránsito que le impuso el comparendo.

1. Consulta y registro de información del comparendo:

- a) Como requisito previo a la inscripción formal del infractor al curso, el SICOV deberá consultar en el SIMIT, utilizando el número de documento de identidad del usuario y/o el número del comparendo, la información relevante de la infracción.
- b) Esta consulta deberá verificar, como mínimo, la existencia y estado del comparendo, el código y descripción de la infracción, la fecha de imposición y, de estar disponible, la fecha de su notificación.
- c) El SICOV registrará y asociará esta información verificada del comparendo al proceso del curso del usuario.

2. Cálculo automático de descuentos:

- a) A partir de la información obtenida del SIMIT (especialmente las fechas de imposición y notificación) y la fecha de realización efectiva del curso registrada en SICOV, el Sistema deberá calcular automáticamente el porcentaje de descuento sobre el valor de la multa al que el usuario tendría derecho, de estricta conformidad con los términos y plazos establecidos en el Código Nacional de Tránsito y la normatividad

RESOLUCIÓN NÚMERO _____ DE _____

"Por medio de la cual se modifican las Resoluciones 5790 y 60832 de 2016 de la Superintendencia de Transporte y se introducen mejoras y medidas para fortalecer las capacidades de inspección, Vigilancia y Control a través de su Sistema de Control y Vigilancia para CEA, CIA y OTT" complementaria, teniendo en cuenta para ello los efectos de figuras como la notificación por conducta concluyente, según los lineamientos impartidos por el Ministerio de Transporte.

b) El SICOV registrará tanto el porcentaje de descuento calculado como los datos base para dicho cálculo, y esta información será un componente indispensable del certificado de asistencia que se expida.

3. **Seguridad y fiabilidad de la interoperabilidad:** La comunicación e intercambio de información entre el SICOV y el SIMIT deberá realizarse a través de mecanismos de interoperabilidad seguros que garanticen la autenticidad, integridad y confidencialidad de los datos transmitidos. La operatividad de esta función del SICOV dependerá de la disponibilidad y calidad del servicio de consulta que provea el SIMIT.

2.5.8.3.4. Contenido específico del registro histórico de certificados de asistencia.

En adición a la información general requerida en el numeral transversal 2.5.7.1.20. sobre la gestión del registro histórico de certificados, para los CIA y OTT, el registro histórico de cada Certificado de Asistencia a un curso para infractores deberá incluir de manera obligatoria la información del comparendo que motivó la realización del curso (número y código de la infracción).

Adicionalmente, el registro histórico deberá distinguir la modalidad del curso (presencial o virtual). Para los cursos virtuales, se deberá almacenar la dirección IP de conexión del usuario, la ciudad y departamento desde donde se conectó, el tipo de dispositivo utilizado y los logs de conexión y desconexión a la plataforma de videoconferencia.

2.5.8.3.5. Contenido específico de los informes para CIA y OTT.

En desarrollo de lo dispuesto en el numeral transversal 2.5.7.1.17. sobre las herramientas de autoconsulta, y sin perjuicio de otros indicadores que pueda definir la Superintendencia de Transporte, los informes operativos que el SICOV genere para los CIA y OTT deberán incluir, como mínimo, las siguientes estadísticas y datos:

- a. Número de usuarios (infractores) inscritos.
- b. Número de cursos impartidos y distribución de estos por tipo de infracción.

RESOLUCIÓN NÚMERO _____ DE _____

"Por medio de la cual se modifican las Resoluciones 5790 y 60832 de 2016 de la Superintendencia de Transporte y se introducen mejoras y medidas para fortalecer las capacidades de inspección, Vigilancia y Control a través de su Sistema de Control y Vigilancia para CEA, CIA y OTT"

- c. Resultados agregados de las validaciones de identidad y permanencia, incluyendo tasas de fallos.
- d. Número de certificados de asistencia expedidos.
- e. Indicadores de utilización de la capacidad instalada (aulas e instructores).
- f. Alertas generadas por el SICOV ante el vencimiento de la vigencia o inexistencia de documentos que soporten el cumplimiento de requisitos críticos de operación del CIA u OTT.

Todos los informes y estadísticas mencionados deberán presentarse de manera desagregada, permitiendo visualizar la información exclusivamente para la modalidad presencial, exclusivamente para la modalidad virtual, y el consolidado de ambas.

2.5.8.3.6. Funcionalidades específicas de la aplicación móvil para el entorno CIA y OTT.

En adición a las capacidades generales descritas en el numeral transversal sobre la aplicación móvil, para los usuarios e instructores de los CIA y OTT, la aplicación deberá ofrecer vistas y funcionalidades específicas para el curso de infractores:

1. Funcionalidades para usuarios (infractores):

- a) Consultar la información del curso programado, su estado ("Cursado" o "No Cursado") y el motivo en caso de no haber sido cursado.
- b) Acceder a la agenda del CIA u OTT para la programación del curso.
- c) Recibir notificaciones y recordatorios sobre su curso y los requerimientos de validación de identidad.
- d) Acceder a la funcionalidad de valoración de la calidad del curso y del instructor.
- e) Para cursos virtuales, permitir el acceso al enlace de la sesión una vez superado el enrolamiento y la validación de identidad inicial, y servir como dispositivo de captura para la validación biométrica facial y de permanencia cuando el usuario realice el curso desde un equipo de escritorio sin cámara confiable.

2. Funcionalidades para instructores:

- a) Consultar su agenda personal de cursos programados en el SICOV.
- b) Recibir notificaciones y recordatorios sobre sus cursos asignados.

RESOLUCIÓN NÚMERO _____ DE _____

"Por medio de la cual se modifican las Resoluciones 5790 y 60832 de 2016 de la Superintendencia de Transporte y se introducen mejoras y medidas para fortalecer las capacidades de inspección, Vigilancia y Control a través de su Sistema de Control y Vigilancia para CEA, CIA y OTT"

c) Recibir información sobre los requerimientos de validación de identidad que se le aplicarán.

2.5.8.3.7. Contenido específico para la expedición de certificados de asistencia.

En adición a la función transversal sobre la expedición de certificados, para los CIA y OTT, el SICOV implementará las siguientes reglas y contenidos específicos para la generación del Certificado de asistencia al curso para infractores:

a) El certificado solo podrá ser habilitado para expedición si el curso ha sido clasificado como "Cursado" por el SICOV.

b) El certificado generado por el SICOV deberá incluir, además de los datos del usuario y del organismo, la información del descuento aplicable calculado por el sistema y los datos del comparendo asociado.

c) El certificado deberá ser firmado digitalmente por el representante legal del CIA u OTT y/o el personal autorizado para dicha expedición.

d) El certificado deberá indicar expresamente la modalidad en la que se impartió el curso (presencial o virtual), conforme a la información registrada en el SICOV.

2.5.8.3.8. Documentación mínima requerida en el repositorio para los CIA y OTT.

En desarrollo de lo dispuesto en el numeral transversal 2.5.7.1.11., los CIA y OTT deberán cargar y mantener vigentes en el repositorio del SICOV, como mínimo, los siguientes documentos para acreditar su operación legal y continua:

a) Certificado de existencia y representación legal expedido por la Cámara de Comercio.

b) Acto administrativo de la autoridad competente / constancia de registro activo en el RUNT que autoriza al organismo de apoyo u organismo de tránsito y transporte para impartir cursos a infractores de las normas de tránsito.

c) Certificado de conformidad de producto u organismo vigente, así como los informes de seguimiento anual.

d) Póliza vigente de responsabilidad civil extracontractual.

e) Documentación que acredite el cumplimiento de los requisitos de personal mínimo e idoneidad de los instructores, conforme a la normatividad vigente.

RESOLUCIÓN NÚMERO _____ DE _____

"Por medio de la cual se modifican las Resoluciones 5790 y 60832 de 2016 de la Superintendencia de Transporte y se introducen mejoras y medidas para fortalecer las capacidades de inspección, Vigilancia y Control a través de su Sistema de Control y Vigilancia para CEA, CIA y OTT"

f) Resolución de habilitación como casa-cárcel y/o escan del convenio con casa-cárcel vigente.

2.5.8.3.9. Proceso específico de validación de identidad y permanencia.

En adición a las funciones transversales, y para atender las características específicas de los cursos para infractores, el SICOV implementará un proceso de verificación de identidad en tres (3) momentos clave para cada usuario (infractor) e instructor. El cumplimiento satisfactorio de la totalidad de estas verificaciones será requisito indispensable para que el curso sea considerado válido.

a) En cursos presenciales:

1. **Verificación al inicio y al final del curso:** El mecanismo principal y obligatorio para la verificación de identidad tanto al inicio como al finalizar cada curso será el cotejo biométrico de la huella dactilar del individuo contra las bases de datos de la Registraduría Nacional del Estado Civil (RNEC), utilizando lectores de huella especializados con funcionalidad certificada de detección de vida (liveness detection).
2. **Verificación de permanencia durante el curso:** Para verificar la permanencia, el SICOV realizará por lo menos un (1) procedimiento de validación aleatorio, en cualquier momento no predecible durante el desarrollo del curso. Este mecanismo será el reconocimiento facial, utilizando un sistema de captura visual panorámica del aula para identificar a los asistentes.
3. **Procedimiento de revalidación:** Si como resultado de la verificación panorámica, un participante no es detectado, el SICOV lo requerirá inmediatamente para que, en un plazo perentorio de cinco (5) minutos, realice una nueva validación de su identidad mediante el cotejo biométrico de su huella dactilar directamente contra las bases de datos de la RNEC. El cumplimiento exitoso de esta revalidación se considerará como la superación del requisito de permanencia.

b) En cursos virtuales:

1. **Inicio y fin:** Validación obligatoria mediante reconocimiento facial con prueba de vida (liveness detection) contra el patrón biométrico del usuario (template) o contra la base de datos de la RNEC (cuando esté disponible el servicio).

