

**MINISTERIO DE TRANSPORTE
SUPERINTENDENCIA DE TRANSPORTE**

RESOLUCIÓN NÚMERO 009981 DE 6 agosto 2026

"Por medio de la cual se modifica la Resolución 2878 de 2026 y su Anexo Técnico, se ajustan disposiciones relativas al periodo de implementación del Sistema de Control y Vigilancia para los CDA, y se dictan otras disposiciones"

SUPERINTENDENTE

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 Único Reglamentario 1079 de 2015, el Decreto 2409 de 2018 y las demás normas concordantes y,

CONSIDERANDO

Que los Artículos 2, 24 y 365 de la Constitución Política y el literal b del Artículo 2 de la Ley 105 de 1993 establecen el deber del Estado de ejercer funciones de planeación, regulación, control y vigilancia del servicio público de transporte y las actividades a él vinculadas, garantizando la seguridad de los usuarios y la libre circulación en el territorio nacional.

Que la Ley 769 de 2002, en su Artículo 3, parágrafo 1, dispuso que determinadas funciones de tránsito pueden asignarse a entidades públicas o privadas que actúan como organismos de apoyo a las autoridades de tránsito, y en su parágrafo 3 atribuyó a la Superintendencia de Transporte la función de vigilar y controlar dichos organismos. Así mismo, el Artículo 1 de la misma ley estableció como principios rectores del tránsito terrestre 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.

Que el Decreto 2409 de 2018 facultó a la Superintendencia de Transporte para ejercer funciones de inspección, vigilancia y control de la debida prestación del servicio de transporte y sus servicios conexos, y para expedir los reglamentos, manuales e instructivos necesarios para el ejercicio de dichas funciones, en el marco de los numerales 2 y 15 del Artículo 7 de ese decreto.

Que los operadores homologados del SICOV están obligados a registrarse en el Sistema Inteligente Nacional de Supervisión al Transporte (SINST VIGIA 2) de la Superintendencia de Transporte y a mantenerse al día en el cumplimiento de sus obligaciones, por lo que resulta necesario incorporar dicho registro como requisito jurídico para la obtención y mantenimiento de la homologación como operador del SICOV, garantizando que los operadores homologados cumplan sus obligaciones institucionales frente a la Superintendencia.

Que, mediante la Resolución 2878 de 2026, la Superintendencia de Transporte modificó las Resoluciones 9304 de 2012 y 13830 de 2014, introdujo mejoras al Sistema de Control y Vigilancia para Centros de Diagnóstico Automotor —SICOV

RESOLUCIÓN No 009981 DE 6 agosto 2026

"Por medio de la cual se modifica la Resolución 2878 de 2026 y su Anexo Técnico, se ajustan disposiciones relativas al periodo de implementación del Sistema de Control y Vigilancia para los CDA, y se dictan otras disposiciones"

CDA, sustituyó el Anexo Técnico aplicable a dicho sistema, derogó algunas disposiciones y dictó medidas orientadas a su fortalecimiento.

Que la Resolución 2878 de 2026 actualizó las condiciones técnicas, tecnológicas, operativas y funcionales del SICOV aplicable a los Centros de Diagnóstico Automotor, con el propósito de fortalecer la trazabilidad de los procesos de revisión técnico-mecánica y de emisiones contaminantes, la validación de identidad de los actores intervinientes, la integridad de la información, la interoperabilidad y la disponibilidad del sistema.

Que mediante la Resolución 2878 de 2026, la Superintendencia de Transporte estableció un régimen de transición de seis (6) meses, prorrogable de manera excepcional hasta por tres (3) meses adicionales, para que los operadores homologados que manifestaran su interés en continuar operando el SICOV implementaran las nuevas condiciones previstas.

Que la implementación de las funcionalidades previstas en la Resolución 2878 de 2026 exige la ejecución coordinada de desarrollos de software, adquisición de equipos tecnológicos, adecuaciones de infraestructura, desarrollo e implementación de protocolos de interoperabilidad con terceros, pruebas, despliegue territorial y gestión del cambio con los CDA vinculados, siendo la infraestructura tecnológica descentralizada un componente esencial que incluye, entre otros, estaciones de trabajo, servidores, dispositivos biométricos, cámaras, equipos de comunicaciones y componentes de seguridad.

Que distintos operadores homologados del SICOV, para diferentes organismos de apoyo, manifestaron formalmente en diferentes oportunidades a la Superintendencia que la adquisición de dicha infraestructura depende de cadenas de suministro internacionales cuyos tiempos de entrega oscilan entre noventa (90) y ciento veinte (120) días, a lo que se suman los tiempos de nacionalización, configuración, integración y despliegue en los organismos de apoyo vinculados, y que la volumetría de equipos requerida supera la disponibilidad inmediata del mercado, haciendo materialmente imposible cumplir los plazos originales por causas ajenas al control de los operadores.