RESOLUCIÓN NÚMERO _____ DE _____

"Por medio de la cual se modifican las Resoluciones 5790 y 60832 de 2016 de la Superintendencia de Transporte y se introducen mejoras y medidas para fortalecer las capacidades de inspección, Vigilancia y Control a través de su Sistema de Control y Vigilancia para CEA, CIA y OTT"

2. **Permanencia:** El SICOV realizará capturas aleatorias y silenciosas del rostro del usuario frente a la cámara durante la sesión.
3. **Procedimiento de revalidación:** Si el sistema detecta ausencia del usuario o presunta suplantación de identidad, lo requerirá para que haga una re-validación de identidad inmediatamente en un plazo perentorio de cinco (5) minutos. El cumplimiento exitoso de esta revalidación se considerará como la superación del requisito de permanencia. Si no se realiza este procedimiento el curso se tendrá por no realizado.

2.5.8.3.10. Correspondencia entre el contenido del curso y la infracción.

Para asegurar la finalidad pedagógica de los cursos para infractores, el SICOV deberá facilitar la trazabilidad de la pertinencia del contenido impartido. Para ello, el Sistema deberá:

- a) Permitir al CIA u OTT registrar, para cada curso programado, las temáticas principales que se abordarán.
- b) Asegurar que dichas temáticas tengan correspondencia con la naturaleza de la infracción cometida por el usuario, conforme a los lineamientos que establezca la Agencia Nacional de Seguridad Vial (ANSV) o la autoridad competente.
- c) Generar los reportes que permitan a la Superintendencia de Transporte supervisar esta correspondencia.

2.5.8.3.11. Contenido específico de la integración e interfaz de validación con RUNT.

En adición a la función transversal sobre la integración e interfaz de validación con el RUNT, para la verificación de los Certificados de Asistencia expedidos por los CIA y OTT, la integración del SICOV con el RUNT deberá incluir, además de la confirmación de identidad y el estado de la "Decisión de certificación", el siguiente dato específico:

La información del comparendo que motivó la realización del curso (número y código de la infracción), cuando esta sea relevante para el registro del beneficio en el RUNT.

2.5.8.3.12. Control de capacidad instalada para cursos virtuales.

RESOLUCIÓN NÚMERO _____ DE _____

"Por medio de la cual se modifican las Resoluciones 5790 y 60832 de 2016 de la Superintendencia de Transporte y se introducen mejoras y medidas para fortalecer las capacidades de inspección, Vigilancia y Control a través de su Sistema de Control y Vigilancia para CEA, CIA y OTT"

En cumplimiento de lo dispuesto en el parágrafo 3 del artículo 136 de la Ley 769 de 2002, el SICOV aplicará un límite técnico a la programación de cursos virtuales. El sistema no permitirá programar, por sesión, un número de alumnos que supere el número de usuarios que el CIA puede atender presencialmente de acuerdo con su capacidad instalada, para lo cual se tendrá en cuenta lo dispuesto en este Anexo.

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 vigilar y controlar 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.

RESOLUCIÓN NÚMERO _____ DE _____

"Por medio de la cual se modifican las Resoluciones 5790 y 60832 de 2016 de la Superintendencia de Transporte y se introducen mejoras y medidas para fortalecer las capacidades de inspección, Vigilancia y Control a través de su Sistema de Control y Vigilancia para CEA, CIA y OTT"

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:

RESOLUCIÓN NÚMERO _____ DE _____

"Por medio de la cual se modifican las Resoluciones 5790 y 60832 de 2016 de la Superintendencia de Transporte y se introducen mejoras y medidas para fortalecer las capacidades de inspección, Vigilancia y Control a través de su Sistema de Control y Vigilancia para CEA, CIA y OTT"

- 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.

RESOLUCIÓN NÚMERO _____ DE _____

"Por medio de la cual se modifican las Resoluciones 5790 y 60832 de 2016 de la Superintendencia de Transporte y se introducen mejoras y medidas para fortalecer las capacidades de inspección, Vigilancia y Control a través de su Sistema de Control y Vigilancia para CEA, CIA y OTT"

- **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.

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 con 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 CEA, CIA y OTT para el funcionamiento del software SICOV

Los organismos de apoyo al tránsito 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 equipos, 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

RESOLUCIÓN NÚMERO _____ DE _____

"Por medio de la cual se modifican las Resoluciones 5790 y 60832 de 2016 de la Superintendencia de Transporte y se introducen mejoras y medidas para fortalecer las capacidades de inspección, Vigilancia y Control a través de su Sistema de Control y Vigilancia para CEA, CIA y OTT"

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 del SICOV.

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 Enseñanza Automovilística, Centro Integral de Atención y Organismo de Tránsito y Transporte.

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 CEA, CIA y OTT 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).

RESOLUCIÓN NÚMERO _____ DE _____

"Por medio de la cual se modifican las Resoluciones 5790 y 60832 de 2016 de la Superintendencia de Transporte y se introducen mejoras y medidas para fortalecer las capacidades de inspección, Vigilancia y Control a través de su Sistema de Control y Vigilancia para CEA, CIA y OTT"

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	

RESOLUCIÓN NÚMERO _____ DE _____

"Por medio de la cual se modifican las Resoluciones 5790 y 60832 de 2016 de la Superintendencia de Transporte y se introducen mejoras y medidas para fortalecer las capacidades de inspección, Vigilancia y Control a través de su Sistema de Control y Vigilancia para CEA, CIA y OTT"

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

RESOLUCIÓN NÚMERO _____ DE _____

"Por medio de la cual se modifican las Resoluciones 5790 y 60832 de 2016 de la Superintendencia de Transporte y se introducen mejoras y medidas para fortalecer las capacidades de inspección, Vigilancia y Control a través de su Sistema de Control y Vigilancia para CEA, CIA y OTT"

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 CEA, CIA y OTT para el enrolamiento inicial del personal y los usuarios servicio, así como en **(ii)** los puntos fijos de validación de identidad ubicados dentro y/o fuera de las aulas en las que se dicten clases teóricas y cursos, 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:

Deberá permitir la captura de fotografías para el enrolamiento inicial del personal y usuarios del organismo de apoyo al tránsito y 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.

2.5.10.1.3. Cámara fija de alta definición tipo domo o similar:

Este dispositivo permitirá capturar fotografías y/o secuencias de video cortas que permitan hacer validación de identidad de asistentes en recintos cerrados. Deberán reunir los siguientes requisitos:

- Con sensor digital de alta definición y componentes ópticos que generen imágenes nítidas, para la captura automática de fotografías en recintos cerrados (aulas donde se dicten clases teóricas y/o cursos). Deberán ser instaladas estratégicamente en las aulas del establecimiento del CEA, CIA y OTT.

RESOLUCIÓN NÚMERO _____ DE _____

"Por medio de la cual se modifican las Resoluciones 5790 y 60832 de 2016 de la Superintendencia de Transporte y se introducen mejoras y medidas para fortalecer las capacidades de inspección, Vigilancia y Control a través de su Sistema de Control y Vigilancia para CEA, CIA y OTT"

- **Tecnología y estándares:** Debe ser compatible con la tecnología de reconocimiento facial descrita en el presente Anexo Técnico.
- **Especificaciones técnicas mínimas:**
 - o Resolución Mínima: Full HD (1080p), ideal: 4k
 - o FPS: Mínimo 25fps en 1080
 - o Iluminación: WDR (Wide Dynamics Range) y bajo ruido en baja luz
 - o Campo de visión: Horizontal >80°, o lente varifocal para ajustar
 - o Procesamiento: Edge AI o Servidor con capacidad de procesamiento facial 1:N
 - o Compatibilidad: SDKs o integración con Motores Face++, Cognitec, NEC o software open source (FaceNet, Dlib, etc)

2.5.10.1.4. Dispositivos móviles para la validación de identidad:

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:

- En la recepción del establecimiento.
- **En recintos de clases teóricas y cursos:** En puntos estratégicos del establecimiento o sede del organismo (interior o exterior de las aulas), para realizar la validación de identidad de los asistentes al inicio y al final de las clases teóricas y cursos.
- **En vehículos de clases prácticas y/o evaluaciones prácticas:** Para la validación de identidad durante las actividades en movimiento.

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

RESOLUCIÓN NÚMERO _____ DE _____

"Por medio de la cual se modifican las Resoluciones 5790 y 60832 de 2016 de la Superintendencia de Transporte y se introducen mejoras y medidas para fortalecer las capacidades de inspección, Vigilancia y Control a través de su Sistema de Control y Vigilancia para CEA, CIA y OTT" 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 organismo de apoyo (CEA, CIA, OTT), estos dispositivos móviles deberán estar acompañados adicionalmente de un huellero (lector biométrico especializado) preferiblemente 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).

5. Flexibilidad de instalación: Estos puntos podrán instalarse en el interior o exterior de las aulas/recintos a conveniencia, en función de la infraestructura física disponible en el establecimiento y la optimización de costos.

Estos puntos son indispensables para la validación de identidad de usuarios e instructores al inicio y al final de cada sesión.

2.5.10.1.5. Pad de firmas digitalizador

Es el dispositivo para la captura de la firma manuscrita digitalizada de los usuarios y personal del organismo de apoyo.