Que mantener los plazos inicialmente previstos colocaría a los operadores en condición de incumplimiento por causas objetivas de abastecimiento y disponibilidad tecnológica, lo cual resulta contrario a los principios de proporcionalidad, razonabilidad, buena fe, confianza legítima, eficacia administrativa y continuidad del servicio, por lo que la Superintendencia de Transporte considera necesario ampliar los plazos y modular la implementación en fases, bajo criterios de gradualidad, seguridad, trazabilidad y continuidad del servicio, sin que ello modifique la finalidad estructural del SICOV ni elimine las obligaciones sustanciales de implementación a cargo de los operadores homologados.

Que resulta procedente, en razón de lo anterior, replantear los plazos de implementación del SICOV y establecer tres fases: una primera fase de desarrollo de software entre el 01 de mayo y el 01 noviembre de 2026, al término de la cual la Superintendencia verificará que el operador está en condiciones de desplegar la versión básica del SICOV; una segunda fase de

RESOLUCIÓN No 009981 DE 6 agosto 2026

"Por medio de la cual se modifica la Resolución 2878 de 2026 y su Anexo Técnico, se ajustan disposiciones relativas al periodo de implementación del Sistema de Control y Vigilancia para los CDA, y se dictan otras disposiciones"

despliegue de la versión básica con infraestructura centralizada, obligatoria para todos los CDA a partir del 18 de noviembre de 2026 y vigente hasta el 18 de julio de 2027; y una tercera fase de implementación integral del SICOV a partir del 19 de julio de 2027.

Que las fases transitorias de implementación aquí previstas no sustituyen ni eliminan el modelo integral definido para el SICOV, ni exoneran a los CDA, operadores homologados ni demás actores obligados a dar cumplimiento a lo previsto en el Anexo Técnico de la Resolución 2878 de 2026 y sus actos modificatorios.

Que en el marco de sus funciones de Inspección, Vigilancia y Control, la Superintendencia de Transporte ha identificado la necesidad de establecer un mecanismo de respuesta gradual y proporcional ante el vencimiento de documentos críticos para la operación de los CDA, consistente en una ventana de cuatro (4) horas de operación bajo marcación de irregularidad para proteger a los usuarios que de buena fe acuden al organismo durante ese período.

Que, previa evaluación técnica, la Superintendencia de Transporte considera procedente incorporar al Anexo Técnico los siguientes ajustes: admitir lectores biométricos de huella siempre que se encuentren homologados por la RNEC bajo los estándares del último Anexo Técnico vigente de esa entidad, en respuesta a restricciones de disponibilidad y suministro; ampliar los mecanismos admisibles para la captura de firma y manifestación de voluntad, incluyendo dispositivos móviles y firma digital, sin disminuir los estándares de autenticidad, integridad y trazabilidad; y precisar los requisitos de software de reconocimiento facial diferenciando los componentes para enrolamiento y validaciones puntuales de los componentes para verificación de identidad durante la realización de las inspecciones técnicas vehiculares. Ninguno de estos ajustes implica una disminución de los estándares de seguridad, trazabilidad, confiabilidad, interoperabilidad ni calidad de la información requerida para la operación del SICOV.

Que las alertas, logs, registros transaccionales, evidencias biométricas, registros de conectividad, soportes documentales, trazas de geolocalización, registros de validación y demás evidencias generadas por el SICOV constituyen insumos técnicos sobre el cumplimiento de las verificaciones de seguridad del servicio exigidas por la Superintendencia de Transporte, los cuales resultan de su interés y pueden ser utilizadas en actuaciones administrativas que se lleguen a adelantar.

Que los operadores homologados en régimen de transición deberán actualizar sus planes de trabajo dentro de los diez (10) días siguientes a la entrada en vigencia de la presente resolución, conforme al nuevo cronograma de fases y fechas aquí establecido, de manera que la Superintendencia de Transporte pueda realizar un seguimiento ordenado y progresivo de los avances de implementación.

Que la presente modificación se justifica en razones de seguridad jurídica, eficacia administrativa y proporcionalidad, permitiendo precisar oportunamente las reglas aplicables durante el periodo de transición y asegurar que la

RESOLUCIÓN No 009981 DE 6 agosto 2026

"Por medio de la cual se modifica la Resolución 2878 de 2026 y su Anexo Técnico, se ajustan disposiciones relativas al periodo de implementación del Sistema de Control y Vigilancia para los CDA, y se dictan otras disposiciones"

exigibilidad de las nuevas obligaciones se acompañe con condiciones reales, verificables y técnicamente ejecutables, sin modificar la finalidad estructural de la Resolución 2878 de 2026 ni eliminar las obligaciones sustanciales de implementación a cargo de los operadores homologados.

Que el Comité Técnico Operativo para el Fortalecimiento del SICOV, en sesión extraordinaria del 7 de julio de 2026, recomendó al Superintendente de Transporte efectuar las modificaciones aquí previstas, una vez socializados los argumentos de los operadores homologados y las razones detrás de los demás aspectos a modificar.

Que, en mérito de lo expuesto,

RESUELVE:

Artículo 1. Objeto y ámbito de aplicación. La presente resolución tiene por objeto modificar la Resolución 2878 de 2026 de la Superintendencia de Transporte, ajustar el plazo de implementación y la fecha de entrada en operación integral del Sistema de Control y Vigilancia para Centros de Diagnóstico Automotor, incorporar precisiones técnicas necesarias para su operación y dictar otras disposiciones.