RESOLUCIÓN NÚMERO _____ DE _____

"Por medio de la cual se modifican las Resoluciones 5790 y 60832 de 2016 de la Superintendencia de Transporte y se introducen mejoras y medidas para fortalecer las capacidades de inspección, Vigilancia y Control a través de su Sistema de Control y Vigilancia para CEA, CIA y OTT"

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.

2.5.10.1.6. Infraestructura descentralizada para el reconocimiento facial:

Los proveedores 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 CEA, 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 CEA, CIA y OTT.

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

RESOLUCIÓN NÚMERO _____ DE _____

"Por medio de la cual se modifican las Resoluciones 5790 y 60832 de 2016 de la Superintendencia de Transporte y se introducen mejoras y medidas para fortalecer las capacidades de inspección, Vigilancia y Control a través de su Sistema de Control y Vigilancia para CEA, CIA y OTT"

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

2.5.10.1.6.1. 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.

2.5.10.1.6.2. NAS

Requisitos mínimos:

- Bahías: 6
- Procesador: Quad Core AMD Ryzen ó Intel Core I5 ó I7 Compatible (ó Superior)
- Memoria RAM: 16 GB expandible

2.5.10.1.6.3. Switches de red administrables:

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

RESOLUCIÓN NÚMERO _____ DE _____

"Por medio de la cual se modifican las Resoluciones 5790 y 60832 de 2016 de la Superintendencia de Transporte y se introducen mejoras y medidas para fortalecer las capacidades de inspección, Vigilancia y Control a través de su Sistema de Control y Vigilancia para CEA, CIA y OTT"

- 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).

2.5.10.1.6.4. 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 estas UPS se deben conectar y se debe soportar el rack de comunicaciones que contiene los equipos que integran el Sistema de Control y Vigilancia para los CEA, CIA .

RESOLUCIÓN NÚMERO _____ DE _____

"Por medio de la cual se modifican las Resoluciones 5790 y 60832 de 2016 de la Superintendencia de Transporte y se introducen mejoras y medidas para fortalecer las capacidades de inspección, Vigilancia y Control a través de su Sistema de Control y Vigilancia para CEA, CIA y OTT"

2.5.10.1.6.5. Rack de equipos:

Con las siguientes características mínimas:

- Rack de piso, tipo metálico con pintura electrostática, con llave y con rodachinas.
- Altura mínima de 1,50 m, 24 unidades de rack, suficiente para alojar la Workstation, NAS, UPS y equipos de comunicaciones con holgura para ventilación.
- Compuerta de seguridad y alarma antivandálica.

2.5.10.2. Software y componentes de software especializados requeridos para el funcionamiento del software SICOV CEA, CIA y OTT.

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 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 contra documento, y
- Validación de identidad simultánea de un número plural de personas en recintos cerrados.

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

RESOLUCIÓN NÚMERO _____ DE _____

"Por medio de la cual se modifican las Resoluciones 5790 y 60832 de 2016 de la Superintendencia de Transporte y se introducen mejoras y medidas para fortalecer las capacidades de inspección, Vigilancia y Control a través de su Sistema de Control y Vigilancia para CEA, CIA y OTT"

El servicio debe tener mínimo las siguientes características y componentes técnicos:

- 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.

Componentes técnicos:

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

1. **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).

Validaciones de identidad antes y al cierre de la sesión:

RESOLUCIÓN NÚMERO _____ DE _____

"Por medio de la cual se modifican las Resoluciones 5790 y 60832 de 2016 de la Superintendencia de Transporte y se introducen mejoras y medidas para fortalecer las capacidades de inspección, Vigilancia y Control a través de su Sistema de Control y Vigilancia para CEA, CIA y OTT"

Para la validación de identidad de los usuarios antes y después de la clase o curso, en los términos planteados 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** (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 algoritmo 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 $\Delta T \geq 12$ 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.

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 (MRZ 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.

RESOLUCIÓN NÚMERO _____ DE _____

"Por medio de la cual se modifican las Resoluciones 5790 y 60832 de 2016 de la Superintendencia de Transporte y se introducen mejoras y medidas para fortalecer las capacidades de inspección, Vigilancia y Control a través de su Sistema de Control y Vigilancia para CEA, CIA y OTT"

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 CEA, CIA y OTT, 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 y cámaras:

Para gestionar la geolocalización de los equipos de cómputo fijos y las cámaras empleados en el organismo de apoyo para la prestación del servicio, el operador homologado deberá contar con una solución integral de gestión de geolocalización de equipos de cómputo que sea segura y esté soportada por tecnologías eficientes, de tal manera que permita hacer seguimiento permanente a los dispositivos empleados para ello.

Como requisitos mínimos, se describen a continuación las características técnicas de sistemas que reúnen las condiciones mínimas esperadas del funcionamiento de la tecnología de geoposición deseada:

La solución debe funcionar con 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.

Características mínimas de los componentes esperados:

- a) **Etiqueta o tamper bluetooth** con botón antimanipulación para control de activos (equipos de cómputo y cámaras) 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:

RESOLUCIÓN NÚMERO _____ DE _____

"Por medio de la cual se modifican las Resoluciones 5790 y 60832 de 2016 de la Superintendencia de Transporte y se introducen mejoras y medidas para fortalecer las capacidades de inspección, Vigilancia y Control a través de su Sistema de Control y Vigilancia para CEA, CIA y OTT"

- 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 permitir conectarse por bluetooth a un gateway o puerta de enlace.
- Debe garantizar la inalterabilidad.

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 tampo 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

RESOLUCIÓN NÚMERO _____ DE _____

"Por medio de la cual se modifican las Resoluciones 5790 y 60832 de 2016 de la Superintendencia de Transporte y se introducen mejoras y medidas para fortalecer las capacidades de inspección, Vigilancia y Control a través de su Sistema de Control y Vigilancia para CEA, CIA y OTT"

- 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)

2.5.10.2.6. Software para la de identificación de geoposición (GPS) de vehículos (CEA):

Con el fin de gestionar la geolocalización de los vehículos de enseñanza de los CEA para la realización de las clases y evaluaciones de práctica, el homologado del SICOV deberá contar con una solución integral de gestión para su geolocalización, que sea segura y esté soportada por tecnologías eficientes, de tal manera que permita hacer seguimiento permanente a los dispositivos empleados para ello.

Como requisitos mínimos, se describen a continuación las características técnicas de sistemas que reúnen las condiciones mínimas esperadas del funcionamiento de la tecnología de geoposición deseada:

La solución debe contar con tres componentes: (i) una etiqueta adhesiva de control de activos, (ii) un gateway o puerta de enlace y (iii) un software o

RESOLUCIÓN NÚMERO _____ DE _____

"Por medio de la cual se modifican las Resoluciones 5790 y 60832 de 2016 de la Superintendencia de Transporte y se introducen mejoras y medidas para fortalecer las capacidades de inspección, Vigilancia y Control a través de su Sistema de Control y Vigilancia para CEA, CIA y OTT" plataforma de gestión y control, que reúnan como mínimo las siguientes características:

Este sistema permitirá llevar la trazabilidad precisa de la geoposición de todos los vehículos durante toda la capacitación, permitiendo rastrear y enviar coordenadas geográficas de los recorridos.

- a. **Etiqueta o Tamper Bluetooth con botón antimanipulación:** para identificación y control de los vehículos, que deben ser instalados dentro del vehículo en una superficie plana y limpia. En el caso de ser removido a la fuerza generará una señal de alarma a un Gateway ubicado también dentro del mismo vehículo, dicho componente deberá tener las siguientes especificaciones de fábrica como mínimo:
 - Conexión - Bluetooth LE 5.0
 - Botón anti manipulación 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 permitir conectarse por Bluetooth a un Gateway o puerta de enlace.
- b. **Gateway o puerta de enlace Móvil LTE para exteriores:** Es un dispositivo que funciona como puerta de enlace con las etiquetas o tampers (descritos en el literal anterior) para comunicarse a través de Bluetooth instalados en cada vehículo, con el fin de recopilar datos a través de bluetooth y el monitoreo continuo de la(s) etiqueta(S), en el caso de ser manipulados o no identificados dentro del vehículo, generará una alarma al software o plataforma de gestión. Dicho Gateway deberá tener las siguientes características como mínimo:

Especificaciones

- Edge Computing y filtrado de datos Bluetooth
- Almacenamiento de datos sin conexión y reconexión automática
- LTE-M / NB-IoT/ 4G Cat.1
- GPS en tiempo real

RESOLUCIÓN NÚMERO _____ DE _____

"Por medio de la cual se modifican las Resoluciones 5790 y 60832 de 2016 de la Superintendencia de Transporte y se introducen mejoras y medidas para fortalecer las capacidades de inspección, Vigilancia y Control a través de su Sistema de Control y Vigilancia para CEA, CIA y OTT"

- Detección de encendido y entrada digital
- Seguridad de datos (SSL/TLS/ MQTT)
- Compatible con: Plataformas en la nube de terceros: AWS/Azure,Google, IBM.
- Batería de litio recargable para resistencia a altas temperaturas.
- Fuentes de Alimentación: del vehículo (8V-52V), encendedor del coche, adaptador CC de 12V, panel solar (12V)
- Ahorro de energía / modos de funcionamiento del disparador cambio automático
- Protección: Clasificación IP68
- Sensor: Acelerómetro (detección de movimiento) /Sensor de temperatura/barómetro
- Temperatura de Funcionamiento: -20°C ~ 70°C
- Se podrán presentar otras opciones de Plataformas de Gestión de Identificación y Georreferenciación de Vehículos y de equipos de cómputo similares, y serán evaluados, avalados o rechazados por parte de la Supertransporte o a quien esta delegue.

Consideraciones adicionales:

- El Representante Legal del CEA, CIA u OTT será responsable de la buena utilización del sistema de geo-posición, de acuerdo con las recomendaciones del proveedor autorizado, para evitar manipulación o daños.
- **Actualización y envío de información:** Deberá permitir la actualización máxima de la geo-referenciación, comunicación celular y/o satelital. La marcación del posicionamiento interno y el envío de la información de ubicación al centro de control y la plataforma de monitoreo se realizarán con una frecuencia mínima de cada 60 minutos, incluyendo la identificación del PC, dirección MAC y número de serie de la tarjeta madre asociada.
- **Compatibilidad:** Compatibilidad con los prestadores de servicios móviles de comunicación en cuanto a tecnología, cobertura y disponibilidad requerida en el mercado.

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

RESOLUCIÓN NÚMERO _____ DE _____

"Por medio de la cual se modifican las Resoluciones 5790 y 60832 de 2016 de la Superintendencia de Transporte y se introducen mejoras y medidas para fortalecer las capacidades de inspección, Vigilancia y Control a través de su Sistema de Control y Vigilancia para CEA, CIA y OTT" 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 proveedores homologados del SICOV por la Superintendencia de Transporte deberán:

- Mantener actualizado y reportar el equipamiento tecnológico desplegado en los CEA, CIA y OTT, 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 y recibo a satisfacción 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

RESOLUCIÓN NÚMERO _____ DE _____

"Por medio de la cual se modifican las Resoluciones 5790 y 60832 de 2016 de la Superintendencia de Transporte y se introducen mejoras y medidas para fortalecer las capacidades de inspección, Vigilancia y Control a través de su Sistema de Control y Vigilancia para CEA, CIA y OTT"

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 Enseñanza Automovilística, Centros Integrales de Atención y Organismos de Tránsito y Transporte a los que el 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 y según las necesidades 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 Enseñanza Automovilística, dos (2) Centros Integrales de Atención y dos (2) Organismos de Tránsito y Transporte a los que el proveedor homologado desee prestar el servicio 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.

RESOLUCIÓN NÚMERO _____ DE _____

"Por medio de la cual se modifican las Resoluciones 5790 y 60832 de 2016 de la Superintendencia de Transporte y se introducen mejoras y medidas para fortalecer las capacidades de inspección, Vigilancia y Control a través de su Sistema de Control y Vigilancia para CEA, CIA y OTT"

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, control de permanencia, expedición de certificados, interoperabilidad, etc.).
- La correcta implementación y operación de los **dispositivos y tecnologías en los organismos de apoyo** (lectores, capturadores, computadores, dispositivos vehiculares), 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 y permanencia de usuarios e instructores.
- Verificaciones de la trazabilidad y geolocalización de operaciones.
- Pruebas de resistencia del sistema ante intentos de vulneración o frustración de funcionalidades.

RESOLUCIÓN NÚMERO _____ DE _____

"Por medio de la cual se modifican las Resoluciones 5790 y 60832 de 2016 de la Superintendencia de Transporte y se introducen mejoras y medidas para fortalecer las capacidades de inspección, Vigilancia y Control a través de su Sistema de Control y Vigilancia para CEA, CIA y OTT"

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.

2.5.11.4. Consecuencias de incumplimientos detectado en visita u otras 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 revocatoria de la autorización concedida.
- 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 (CPD-Analítico) Y Módulo de Consulta, IVC e Inteligencia de Negocio

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 CEA, CIA y OTT y del SICOV.

RESOLUCIÓN NÚMERO _____ DE _____

"Por medio de la cual se modifican las Resoluciones 5790 y 60832 de 2016 de la Superintendencia de Transporte y se introducen mejoras y medidas para fortalecer las capacidades de inspección, Vigilancia y Control a través de su Sistema de Control y Vigilancia para CEA, CIA y OTT"

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 CEA, CIA y OTT.

2.5.12.1. Arquitectura y condiciones de infraestructura del CPD-Analítico

El CPD-Analítico 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 deberá estar conformado obligatoriamente por dos sitios físicos independientes:

- Un Centro de Procesamiento Analítico Principal (**CPD-A**).
- Un Centro Alternativo 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 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

RESOLUCIÓN NÚMERO _____ DE _____

"Por medio de la cual se modifican las Resoluciones 5790 y 60832 de 2016 de la Superintendencia de Transporte y se introducen mejoras y medidas para fortalecer las capacidades de inspección, Vigilancia y Control a través de su Sistema de Control y Vigilancia para CEA, CIA y OTT" 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 entre el CPD-A y el CAPD-A.
- **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):

RESOLUCIÓN NÚMERO _____ DE _____

"Por medio de la cual se modifican las Resoluciones 5790 y 60832 de 2016 de la Superintendencia de Transporte y se introducen mejoras y medidas para fortalecer las capacidades de inspección, Vigilancia y Control a través de su Sistema de Control y Vigilancia para CEA, CIA y OTT"

- 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):
 - o **Cinco (5) minutos** para datos transaccionales críticos (disponibilidad, validación biométrica, recaudo).
 - o **Una (1) hora** para la totalidad de la operación detallada (clases, evidencias, alertas, información de vehículos e instructores).
 - o **Diaria** para datos históricos consolidados y reportes estadísticos agregados.

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 exclusivo, 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.
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 NÚMERO _____ DE _____

"Por medio de la cual se modifican las Resoluciones 5790 y 60832 de 2016 de la Superintendencia de Transporte y se introducen mejoras y medidas para fortalecer las capacidades de inspección, Vigilancia y Control a través de su Sistema de Control y Vigilancia para CEA, CIA y OTT" 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 y agregada de los organismos de apoyo, 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 de capacitación y cursos 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 CEA, 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.

RESOLUCIÓN NÚMERO _____ DE _____

"Por medio de la cual se modifican las Resoluciones 5790 y 60832 de 2016 de la Superintendencia de Transporte y se introducen mejoras y medidas para fortalecer las capacidades de inspección, Vigilancia y Control a través de su Sistema de Control y Vigilancia para CEA, CIA y OTT"

- 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 CEA, CIA y OTT 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 (i) 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:

RESOLUCIÓN NÚMERO _____ DE _____

"Por medio de la cual se modifican las Resoluciones 5790 y 60832 de 2016 de la Superintendencia de Transporte y se introducen mejoras y medidas para fortalecer las capacidades de inspección, Vigilancia y Control a través de su Sistema de Control y Vigilancia para CEA, CIA y OTT"

- **CEA, CIA y OTT con medidas:** 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 RUNT, o no, con base en la información disponible para el efecto.
- **Información de servicios afectados:** Listados de todos los servicios a usuarios que, habiendo sido pagados (PIN generado y consumido), no hayan culminado su prestación o no hayan sido registrados en el SICOV (con el enrolamiento) al momento de la ejecución de la medida adoptada por la entidad.
- **Datos del usuario y del servicio:** Incluir la información de los usuarios (nombre, cédula, etc.) de los servicios activos afectados con la ejecución de la medida y del servicio en sí mismo.
- **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 CEA, CIA u OTT 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 CEA, CIA y OTT a necesidad.

El Sistema deberá permitir la consulta y generación de informes sobre la operación de cualquier CEA, CIA u OTT, 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

RESOLUCIÓN NÚMERO _____ DE _____

"Por medio de la cual se modifican las Resoluciones 5790 y 60832 de 2016 de la Superintendencia de Transporte y se introducen mejoras y medidas para fortalecer las capacidades de inspección, Vigilancia y Control a través de su Sistema de Control y Vigilancia para CEA, CIA y OTT"

SICOV del CEA, CIA u OTT, 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 CEA, CIA y OTT.**

El Sistema deberá permitir hacer una consulta al registro que debe existir con la información de las visitas realizadas por parte de los operadores homologados a CEA, CIA y OTT 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 CEA, CIA y OTT.** 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 CEA, CIA y OTT.

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.

RESOLUCIÓN NÚMERO _____ DE _____

"Por medio de la cual se modifican las Resoluciones 5790 y 60832 de 2016 de la Superintendencia de Transporte y se introducen mejoras y medidas para fortalecer las capacidades de inspección, Vigilancia y Control a través de su Sistema de Control y Vigilancia para CEA, CIA y OTT"

- 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.

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 CEA, CIA y OTT como información, evidencias y alertas, al igual que para aquella información necesari
- Actualización diaria para los datos operativos históricos y reportes estadísticos agregados, cumpliendo los ANS que la Superintendencia determine.

RESOLUCIÓN NÚMERO _____ DE _____

"Por medio de la cual se modifican las Resoluciones 5790 y 60832 de 2016 de la Superintendencia de Transporte y se introducen mejoras y medidas para fortalecer las capacidades de inspección, Vigilancia y Control a través de su Sistema de Control y Vigilancia para CEA, CIA y OTT"

2.5.12.4. 2.5.12.3. Subsistema ABIS y capacidades de Inteligencia Artificial

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

1. **Subsistema ABIS (Automated Biometric Identification System):** Conforme a lo descrito en el capítulo 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.

2.5.12.4. Seguridad, licenciamiento y soporte del CPD-Analítico

- **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 1.3).
- **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.