Artículo 2. Modifíquese el Artículo 13 de la Resolución 2878 de 2026, el cual quedará así:

"Artículo 13. Desarrollo, implementación, despliegue de mejoras del SICOV para CDA y periodo de transición. Los actuales operadores homologados del Sistema de Control y Vigilancia para CDA que manifiesten su interés en continuar en la operación contarán con los plazos que a continuación se establecen para la implementación de las nuevas condiciones y requisitos exigidos en el Anexo Técnico del SICOV adoptado mediante el Artículo 14 de la presente Resolución.

Presentación del Plan de trabajo y cronograma:

Dentro de los diez (10) días siguientes a la radicación de la manifestación de interés de que trata el Artículo 14, 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 del objetivo.
- El cronograma de desarrollo, pruebas y despliegue de la arquitectura.
- El plan de migración de datos históricos.
- La estrategia de socialización y gestión del cambio con los organismos de apoyo vinculados.

Implementación del SICOV en Centros de Diagnóstico Automotor

Primera fase. Desarrollo de software:

RESOLUCIÓN No 009981 DE 6 agosto 2026

"Por medio de la cual se modifica la Resolución 2878 de 2026 y su Anexo Técnico, se ajustan disposiciones relativas al periodo de implementación del Sistema de Control y Vigilancia para los CDA, y se dictan otras disposiciones"

Durante los primeros seis (6) meses contados desde el día siguiente al vencimiento del término para presentar la manifestación de interés, esto es, del primero (1) de mayo al primero (1) de noviembre de 2026, los operadores homologados desarrollarán el software del SICOV para CDA en sus versiones básica e integral y realizarán las pruebas necesarias para garantizar el correcto funcionamiento de todas las funcionalidades previstas en el Anexo Técnico. Durante esta fase, los operadores continuarán prestando el servicio del SICOV para CDA conforme a las condiciones vigentes de operación.

Además, durante los seis (6) meses que cubre esta Fase, los operadores homologados deberán simultáneamente avanzar en todo lo necesario para implementar y poner en producción, a su término, la versión básica del SICOV que se describe a continuación, en todos los CDA que tengan vinculados, pues esta versión debe estar lista para entrar en operación al inicio de la Segunda fase.

La versión básica del SICOV incluye:

- El enrolamiento del personal técnico de inspección, ingenieros certificadores y de los usuarios del servicio de RTMyEC, el cual comprenderá: la validación de identidad mediante cotejo dactilar contra las bases de datos de la Registraduría Nacional del Estado Civil, la verificación de la autenticidad del documento de identidad, la validación de identidad con tecnología de reconocimiento facial (Selfie vs. documento), la generación de los template biométricos faciales de referencia para la validación del personal de inspección y de certificación de resultados.
- La validación de identidad del personal de inspección que participa en la realización de las pruebas de la RTMyEC a lo largo de cada jornada de prestación del servicio diaria, al inicio y al final de sus actividades en el día, con la tecnología de reconocimiento facial (Selfie vs. Template).
- La validación de identidad de los ingenieros que certifican los resultados de la RTMyEC al momento de certificar, con tecnología de reconocimiento facial (Selfie vs. Template). Esta validación operará con infraestructura centralizada del operador homologado, incluyendo el ABIS en el que se alojarán los template biométricos de referencia, sin requerirse infraestructura descentralizada en la sede del CDA durante esta etapa.
- Conservación de los registros transaccionales de todas las operaciones, que incluirán como mínimo: fecha, hora, sede, identificación del usuario, vehículo y del personal técnico que participó en la inspección, resultados de los intentos de validación de identidad y demás información que permita la trazabilidad, auditoría y verificación posterior por parte de la Superintendencia de Transporte. Estos registros serán inmutables y se conservarán por un período mínimo de cinco (5) años.

Durante los cinco (5) días siguientes al vencimiento de esta Fase, esto es, entre el tres (3) y el nueve (9) de noviembre de 2026, la Superintendencia de Transporte realizará una verificación del software desarrollado por cada

RESOLUCIÓN No 009981 DE 6 agosto 2026

"Por medio de la cual se modifica la Resolución 2878 de 2026 y su Anexo Técnico, se ajustan disposiciones relativas al periodo de implementación del Sistema de Control y Vigilancia para los CDA, y se dictan otras disposiciones"

operador homologado, con el fin de corroborar que está en condiciones de colocar en producción la versión básica del SICOV y que cuenta con el desarrollo de software necesario para comenzar la implementación gradual de la versión integral conforme a lo que dicta el Anexo Técnico.

La verificación será satisfactoria cuando el operador demuestre que la versión básica se encuentra lista para su despliegue y que ha avanzado en el desarrollo de la versión integral. La Superintendencia de Transporte comunicará el resultado de la verificación a cada operador a más tardar el diecisiete (17) de noviembre de 2026.