RESOLUCIÓN NÚMERO _____ DE _____

"Por medio de la cual se modifican las Resoluciones 5790 y 60832 de 2016 de la Superintendencia de Transporte y se introducen mejoras y medidas para fortalecer las capacidades de inspección, Vigilancia y Control a través de su Sistema de Control y Vigilancia para CEA, CIA y OTT"

2.5.12.4. 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 forense por parte de la Entidad.

2.5.12.5. 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

RESOLUCIÓN NÚMERO _____ DE _____

"Por medio de la cual se modifican las Resoluciones 5790 y 60832 de 2016 de la Superintendencia de Transporte y se introducen mejoras y medidas para fortalecer las capacidades de inspección, Vigilancia y Control a través de su Sistema de Control y Vigilancia para CEA, CIA y OTT"

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.

2.6. 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 la 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

AUDITORÍAS DEL SICOV

3. AUDITORÍAS A LOS PROVEEDORES HOMOLOGADOS DEL SICOV

3.1. Objetivo de las auditorías

RESOLUCIÓN NÚMERO _____ DE _____

"Por medio de la cual se modifican las Resoluciones 5790 y 60832 de 2016 de la Superintendencia de Transporte y se introducen mejoras y medidas para fortalecer las capacidades de inspección, Vigilancia y Control a través de su Sistema de Control y Vigilancia para CEA, CIA y OTT"

Las auditorías al Sistema de Control y Vigilancia serán realizadas por terceros y tienen como objetivo primordial verificar y certificar de manera independiente el cumplimiento permanente de los requisitos técnicos, tecnológicos y de seguridad establecidos en el presente Anexo Técnico y las demás disposiciones complementarias. Buscan asegurar la confidencialidad, integridad y disponibilidad, entre otros, de la información procesada por el SICOV, así como la conformidad de su operación con los niveles de servicio y las políticas definidas por la Superintendencia de Transporte.

Las directrices, 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

El SICOV y sus proveedores homologados, así como las instalaciones y procesos relacionados con su operación (incluyendo Centros de Procesamiento de Datos, Centros de Operaciones de Seguridad y hardware y software instalados en los organismos de apoyo), serán objeto de auditorías periódicas, con una frecuencia mínima de una auditoría cada (2) dos 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, 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:

RESOLUCIÓN NÚMERO _____ DE _____

"Por medio de la cual se modifican las Resoluciones 5790 y 60832 de 2016 de la Superintendencia de Transporte y se introducen mejoras y medidas para fortalecer las capacidades de inspección, Vigilancia y Control a través de su Sistema de Control y Vigilancia para CEA, CIA y OTT"

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.

3.6. Consecuencias del incumplimiento de las obligaciones en auditoría

El incumplimiento de las obligaciones establecidas en este capítulo, la reincidencia en hallazgos críticos o la no subsanación oportuna de no conformidades, podrá dar lugar a la imposición de medidas administrativas, la aplicación de restricciones en el uso del SICOV y, en casos graves, a la revocatoria de la homologación, sin perjuicio de las demás acciones legales a que haya lugar. En todo caso se tendrán en cuenta las disposiciones y lineamiento que la Superintendencia defina y las consecuencias serán las mismas previstas como consecuencias del incumplimientos detectado en visitas y/o en ejercicios de verificación de cumplimiento de obligaciones por parte de la entidad.

3.7. Condiciones de realización de las auditorías

Los parámetros de realización de las auditorías serán precisados por el Comité Técnico y Operativo para el Fortalecimiento del SICOV.

TÍTULO 4

ACUERDOS DE NIVELES DE SERVICIO Y OBLIGACIONES DE LAS PARTES

4.1. ACUERDOS DE NIVELES DE SERVICIO

RESOLUCIÓN NÚMERO _____ DE _____

"Por medio de la cual se modifican las Resoluciones 5790 y 60832 de 2016 de la Superintendencia de Transporte y se introducen mejoras y medidas para fortalecer las capacidades de inspección, Vigilancia y Control a través de su Sistema de Control y Vigilancia para CEA, CIA y OTT"

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 módulo de consulta 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.

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 la radicación/5	98 %

RESOLUCIÓN NÚMERO _____ DE _____

"Por medio de la cual se modifican las Resoluciones 5790 y 60832 de 2016 de la Superintendencia de Transporte y se introducen mejoras y medidas para fortalecer las capacidades de inspección, Vigilancia y Control a través de su Sistema de Control y Vigilancia para CEA, CIA y OTT"

Autoridades administrativas y judiciales	10 días	No. días en los cuáles se da respuesta desde el momento de la radicación/10	95 %
--	---------	---	------

Niveles de atención de incidentes

Categoría	Nombre	Descripción	Objetivo	Rango de cumplimiento	Formul a 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: $DMS = \frac{(TTD - TCMS)}{TTD} * 100$

RESOLUCIÓN NÚMERO _____ DE _____

"Por medio de la cual se modifican las Resoluciones 5790 y 60832 de 2016 de la Superintendencia de Transporte y se introducen mejoras y medidas para fortalecer las capacidades de inspección, Vigilancia y Control a través de su Sistema de Control y Vigilancia para CEA, CIA y OTT"

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%		

RESOLUCIÓN NÚMERO _____ DE _____

"Por medio de la cual se modifican las Resoluciones 5790 y 60832 de 2016 de la Superintendencia de Transporte y se introducen mejoras y medidas para fortalecer las capacidades de inspección, Vigilancia y Control a través de su Sistema de Control y Vigilancia para CEA, CIA y OTT"

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
Cientes 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	95 %

RESOLUCIÓN NÚMERO _____ DE _____

"Por medio de la cual se modifican las Resoluciones 5790 y 60832 de 2016 de la Superintendencia de Transporte y se introducen mejoras y medidas para fortalecer las capacidades de inspección, Vigilancia y Control a través de su Sistema de Control y Vigilancia para CEA, CIA y OTT"

		momento de la radicación/5	
--	--	-------------------------------	--

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 para, para lo cual iniciará el proceso de asignación de responsabilidad que podrá derivar en la adopción de medidas como la orden de presentación de un Plan de mejoramiento, la suspensión de la homologación o pérdida de fuerza ejecutora de la homologación.

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 cumplir con los fines de naturaleza pública de la función de inspección, vigilancia y control, a cargo de la Superintendencia; siendo este el fin exclusivo de su tratamiento.

Los proveedores tecnológicos homologados actúan en calidad de Encargados del Tratamiento y custodios temporales de dicha información. En consecuencia, no podrán invocar derechos de propiedad intelectual, secretos industriales o derechos de retención sobre los datos operativos del Sistema para impedir su acceso, consulta, migración o entrega a la Superintendencia de Transporte cuando esta lo requiera.

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.

RESOLUCIÓN NÚMERO _____ DE _____

"Por medio de la cual se modifican las Resoluciones 5790 y 60832 de 2016 de la Superintendencia de Transporte y se introducen mejoras y medidas para fortalecer las capacidades de inspección, Vigilancia y Control a través de su Sistema de Control y Vigilancia para CEA, CIA y OTT"

4.2.1. Categorías de información y plazos de conservación:

- a) **Registros del proceso de capacitación, curso y certificación:** Comprende el conjunto de datos que constituyen el expediente electrónico de cada servicio prestado a un usuario, incluyendo su historial de clases o sesiones (asistencia, permanencia), los resultados de todas las validaciones de identidad (exitosas y fallidas), los resultados de las evaluaciones teóricas y prácticas, los recorridos georreferenciados de las clases prácticas, y el Certificado de Aptitud en Conducción (CAC) o de asistencia 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 CEA, CIA u OTT para acreditar el cumplimiento de sus requisitos de registro y operación, tales como certificados de conformidad, informes de auditoría de los OEC, pólizas de responsabilidad civil, licencias de funcionamiento y registros de programas

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 archivar 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 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

RESOLUCIÓN NÚMERO _____ DE _____

"Por medio de la cual se modifican las Resoluciones 5790 y 60832 de 2016 de la Superintendencia de Transporte y se introducen mejoras y medidas para fortalecer las capacidades de inspección, Vigilancia y Control a través de su Sistema de Control y Vigilancia para CEA, CIA y OTT"

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 no mayor a **doce (12) meses** 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.

- 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 forense 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.

RESOLUCIÓN NÚMERO _____ DE _____

"Por medio de la cual se modifican las Resoluciones 5790 y 60832 de 2016 de la Superintendencia de Transporte y se introducen mejoras y medidas para fortalecer las capacidades de inspección, Vigilancia y Control a través de su Sistema de Control y Vigilancia para CEA, CIA y OTT"

4.3. OBLIGACIONES DE LOS PROVEEDORES 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 Enseñanza Automovilística, Centros Integrales de Atención y Organismos de Tránsito y Transporte, 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) robusto, basado en estándares internacionales reconocidos (como la familia ISO 27000), 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

RESOLUCIÓN NÚMERO _____ DE _____

"Por medio de la cual se modifican las Resoluciones 5790 y 60832 de 2016 de la Superintendencia de Transporte y se introducen mejoras y medidas para fortalecer las capacidades de inspección, Vigilancia y Control a través de su Sistema de Control y Vigilancia para CEA, CIA y OTT" 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.

RESOLUCIÓN NÚMERO _____ DE _____

"Por medio de la cual se modifican las Resoluciones 5790 y 60832 de 2016 de la Superintendencia de Transporte y se introducen mejoras y medidas para fortalecer las capacidades de inspección, Vigilancia y Control a través de su Sistema de Control y Vigilancia para CEA, CIA y OTT"

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 la aplicación móvil para usuarios e instructores, el Módulo de consulta, IVC e inteligencia de negocio para la Superintendencia, el sistema de valoración de la calidad, y todas las demás especificadas en el presente Anexo Técnico, asegurando su correcta operación y la consecución de los objetivos de control para los cuales fueron diseñadas.

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 el Sistema de Control y Vigilancia para Centros de Reconocimiento de Conductores (SICOV-CRC) cuando aplique, con el Sistema Integrado de Información sobre Multas y Sanciones por Infracciones de Tránsito (SIMIT) cuando aplique, 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 homologados, trazabilidad y avances en los procesos de capacitación 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

RESOLUCIÓN NÚMERO _____ DE _____

"Por medio de la cual se modifican las Resoluciones 5790 y 60832 de 2016 de la Superintendencia de Transporte y se introducen mejoras y medidas para fortalecer las capacidades de inspección, Vigilancia y Control a través de su Sistema de Control y Vigilancia para CEA, CIA y OTT" 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.
11. **Gestión técnica del repositorio de preguntas para evaluaciones teóricas:** Administrar técnicamente la plataforma que soporta el repositorio centralizado de preguntas para las evaluaciones teóricas de los CEA, asegurando su integridad, seguridad y la correcta aplicación de las preguntas que hayan sido elaboradas.
12. **Mantenimiento y soporte de la aplicación móvil:** Asegurar el desarrollo continuo, mantenimiento, seguridad y disponibilidad de la aplicación móvil del SICOV para usuarios e instructores, garantizando su compatibilidad con las versiones vigentes de los sistemas operativos Android e iOS y la correcta operación de todas sus funcionalidades.
13. **Gestión del sistema de valoración de la calidad:** Implementar y mantener el sistema de valoración de instructores y contenidos por parte de los usuarios, asegurando los mecanismos de anonimización o seudonimización requeridos, la correcta agregación de los datos y la generación de reportes para la Superintendencia y los CEA, conforme a lo establecido en el Anexo Técnico.

Gestión de información, reportes y soporte a la IVC de la Superintendencia

RESOLUCIÓN NÚMERO _____ DE _____

"Por medio de la cual se modifican las Resoluciones 5790 y 60832 de 2016 de la Superintendencia de Transporte y se introducen mejoras y medidas para fortalecer las capacidades de inspección, Vigilancia y Control a través de su Sistema de Control y Vigilancia para CEA, CIA y OTT"

14. **Provisión de acceso y herramientas de consulta para la superintendencia:** garantizar a la superintendencia de transporte el acceso exclusivo, 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.
15. **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.
16. **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.
17. **Notificación automática de alertas y marcaciones:** Garantizar que, ante cualquier alerta o marcación de irregularidad generada por el sistema, el CEA, CIA u OTT 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.

RESOLUCIÓN NÚMERO _____ DE _____

"Por medio de la cual se modifican las Resoluciones 5790 y 60832 de 2016 de la Superintendencia de Transporte y se introducen mejoras y medidas para fortalecer las capacidades de inspección, Vigilancia y Control a través de su Sistema de Control y Vigilancia para CEA, CIA y OTT"

18. 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 organismo de apoyo al tránsito.

19. 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 CEA, CIA y OTT. 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.

20. 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.

21. 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.

RESOLUCIÓN NÚMERO _____ DE _____

"Por medio de la cual se modifican las Resoluciones 5790 y 60832 de 2016 de la Superintendencia de Transporte y se introducen mejoras y medidas para fortalecer las capacidades de inspección, Vigilancia y Control a través de su Sistema de Control y Vigilancia para CEA, CIA y OTT"

- 22. 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 por parte de los organismos de apoyo. Proveer a la Superintendencia la información técnica y los registros del sistema que esta requiera para el análisis de casos específicos de incidentes reportados.
- 23. 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

- 22. Calidad del servicio, soporte técnico y capacitación a organismos de apoyo:** Garantizar la prestación del servicio SICOV a los CEA, CIA y OTT 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.
- 23. 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 CEA, CIA y OTT FRENTE AL SICOV

RESOLUCIÓN NÚMERO _____ DE _____

"Por medio de la cual se modifican las Resoluciones 5790 y 60832 de 2016 de la Superintendencia de Transporte y se introducen mejoras y medidas para fortalecer las capacidades de inspección, Vigilancia y Control a través de su Sistema de Control y Vigilancia para CEA, CIA y OTT"

Además de las obligaciones generales derivadas de la normatividad que rige su actividad y de aquellas específicas contenidas en otros apartados del presente acto administrativo y su Anexo Técnico, los CEA, los CIA y OTT que dicten cursos a infractores, según corresponda a la naturaleza del servicio que prestan, 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 y permanencia, evaluación, certificación y reporte de información relacionados con la prestación de sus servicios de capacitación o cursos, 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, vehículos 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 (instructores, directivos, administrativos), físicos

RESOLUCIÓN NÚMERO _____ DE _____

"Por medio de la cual se modifican las Resoluciones 5790 y 60832 de 2016 de la Superintendencia de Transporte y se introducen mejoras y medidas para fortalecer las capacidades de inspección, Vigilancia y Control a través de su Sistema de Control y Vigilancia para CEA, CIA y OTT"

(aulas, infraestructura de puntos de validación, computadores, vehículos) 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 CEA, CIA y OTT 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 o vehículos 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 CEA, CIA u OTT 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

RESOLUCIÓN NÚMERO _____ DE _____

"Por medio de la cual se modifican las Resoluciones 5790 y 60832 de 2016 de la Superintendencia de Transporte y se introducen mejoras y medidas para fortalecer las capacidades de inspección, Vigilancia y Control a través de su Sistema de Control y Vigilancia para CEA, CIA y OTT"
suspensión provisional inmediata del servicio en el organismo de apoyo implicado, hasta que se resuelva la situación.

La sanción se aplicará directamente al CEA, CIA u OTT 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 el servicio, incluyendo el mantenimiento, y actualización de los equipos que hacen parte de las funciones del Organismo de Apoyo. 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

RESOLUCIÓN NÚMERO _____ DE _____

"Por medio de la cual se modifican las Resoluciones 5790 y 60832 de 2016 de la Superintendencia de Transporte y se introducen mejoras y medidas para fortalecer las capacidades de inspección, Vigilancia y Control a través de su Sistema de Control y Vigilancia para CEA, CIA y OTT"

Pública Fija exclusiva, descritas en el presente Anexo Técnico. El CEA, CIA y OTT 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 o comunicaciones.
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

RESOLUCIÓN NÚMERO _____ DE _____

"Por medio de la cual se modifican las Resoluciones 5790 y 60832 de 2016 de la Superintendencia de Transporte y se introducen mejoras y medidas para fortalecer las capacidades de inspección, Vigilancia y Control a través de su Sistema de Control y Vigilancia para CEA, CIA y OTT"

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, monitoreo de permanencia, 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 evaluaciones y bancos de preguntas (para CEA):

Para los CEA, elaborar y cargar en SICOV los bancos de preguntas para las evaluaciones teóricas siguiendo los lineamientos y procesos de validación definidos por la ANSV o el Ministerio de Transporte, cuando aplique. Configurar los parámetros de aprobación de las evaluaciones teóricas de conformidad con la normatividad vigente. Garantizar la idoneidad en la realización de las evaluaciones prácticas y el correcto registro de sus resultados en SICOV, cuando aplique.

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 en Conducción (para CEA) o Certificados de Asistencia (para CIA/OTT), y solo cuando el SICOV haya habilitado dicha expedición por el cumplimiento verificado de todos los requisitos. El representante legal del organismo de apoyo o su delegado será el único responsable de la decisión de certificación.

23. Gestión de auditorías de conformidad:

Cargar oportunamente en SICOV los informes de auditoría de los Organismos Evaluadores de la Conformidad 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.

RESOLUCIÓN NÚMERO _____ DE _____

"Por medio de la cual se modifican las Resoluciones 5790 y 60832 de 2016 de la Superintendencia de Transporte y se introducen mejoras y medidas para fortalecer las capacidades de inspección, Vigilancia y Control a través de su Sistema de Control y Vigilancia para CEA, CIA y OTT"

24. **Cumplimiento de medidas de suspensión:** El CEA, CIA u OTT 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 CEA, CIA u OTT 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 todos sus servicios de capacitación o cursos, de forma veraz y transparente, asegurando que el SICOV controle el pago de la capacitación.
26. **Fomento del uso de la aplicación móvil SICOV:** Promover el uso de la aplicación móvil del SICOV entre sus usuarios e instructores para las gestiones que esta permita, y asegurar que sus políticas operativas internas sean compatibles con las funcionalidades de dicha aplicación.
27. **Información sobre el sistema de valoración:** Informar a sus usuarios sobre la existencia del sistema de valoración de la calidad de la capacitación y de los instructores a través de la aplicación móvil SICOV, y abstenerse de cualquier práctica que coarte la libertad del usuario para emitir una valoración objetiva.

Hasta aquí el Anexo Técnico.

Artículo 13. De la protección del usuario en caso de suspensión de la conexión de un CEA, CIA u OTT. Como medida especial de protección del usuario y de la continuidad del servicio, el CEA, CIA u OTT que sea objeto de una medida de suspensión de la conexión en el Registro Único Nacional de Tránsito tendrá la obligación de garantizar la culminación del servicio a todos los usuarios que hayan pagado y a quienes se les haya generado un PIN antes de la adopción de la medida. La Superintendencia de Transporte, a través del SICOV, velará por el cumplimiento de esta obligación mediante los mecanismos de reporte y trazabilidad que se detallan en el Anexo Técnico de la presente resolución.