Segunda fase. Despliegue de la versión básica del SICOV e inicio del despliegue gradual de la versión integral

La Segunda fase tendrá una duración de ocho (8) meses e irá del dieciocho (18) de noviembre de 2026 al dieciocho (18) de julio de 2027.

Durante este periodo, los operadores homologados deberán tener implementada y mantener operativa, en todos los CDA con los que tengan vínculo, la versión básica del SICOV.

Desde el dieciocho (18) de noviembre de 2026 y durante el término de esta Fase, todos los CDA que presten servicios en el país deberán operar utilizando la versión básica del Sistema de Control y Vigilancia.

La Superintendencia de Transporte verificará la operación de estas funcionalidades mínimas de la versión básica del SICOV entre el diecinueve (19) de noviembre y el dos (2) de diciembre de 2026, en al menos dos (2) CDA ubicados en diferentes ciudades del país.

La verificación será satisfactoria cuando el operador demuestre que en los CDA visitados la versión básica del Sistema implementado cumple con las condiciones mínimas exigidas.

La Superintendencia de Transporte comunicará el resultado de la verificación a cada operador a más tardar el diez (10) de diciembre de 2026.

Durante los ocho (8) meses que cubre esta etapa, además, los operadores homologados deberán simultáneamente iniciar el despliegue gradual de las funcionalidades del SICOV en su versión integral para CDA, realizar las pruebas que sean necesarias y desplegar y poner a punto toda la infraestructura descentralizada requerida, pues esta versión debe estar lista para entrar en operación al inicio de la Tercera fase.

Tercera fase. Implementación de la versión integral del SICOV

A partir del diecinueve (19) de julio de 2027, los operadores homologados deberán colocar en producción la versión integral del SICOV en la totalidad de CDA que tengan vinculados. Desde esa fecha, es obligación de todos los CDA que presten servicios en el país operar utilizando la versión integral del Sistema de Control y Vigilancia.

RESOLUCIÓN No 009981 DE 6 agosto 2026

"Por medio de la cual se modifica la Resolución 2878 de 2026 y su Anexo Técnico, se ajustan disposiciones relativas al periodo de implementación del Sistema de Control y Vigilancia para los CDA, y se dictan otras disposiciones"

La Superintendencia de Transporte realizará visitas de verificación de la operación del SICOV en al menos dos (2) CDA ubicados en diferentes partes del país dentro entre el veintiuno (21) de julio y el tres (3) de agosto de 2027.

La verificación será satisfactoria cuando el operador demuestre que en los CDA la versión integral del SICOV implementado cumple con las condiciones exigidas en el Anexo Técnico.

La Superintendencia de Transporte comunicará el resultado de la verificación a cada operador a más tardar el trece (13) de agosto de 2027.

Parágrafo 1. Si el resultado de las verificaciones que realice la Superintendencia al término de cualquiera de las Fases descritas no es satisfactorio, por cualquier motivo, la entidad requerirá al operador homologado para que dentro de los cinco (5) días hábiles siguientes a la comunicación del resultado explique las razones para ello y para que subsane y demuestre, al término de dicho plazo, que cumple con las condiciones exigidas según la fase respectiva.

Al vencimiento del plazo, la Superintendencia realizará una nueva verificación. Si la subsanación es satisfactoria, el operador continuará en el régimen de transición. Si no lo es, se aplicará lo previsto en el inciso siguiente.

Si, vencido ese plazo, la Superintendencia no encuentra satisfactorio el cumplimiento de las obligaciones, la entidad declarará mediante acto administrativo motivado el incumplimiento de la fase correspondiente. Este acto constituirá la desaparición sobreviniente de los fundamentos de hecho que soportan la homologación vigente, y el homologado deberá iniciar un plan de salida de operación y de migración y entrega de información de la operación a la Superintendencia de Transporte, en los términos que esta disponga, dentro de los treinta (30) días siguientes a la notificación del acto de declaratoria, garantizando en todo caso la continuidad del servicio en la versión vigente del SICOV según la fase, en todos los organismos de apoyo que tenga vinculados, durante un período de hasta seis (6) meses.

Este plazo debe permitir la vinculación de los organismos de apoyo a otro operador homologado, la desactivación progresiva y coordinada de los componentes tecnológicos del saliente; y la comunicación a todos los organismos de apoyo vinculados sobre el inicio del plan de salida con su respectivo cronograma.

Parágrafo 2. La Fase de alistamiento operativo y despliegue gradual del SICOV tendrá carácter temporal, sin que pueda entenderse en ningún momento como un esquema permanente, alternativo o sustitutivo del modelo integral del Sistema desarrollado en el Anexo Técnico.

Parágrafo 3. La Superintendencia Delegada de Tránsito y Transporte Terrestre, será responsable de revisar el avance de la implementación de las mejoras del Sistema de Control y Vigilancia en cada una de las fases definidas en el presente artículo y de presentar informe al Comité Técnico Operativo para el Fortalecimiento del SICOV.