Artículo 14. Procedimiento de supervisión de la operación del SICOV y Planes de Mejoramiento.

RESOLUCIÓN NÚMERO _____ DE _____

"Por medio de la cual se modifican las Resoluciones 5790 y 60832 de 2016 de la Superintendencia de Transporte y se introducen mejoras y medidas para fortalecer las capacidades de inspección, Vigilancia y Control a través de su Sistema de Control y Vigilancia para CEA, CIA y OTT"

En desarrollo de las facultades de inspección, vigilancia y control, cuando la Superintendencia de Transporte, a través de visitas de verificación técnica, auditorías o monitoreo tecnológico, identifique presuntos incumplimientos o fallas en la operación del SICOV por parte de los operadores homologados, procederá trasladando los hallazgos y comunicando al Operador el informe técnico o acta de visita o consulta de verificación con los hallazgos, otorgándole un término de cinco (5) días hábiles para presentar explicaciones, soportes o controversias.

Si la Superintendencia determina que el hallazgo no constituye una falta grave que ponga en riesgo la operación de los organismos de apoyo, comprometa la información del Sistema o atente contra el ordenamiento jurídico y que amerite la revocatoria inmediata o inhabilitación, podrá requerir al operador la presentación de un Plan de Mejoramiento. Este plan deberá incluir las acciones correctivas y los tiempos de ejecución, los cuales serán aprobados por la entidad.

Si durante la implementación del Plan de Mejoramiento persisten las deficiencias, o si el operador no logra desvirtuar la desaparición de los fundamentos de hecho de su habilitación, la Superintendencia procederá a declarar la pérdida de fuerza ejecutoria del acto administrativo de homologación, de conformidad con el numeral 2 del artículo 91 de la Ley 1437 de 2011.

Parágrafo: La declaratoria de pérdida de fuerza ejecutoria impedirá que el operador continúe prestando el servicio SICOV, sin perjuicio de que pueda iniciar nuevamente el trámite de homologación una vez acredite el cumplimiento pleno de requisitos.

Artículo 15. Gobernanza del Sistema de Control y Vigilancia en los Centros de Enseñanza Automovilística, Centros Integrales de Atención y Organismos de Tránsito y Transporte. La Superintendencia de Transporte como responsable del diseño, estructuración funcional, determinador de las validaciones y condiciones técnicas, tecnológicas y operativas del Sistema de Control y Vigilancia implementado en los CEA, CIA y OTT, adoptará un modelo institucional de gobernanza de datos y servicios con el propósito de garantizar la integridad, disponibilidad, interoperabilidad, trazabilidad, calidad y seguridad de la información generada, recolectada, procesada, almacenada, reportada y consultada a través de dicho sistema.

La gobernanza del SICOV comprenderá, entre otros, los siguientes aspectos:

RESOLUCIÓN NÚMERO _____ DE _____

"Por medio de la cual se modifican las Resoluciones 5790 y 60832 de 2016 de la Superintendencia de Transporte y se introducen mejoras y medidas para fortalecer las capacidades de inspección, Vigilancia y Control a través de su Sistema de Control y Vigilancia para CEA, CIA y OTT"

1. Definición de roles y responsabilidades para la administración, operación, mantenimiento y uso de la información del sistema, de acuerdo con las competencias institucionales y la normativa vigente.
2. Lineamientos de calidad de datos, orientados a asegurar la validez, completitud, consistencia, actualidad y confiabilidad de los registros captados por los dispositivos tecnológicos y reportados por los CEA, CIA y OTT.
3. Esquemas de interoperabilidad, que permitan el intercambio seguro, ágil y estandarizado de información con otros sistemas de la Entidad, del sector transporte y de otras entidades públicas.
4. Mecanismos de trazabilidad y auditoría de datos, que permitan registrar y monitorear el ciclo de vida de la información, desde su captura hasta su disposición final o uso para fines de inspección, vigilancia y control.
5. Gestión de riesgos tecnológicos, mediante la identificación, evaluación y mitigación de amenazas que puedan comprometer la disponibilidad y funcionamiento del sistema o la integridad de sus datos.
6. Esquemas de mejora continua, orientados a la actualización tecnológica, revisión periódica de los indicadores de calidad, eficiencia y eficacia del SICOV, y la adopción de buenas prácticas en la gestión de datos.

Parágrafo. El Comité Técnico y Operativo para el Fortalecimiento del SICOV será el responsable de definir, coordinar y supervisar la implementación del modelo de gobernanza del SICOV; actividad que será realizada en articulación con los proveedores tecnológicos homologados para su operación, garantizando el cumplimiento de las condiciones técnicas, tecnológicas y operativas establecidas por la Superintendencia de Transporte.

Artículo 16. Desarrollo, implementación, despliegue de mejoras del SICOV y periodo de transición.

Los actuales proveedores homologados del Sistema de Control y Vigilancia para CEA, CIA y OTT que manifiesten su interés en continuar operando, contarán con un plazo máximo de seis (6) meses calendario para la implementación total del nuevo Sistema de Control y Vigilancia, contados a partir del día hábil siguiente al vencimiento del término para presentar la manifestación de interés de que trata el artículo 16.

Presentación del Plan de trabajo y cronograma:

RESOLUCIÓN NÚMERO _____ DE _____

"Por medio de la cual se modifican las Resoluciones 5790 y 60832 de 2016 de la Superintendencia de Transporte y se introducen mejoras y medidas para fortalecer las capacidades de inspección, Vigilancia y Control a través de su Sistema de Control y Vigilancia para CEA, CIA y OTT"

Dentro de los diez (10) días hábiles siguientes a la radicación de la manifestación de interés de que trata el artículo 16, los operadores homologados deberán presentar ante el Comité Técnico Operativo un Plan de trabajo detallado. Este documento deberá contener:

- La desagregación de los hitos técnicos para el cumplimiento de la Fase I y Fase II.
- El cronograma de desarrollo, pruebas y despliegue de la arquitectura de contenedores.
- El plan de migración de datos históricos.
- La estrategia de socialización y gestión del cambio con los Organismos de Apoyo vinculados.

La Superintendencia de Transporte realizará el seguimiento al cumplimiento de los avances con base en este instrumento de planeación.

El periodo de transición se dividirá en dos (2) fases de ejecución obligatoria:

Implementación en CIA y OTT

El término de seis (6) meses se dividirá en dos fases.

Fase I: Alistamiento, desarrollo y piloto.

Durante los primeros tres (3) meses, el operador deberá:

- a) Realizar el desarrollo y ajustes de software necesarios para cumplir con las funcionalidades descritas en el Anexo Técnico
- b) Implementar y poner en operación el SICOV ajustado en, al menos, el 80 % de los establecimientos de los Centros Integrales de Atención y Organismos de Tránsito y Transporte, a modo de ambiente productivo controlado.
- c) Comenzar el despliegue de la infraestructura base del CPD Analítico y el Módulo de Consulta para la Superintendencia (MOCVI).

Fase II: Despliegue masivo y estabilización.

Durante los tres (3) meses restantes, el operador deberá:

- a) Realizar el despliegue masivo del nuevo SICOV en la totalidad de los Centros de Enseñanza Automovilística vinculados a su operación.

RESOLUCIÓN NÚMERO _____ DE _____

"Por medio de la cual se modifican las Resoluciones 5790 y 60832 de 2016 de la Superintendencia de Transporte y se introducen mejoras y medidas para fortalecer las capacidades de inspección, Vigilancia y Control a través de su Sistema de Control y Vigilancia para CEA, CIA y OTT"

b) Completar el despliegue de la infraestructura del CPD Analítico y la implementación del 50 % sus funcionalidades, incluyendo tableros de control.

c) Finalizar la migración de datos históricos al nuevo esquema de almacenamiento.

Parágrafo 1. El Comité Técnico y Operativo para el Fortalecimiento del SICOV será el responsable de revisar y certificar el avance de la implementación de las mejoras técnicas, tecnológicas y operativas del Sistema de Control y Vigilancia en cada una de sus fases, así como de evaluar y autorizar, cuando sea procedente y esté debidamente justificada, la prórroga excepcional de los plazos establecidos.

Parágrafo 2. La Superintendencia podrá otorgar una única prórroga de hasta tres (3) meses, siempre y cuando el operador solicite dicha extensión antes del vencimiento de la Fase II y cuente con el concepto favorable y motivado del Comité Técnico y Operativo.

Para la emisión de dicho concepto, el Comité verificará que el operador ha alcanzado un avance funcional y técnico superior al 85% en la implementación total del sistema.

Este porcentaje se calculará estrictamente con base en la ejecución de los hitos y entregables definidos en el Plan de Trabajo Detallado aprobado al inicio de la transición. La medición se consignará en una Matriz de Avance Técnico, soportada en evidencias documentales y pruebas de funcionamiento en ambiente de calidad (QA) o producción.

Parágrafo 3. Durante todo el régimen de transición, los operadores deberán garantizar la operación ininterrumpida de la versión actual del SICOV, asegurando que no se afecte la prestación del servicio a los usuarios en los organismos de apoyo.

Parágrafo 4. Si, al vencimiento del término de implementación de las mejoras, alguno de los actuales proveedores homologados no demuestra la implementación de la totalidad de las mejoras y requisitos técnicos establecidos en la presente Resolución y su Anexo Técnico, bien por falta de interés, o por incumplimiento de los plazos establecidos, la Entidad procederá de la siguiente manera:

RESOLUCIÓN NÚMERO _____ DE _____

"Por medio de la cual se modifican las Resoluciones 5790 y 60832 de 2016 de la Superintendencia de Transporte y se introducen mejoras y medidas para fortalecer las capacidades de inspección, Vigilancia y Control a través de su Sistema de Control y Vigilancia para CEA, CIA y OTT"

Se requerirá al operador para que, en el término de cinco (5) días hábiles, explique las razones del incumplimiento.