RESOLUCIÓN No 009981 DE 6 agosto 2026

"Por medio de la cual se modifica la Resolución 2878 de 2026 y su Anexo Técnico, se ajustan disposiciones relativas al periodo de implementación del Sistema de Control y Vigilancia para los CDA, y se dictan otras disposiciones"

Parágrafo 4. Durante todo el régimen de transición, los operadores deberán garantizar la operación ininterrumpida de cada versión vigente del SICOV, minimizando al máximo el impacto en la prestación del servicio en los organismos de apoyo a fin de proteger sus derechos y los de sus usuarios.

Parágrafo 5. El cumplimiento de la totalidad de las exigencias asociadas a la operación del SICOV constituye requisito para el mantenimiento de la homologación otorgada por la Superintendencia de Transporte, al ser estos los fundamentos de hecho y de derecho que soportan su existencia. Si, al término de la última Fase de implementación, la entidad encuentra que se cumplen las nuevas condiciones de operación del Sistema, expedirá un acto administrativo motivado que reconozca lo propio y por lo tanto el mantenimiento de la homologación.

Por el contrario, la omisión o el incumplimiento parcial o total de tales requisitos se entiende como la desaparición de los fundamentos que sostienen la homologación vigente de los actuales operadores homologados.

Parágrafo transitorio. Las funcionalidades tecnológicas del software de gestión y control, el CPD Analítico y los 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 un tercero, no serán tenidos en cuenta en la verificación del cumplimiento en los plazos previstos en este artículo, ni impedirán la obtención ni el mantenimiento de la homologación en el caso de los operadores actuales. Será la Superintendencia de Transporte quien determine cuáles son las funcionalidades o parámetros tecnológicos de operación con los que ocurra lo anterior."

Artículo 3. Adiciónese un numeral al acápite de Requerimientos jurídicos del numeral 2.2. del Anexo Técnico adoptado a través de la Resolución 2878 de 2026, así:

"2.2.7. Registro en el VIGIA de la Superintendencia de Transporte.

El aspirante deberá acreditar, para la obtención y/o el mantenimiento de la homologación, como proveedor del Sistema la constancia de registro activo en el Sistema Inteligente Nacional de Supervisión al Transporte (SINST VIGIA 2) de la Superintendencia de Transporte. Este registro deberá mantenerse vigente durante el tiempo que se opere el SICOV."

Artículo 4. Modifíquese el numeral 2.3.3.4.1. del Anexo Técnico adoptado a través de la Resolución 2878 de 2026, el cual quedará así:

"2.3.3.4.1. Profesionales capacitados y con experiencia en Revisión Técnico-Mecánica y de Emisiones Contaminantes —RTMyEC:

Cinco (5) profesionales con título en ingeniería y matrícula profesional vigente. Deberán acreditar formación específica en Revisión Técnico-Mecánica y de Emisiones Contaminantes con una intensidad no inferior a trescientas (300) horas emitida por una Institución de educación superior, así como experiencia certificada mínima de tres (3) años en el ejercicio de funciones relacionadas con

RESOLUCIÓN No 009981 DE 6 agosto 2026

"Por medio de la cual se modifica la Resolución 2878 de 2026 y su Anexo Técnico, se ajustan disposiciones relativas al periodo de implementación del Sistema de Control y Vigilancia para los CDA, y se dictan otras disposiciones"

la dirección técnica de Centros de Diagnóstico Automotor (CDA) legalmente constituidos. Adicionalmente, deberán acreditar certificación vigente en auditoría interna.

Su labor principal consistirá en realizar el análisis técnico de las alertas generadas por el Sistema de Control y Vigilancia, verificar la correcta aplicación de los protocolos de inspección conforme a las normas técnicas y reglamentarias aplicables, efectuar análisis de las evidencias fílmicas de RTMyEC y demás registros que soporten la prestación de ese servicio, así como emitir los conceptos técnicos correspondientes.

Todos los informes de revisión, análisis de evidencias, conceptos técnicos y hallazgos deberán estar suscritos por el profesional experto en RTMyEC que lo elabore y por el representante legal del operador homologado o quien haga sus veces."

Artículo 5. Modifíquese el numeral 2.5.5.3. del Anexo Técnico adoptado a través de la Resolución 2878 de 2026, el cual quedará así:

"2.5.5.3. Recursos de cómputo y procesamiento

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

- ☐ **Servidores:** Equipos tipo servidor de rack, de tipo empresarial y de alta disponibilidad, organizados en granjas de servidores físicos y/o virtuales. Deberán contar con **procesadores multinúcleo** de alto rendimiento de última generación (CPU) y aceleradores gráficos (GPU) para cómputo de propósito general (GPGPU) con soporte a tecnologías como CUDA o Tensor Cores, para ejecutar cargas de inteligencia artificial, inferencias y análisis en tiempo real de datos.
- ☐ **Arquitectura de software:** La infraestructura deberá ser compatible con plataformas de virtualización y deberá permitir la implementación de entornos de contenedorización y orquestación basados en Kubernetes para garantizar escalabilidad, despliegue automatizado, balanceo de cargas y una gestión eficiente de los recursos computacionales. Los servidores también deberán ser compatibles con entornos de ejecución que soporten arquitecturas basadas en microservicios, facilitando la implementación de *pipelines* de procesamiento distribuido y la integración con herramientas de DevOps, CI/CD y gestión de clústeres.

Para implementar esta arquitectura, se debe contemplar una etapa de realización de pruebas funcionales con el RUNT, a fin de evitar traumatismos en la prestación de servicios en los CDA y en el registro de información que allí se carga. El operador homologado deberá documentar y ejecutar estas actividades de manera previa a la entrada en producción, efectuando las validaciones técnicas necesarias, la migración progresiva de la información histórica y garantizando en todo caso la continuidad del servicio, la integridad de la información y la correcta interoperabilidad entre los sistemas.

- ☐ **Resiliencia y tolerancia a fallos:** El sistema debe garantizar tolerancia a fallos, auto-recuperación de servicios y escalabilidad horizontal dinámica,

RESOLUCIÓN No 009981 DE 6 agosto 2026

"Por medio de la cual se modifica la Resolución 2878 de 2026 y su Anexo Técnico, se ajustan disposiciones relativas al periodo de implementación del Sistema de Control y Vigilancia para los CDA, y se dictan otras disposiciones"

permitiendo el aprovisionamiento y redistribución automática de cargas en función de la demanda de procesamiento analítico o de inferencia.

☐ **Arquitectura de Software – Requerimientos técnicos y de seguridad**

La infraestructura deberá soportar una arquitectura moderna, resiliente y escalable, compatible con plataformas de virtualización de nivel empresarial y comportarse como una nube privada, garantizando elasticidad, aislamiento de cargas de trabajo, alta disponibilidad y administración centralizada. Deberá permitir la implementación de entornos de contenedorización y orquestación basados en tecnologías de contenedores (Docker, kubernetes, Containerd), asegurando auto-escalamiento, despliegue automatizado, balanceo de cargas inteligente, auto-recuperación y gestión eficiente del consumo computacional. La arquitectura deberá ser totalmente compatible con modelos basados en microservicios, pipelines de procesamiento distribuido e integración continua con herramientas DevOps, CI/CD e infraestructura como código (IaC).

Desde la perspectiva de seguridad y cumplimiento normativo, la infraestructura deberá alinearse con los controles establecidos en ISO 27001:2022 (Seguridad de red, Seguridad en desarrollo, Monitoreo, Registros, Seguridad en entornos de desarrollo, prueba y producción y Seguridad en servicios en la nube), así como con los principios de SOC 2 orientados a Seguridad, Disponibilidad y Procesamiento Íntegro. Se deberán aplicar estándares de la industria como NIST CSF, Zero Trust Architecture (NIST 800-207), CIS de tecnología de contenedores y las guías de endurecimiento del NSA/CISA para clústeres tecnología de contenedores.

Requerimientos mínimos de seguridad para tecnología de contenedores.

- ☐ El proveedor deberá garantizar que el entorno tecnología de contenedores. cumpla como mínimo con los siguientes controles de seguridad:
- ☐ Implementación de RBAC (Role-Based Access Control) con privilegios mínimos y segregación estricta de funciones.
- ☐ Segmentación mediante Namespaces, con políticas de aislamiento y control de recursos (Resource Quotas, LimitRanges).
- ☐ Uso de Network Policies para controlar el tráfico interno, evitando comunicación no autorizada entre pods o microservicios.
- ☐ Cifrado obligatorio en tránsito (TLS 1.2+) y en reposo para volúmenes, secretos y comunicaciones entre componentes del clúster.
- ☐ Gestión segura de secretos mediante herramientas nativas (Secrets, KMS) o externas (Vault).
- ☐ Escaneo automático de imágenes con análisis de vulnerabilidades previo al despliegue en clúster.
- ☐ Restricción de ejecución privilegiada y políticas de seguridad de pods (PSPs o Pod Security Standards).
- ☐ Auditoría activa del clúster mediante API Audit Logs, monitoreo de integridad y observabilidad con OpenTelemetry, Prometheus, Grafana u otros equivalentes.
- ☐ Hardening del plano de control y nodos de trabajo, con rotación de certificados, autenticación fuerte e integración con IdP corporativo.

RESOLUCIÓN No 009981 DE 6 agosto 2026

"Por medio de la cual se modifica la Resolución 2878 de 2026 y su Anexo Técnico, se ajustan disposiciones relativas al periodo de implementación del Sistema de Control y Vigilancia para los CDA, y se dictan otras disposiciones"

- ☐ Mecanismos de alta disponibilidad, backups consistentes, pruebas de recuperación y resiliencia ante fallos.