De no encontrarse justificada la omisión, o persistiendo el incumplimiento de los requisitos habilitantes técnicos y jurídicos para la operación, se configurará la causal de Pérdida de Fuerza Ejecutoria del acto administrativo de homologación por desaparición de sus fundamentos de hecho y de derecho, de conformidad con el numeral 2 del artículo 91 de la Ley 1437 de 2011. Por la naturaleza de los requisitos habilitantes exigidos en el presente régimen de transición, este incumplimiento se considerará insubsanable, procediéndose directamente a la declaratoria de la pérdida de fuerza ejecutoria.

En este evento, la Superintendencia de Transporte expedirá el acto administrativo motivado que declare la ocurrencia de dicha condición y ordene la terminación de la operación, garantizando los recursos de ley. Una vez en firme dicho acto, se procederá con la desconexión definitiva del operador.

Sin perjuicio de las garantías del debido proceso para la declaratoria de la pérdida de fuerza ejecutoria, la Superintendencia de Transporte podrá ordenar, como medida cautelar de carácter inmediato, la suspensión preventiva de la conexión del operador homologado con el sistema RUNT y con los Organismos de Apoyo vinculados, una vez vencido el plazo de transición sin que se haya acreditado el cumplimiento de los requisitos. Esta medida se mantendrá vigente mientras se surte y queda en firme la actuación administrativa correspondiente, con el fin de salvaguardar la seguridad de la información y la idoneidad técnica del servicio público.

Parágrafo transitorio. Las funcionalidades tecnológicas del software de gestión y control y aspectos de interoperabilidad que requieran de mayor grado de definición por parte de la Superintendencia de Transporte para su desarrollo, o que estén condicionados a la disponibilidad técnica, normativa y voluntad de la entidad tercera, no serán tenidos en cuenta en la verificación del cumplimiento en los plazos previstos en este artículo, no impedirán la obtención ni el mantenimiento de la homologación del operador actual, ni darán lugar a la apertura de un procedimiento de supervisión para determinar el eventual incumplimiento de alguna. La Superintendencia de Transporte especificará aquellas funcionalidades o aspectos tecnológicos con los que ocurra lo anterior.

Artículo 17. Manifestación de interés de mantenimiento de la homologación. Los actuales proveedores homologados que deseen continuar operando el SICOV deberán presentar una comunicación formal ante la

RESOLUCIÓN NÚMERO _____ DE _____

"Por medio de la cual se modifican las Resoluciones 5790 y 60832 de 2016 de la Superintendencia de Transporte y se introducen mejoras y medidas para fortalecer las capacidades de inspección, Vigilancia y Control a través de su Sistema de Control y Vigilancia para CEA, CIA y OTT"

Superintendencia de Transporte manifestando dicho interés, dentro de los diez (10) días hábiles siguientes a la entrada en vigencia de la presente resolución, acompañada de la documentación que acredite el cumplimiento de los requisitos financieros, jurídicos y administrativos actualizados.

La manifestación de interés y la entrega de documentación por parte de los proveedores homologados vigentes no constituye una solicitud para una nueva homologación, sino una solicitud para mantener la homologación vigente.

La presentación de la manifestación de interés no implica la aprobación automática. La Superintendencia contará con un término de hasta quince (15) días hábiles para verificar la documentación financiera y jurídica aportada y confirmar la continuidad del operador en el régimen de transición.

Si vencido el término de diez (10) días hábiles el operador no presenta la manifestación de interés o no acredita los requisitos financieros, jurídicos y administrativos, se entenderá que desiste de mantener su homologación. En consecuencia, deberá iniciar el plan de salida y entrega de información a la Superintendencia, garantizando la operación por el tiempo necesario para que los organismos de apoyo vinculados realicen la migración a otro operador homologado. Este periodo no podrá exceder de doce (12) meses.

Al término del periodo de implementación y transición, el proveedor tecnológico deberá demostrar la implementación de la totalidad de los nuevos requisitos y componentes técnicos, tecnológicos y operativos del Sistema de Control y Vigilancia, lo cual será verificado por la Superintendencia de Transporte condición para el mantenimiento de la homologación.

Parágrafo. A partir de la fecha de puesta en producción del SICOV ajustado según la presente Resolución, los operadores homologados inhabilitarán la opción de enrolar usuarios en la versión anterior del software. En el caso de los CEA, los usuarios que no hayan culminado su proceso de capacitación tendrán un plazo máximo de treinta (30) días para finalizarlo en la versión anterior del Sistema. Superado este término, sus registros deberán ser migrados a la nueva plataforma para su culminación.

Parágrafo transitorio. La nueva experiencia exigida en los requisitos administrativos para la operación del SICOV, conforme a la modificación introducida al Anexo Técnico, podrá ser acreditada por parte de los actuales operadores homologados que deseen mantener su homologación, entre otros, con la obtenida producto de la operación actual del Sistema.

RESOLUCIÓN NÚMERO _____ DE _____

"Por medio de la cual se modifican las Resoluciones 5790 y 60832 de 2016 de la Superintendencia de Transporte y se introducen mejoras y medidas para fortalecer las capacidades de inspección, Vigilancia y Control a través de su Sistema de Control y Vigilancia para CEA, CIA y OTT"

Parágrafo transitorio. El operador homologado que no presente la manifestación de interés dentro del término establecido, o que manifieste expresamente su decisión de no continuar, deberá en todo caso garantizar la operación ininterrumpida del Sistema en las condiciones actuales, hasta que finalice el periodo de implementación de los operadores que sí manifiesten interés, o hasta que se perfeccione la migración de todos los organismos de apoyo vinculados a su plataforma hacia otros operadores habilitados dentro de los doce (12) meses aludidos.

Artículo 18. Apropiación y gestión del cambio. Con el propósito de fomentar el uso adecuado del Sistema de Control y Vigilancia y así garantizar una gestión del cambio que asegure una transición efectiva hacia el nuevo modelo de vigilancia tecnológica en los Centros de Enseñanza Automovilística, Centros Integrales de Atención y Organismos de Tránsito y Transporte, la Superintendencia de Transporte realizará capacitaciones dirigidas al personal vinculado a estos organismos de apoyo al tránsito.

Artículo 19. Comité Técnico Operativo para el Fortalecimiento del SICOV. El Comité Técnico Operativo para el Fortalecimiento del SICOV creado a través de la Resolución 613 de 2023 de la Superintendencia de Transporte en cumplimiento de lo previsto en la Resolución 355 de 2023 para atender la necesidad de definición de criterios, estructura y periodicidad de generación de alertas del Sistema será el encargado, en el marco de sus funciones, de definir y precisar aspectos y criterios técnicos y tecnológicos necesarios para dar cumplimiento a lo dispuesto en el Anexo técnico por parte de los proveedores homologados.

Artículo 20. Modifíquese el artículo 24 de la Resolución 355 de 2023, el cual quedará así

Artículo 24. Informes integrales de operación y supervisión.

Los operadores homologados del SICOV deberán presentar y radicar ante la Superintendencia de Transporte, dentro de los cinco (5) primeros días hábiles de cada mes, un informe detallado sobre los análisis realizados a partir de la información recabada de la operación de los organismos de apoyo al tránsito vinculados a su plataforma.

Dichos informes deberán consolidar los hallazgos derivados del monitoreo de datos, la administración de la información y las visitas realizadas, conforme a los parámetros establecidos en el Anexo Técnico de la presente resolución.

RESOLUCIÓN NÚMERO _____ DE _____

"Por medio de la cual se modifican las Resoluciones 5790 y 60832 de 2016 de la Superintendencia de Transporte y se introducen mejoras y medidas para fortalecer las capacidades de inspección, Vigilancia y Control a través de su Sistema de Control y Vigilancia para CEA, CIA y OTT"

Parágrafo 1. Los informes presentados por los operadores homologados constituirán insumo técnico y probatorio para el ejercicio de las funciones de inspección, vigilancia y control de la Superintendencia de Transporte.

Recibida la información, la Superintendencia, a través de las dependencias competentes, evaluará el contenido y determinará la procedencia de las actuaciones administrativas correspondientes.

Parágrafo 2. La presentación de estos informes no exime a los operadores homologados de su deber de reportar de manera inmediata a la Superintendencia cualquier irregularidad grave o alteración al sistema que detecten en tiempo real.

Artículo 19. Vigencia y publicación. La presente Resolución rige a partir de la fecha de su publicación en el Diario Oficial.

Artículo 20. Derogatorias. La presente Resolución rige a partir de la fecha de su publicación en el Diario Oficial y surte los siguientes efectos normativos:

Sustituye integralmente el Anexo Técnico del Sistema de Control y Vigilancia adoptado mediante la Resolución No. 60832 de 2016, y sus modificatorias, por el Anexo Técnico desarrollado en el presente acto administrativo.

Deroga todas las demás disposiciones de igual o inferior jerarquía que le sean contrarias, y expresamente los artículos 4, 6 y 9 de la Resolución No. 5790 de 2016, así como aquellas que modificaron y/o adicionaron el Anexo Técnico del SICOV de CEA, CIA y OTT contenidas en las Resoluciones 355 y 1164 de 2023