Criterios de aceptación

Para validar el cumplimiento técnico y de seguridad de la solución, se establecen los siguientes criterios de aceptación:

- ☐ La arquitectura deberá estar documentada con topologías de red, flujos de datos, componentes del clúster, políticas de seguridad y segregación de ambientes.
 - ☐ LA tecnología de contenedores deberá cumplir con los estándares mínimos definidos por CIS Benchmark y evidenciarse mediante reportes de hardening y pruebas automáticas de cumplimiento.
 - ☐ El proveedor deberá demostrar la ejecución de pipelines CI/CD seguros con control de versiones, validación automatizada, auditoría y trazabilidad completa de despliegues.
 - ☐ El entorno deberá ser sometido a pruebas de rendimiento, alta disponibilidad y resiliencia, incluyendo simulaciones de fallos de nodos, pods y servicios.
 - ☐ La solución deberá pasar pruebas de seguridad (SAST, DAST, análisis de contenedores, escaneo de imágenes) y entregar los reportes derivados.
 - ☐ Las políticas RBAC, Network Policies, controles de cifrado y logs deberán verificarse mediante revisión técnica y evidencia generada por el clúster.
 - ☐ Se deberá presentar un plan de continuidad y recuperación ante desastres, validado mediante ejercicios prácticos o evidencias de backup/restore funcionales.
 - ☐ Se aceptará la solución únicamente cuando todos los controles de seguridad definidos cumplan y queden alineados con los requerimientos normativos de ISO 27001 y SOC 2.
- ☐ **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."

Artículo 6. Modifíquese el literal (d) del numeral 2.5.8.4. del Anexo Técnico adoptado a través de la Resolución 2878 de 2026, el cual quedará así:

"d) Firma manuscrita digitalizada o firma digital: El SICOV deberá permitir la captura, registro, conservación y consulta de la manifestación de voluntad de los usuarios del servicio y del personal del CDA, a través de su firma manuscrita mediante dispositivo digitalizador o dispositivos móviles equivalentes, o de su firma digital, conforme a lo que a continuación se señala:

RESOLUCIÓN No 009981 DE 6 agosto 2026

"Por medio de la cual se modifica la Resolución 2878 de 2026 y su Anexo Técnico, se ajustan disposiciones relativas al periodo de implementación del Sistema de Control y Vigilancia para los CDA, y se dictan otras disposiciones"

- 1) Pad de firmas digitalizador: dispositivo físico destinado a la captura de la firma manuscrita digitalizada de los usuarios del servicio y del personal del CDA.
- 2) Dispositivos móviles: equipos móviles, tabletas, teléfonos inteligentes u otros dispositivos tecnológicos equivalentes, que permitan la captura segura de la firma manuscrita digitalizada o de la manifestación de aceptación del titular, siempre que se garantice trazabilidad, integridad, autenticidad, disponibilidad, conservación y consulta posterior de la evidencia.

Estos mecanismos deberán garantizar autenticidad, integridad, trazabilidad, disponibilidad, conservación y consulta posterior de la evidencia, así como la asociación inequívoca entre la manifestación de voluntad, el titular de la información, la fecha, hora, sede, canal, dispositivo utilizado y finalidad informada.

La manifestación de voluntad también podrá soportarse mediante mecanismos de firma digital basados en certificados digitales emitidos por entidades de certificación digital acreditadas ante el Organismo Nacional de Acreditación de Colombia — ONAC, o quien haga sus veces, conforme a la Ley 527 de 1999 y demás normas que la modifiquen, adicionen, sustituyan o reglamenten.

Los mecanismos aquí previstos servirán para obtener y conservar 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 de manera clara sobre las finalidades del tratamiento, el uso de tecnologías de validación biométrica, reconocimiento facial, monitoreo de permanencia, conservación de evidencias, trazabilidad de operaciones y demás aspectos relevantes conforme a la Ley 1581 de 2012, sus normas reglamentarias y las políticas de tratamiento de información aplicables."

Artículo 7. Modifíquese el numeral 2.5.8.5. del Anexo Técnico adoptado a través de la Resolución 2878 de 2026, el cual quedará así:

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

El Sistema de Control y Vigilancia deberá asegurar que todo usuario (tenedor del vehículo) y miembro del personal de un CDA (personal técnico de inspección, y director(es) técnico(s)) 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 comenzará con la verificación de identidad de la persona a través del cotejo de sus minucias dactilares contra la réplica de la base de datos de la RNEC y la consulta en las bases de datos biográficas (Archivo Nacional de Identificación).

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

RESOLUCIÓN No 009981 DE 6 agosto 2026

"Por medio de la cual se modifica la Resolución 2878 de 2026 y su Anexo Técnico, se ajustan disposiciones relativas al periodo de implementación del Sistema de Control y Vigilancia para los CDA, y se dictan otras disposiciones"

- Por parte de todos los usuarios (tenedores del vehículo) y miembros del personal de un CDA (inspectores y directores técnicos), al momento del primer acceso o enrolamiento formal en el Sistema.
- Por parte de los ingenieros certificadores, como mecanismo alternativo en caso de no resultar satisfactoria la validación de identidad con el mecanismo de reconocimiento facial, falla o indisponibilidad de dicho servicio.

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

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 bajo el último anexo técnico vigente de esa entidad, 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 condicionado): Se empleará tecnología de reconocimiento facial como mecanismo de verificación principal, una vez esta sea reglamentada, autorizada para su uso en este contexto por la RNEC y provista a través de un operador de validación biométrica debidamente habilitado.

En ausencia o indisponibilidad de este mecanismo principal, mientras no esté plenamente operativo, o mientras no sea autorizado por la Superintendencia de Transporte, se utilizará por defecto el 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.

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 cinco (5) 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.

d) Protocolo de inconsistencia de identidad y actualización de datos biométricos: Si tras realizar tres (5) intentos de cotejo biométrico dactilar contra la base de datos de la RNEC, y posteriormente tres (3) intentos de validación de reconocimiento facial (selfie vs. documento

RESOLUCIÓN No 009981 DE 6 agosto 2026

"Por medio de la cual se modifica la Resolución 2878 de 2026 y su Anexo Técnico, se ajustan disposiciones relativas al periodo de implementación del Sistema de Control y Vigilancia para los CDA, y se dictan otras disposiciones"

original), el resultado persiste como negativo o inconsistente, el sistema bloqueará de manera inmediata el inicio o la continuación de cualquier servicio.

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

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

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

Los resultados de las consultas realizadas al momento del enrolamiento, exitosas o fallidas, quedarán registrados de manera inalterable en los logs del sistema con fecha, hora, tipo de documento consultado, resultado de la consulta y, cuando aplique, la acción adoptada por el sistema."

Artículo 8. Modifíquese el numeral 2.5.8.7. del Anexo Técnico adoptado a través de la Resolución 2878 de 2026, el cual quedará así:

"2.5.8.7. Validación continua de identidad de los inspectores técnicos y del director técnico.

El Sistema de Control y Vigilancia deberá implementar y ejecutar un proceso robusto y continuo de validación de la identidad de los inspectores técnicos del CDA durante todas las etapas del proceso de inspección técnica vehicular.

1. Mecanismos biométricos de validación: El SICOV utilizará los siguientes mecanismos biométricos para las validaciones de identidad continuas:

a) Reconocimiento facial: Validación Selfie/fotografía vs. template:

Como mecanismo ágil de verificación, comparando una imagen facial capturada en tiempo real contra el patrón biométrico de referencia (template) previamente registrado en el SICOV para cada integrante del equipo técnico. Este será el mecanismo de validación de identidad principal. Este mecanismo de identificación permitirá validar en tiempo real la identidad del personal operativo en la pista de inspección, permitiendo realizar procesos de identificación biométrica contra el subsistema ABIS mediante esquemas 1:N.

RESOLUCIÓN No 009981 DE 6 agosto 2026

"Por medio de la cual se modifica la Resolución 2878 de 2026 y su Anexo Técnico, se ajustan disposiciones relativas al periodo de implementación del Sistema de Control y Vigilancia para los CDA, y se dictan otras disposiciones"

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 en caso de que no se logre o no sea posible hacer una verificación exitosa mediante el cotejo a través de la tecnología de reconocimiento facial.

2. Momentos de validación: El SICOV deberá exigir y registrar la validación de identidad de los inspectores técnicos **al inicio y al finalizar cada prueba de la RTMyEC.**

El CDA sólo podrá iniciar cada prueba y transmitir los resultados al SICOV una vez el inspector haya validado su identidad satisfactoriamente conforme a lo aquí dispuesto; razón por la cual el inicio de la prueba estará restringido hasta tanto dicha validación de identidad inicial se realice de manera exitosa.

Al validar su identidad al finalizar cada prueba, el inspector afirmará, a través de la interfaz del sistema y con la validación de su identidad al cierre de la prueba, que certifica que el proceso y el resultado de la inspección realizada a dicho vehículo son veraces y que no han sido manipulados, alterados o modificados. Este aviso deberá ser visible para el inspector en el(los) equipo(s) o dispositivo(s) del SICOV de los que se disponga para efectuar la validación de identidad.

El software de gestión y control del SICOV debe, por lo tanto, informar al CDA, a través del software y tecnología de generación de resultados de la RTMyEC que este emplee, del resultado exitoso de validación inicial y final de identidad del inspector, para el inicio y cierre de la prueba respectivamente.

Los intentos de validación de identidad deberán guardar los registros (logs) con la información de su realización. La validación de identidad satisfactoria habilitará la realización de la prueba. Su resultado, tras su realización y cierre, deberá ser transmitido inmediatamente al software de gestión y control del SICOV.

El evento de validación exitosa de identidad al cierre de la prueba respectiva, dará paso a la realización de la siguiente, y así sucesivamente hasta terminar la inspección. Sin la validación exitosa inicial, la Superintendencia mantendrá restringida la opción de recepción de información de resultados de pruebas.

Para efectos de lo anterior, el SICOV debe garantizar que las cámaras y demás dispositivos de videovigilancia empleados para la grabación de las pruebas en pista cuenten con la tecnología de reconocimiento facial que permita la identificación biométrica en tiempo real del personal técnico mediante su integración con el subsistema ABIS, bajo esquemas de identificación 1:N y 1:1.

La tecnología incorporada debe garantizar el procesamiento de las capturas de video para comparar los rostros detectados contra el sub sistema ABIS, garantizando niveles adecuados de precisión y tiempos de respuesta acordes con la operación. Asimismo, el sistema deberá generar alertas automáticas

RESOLUCIÓN No 009981 DE 6 agosto 2026

"Por medio de la cual se modifica la Resolución 2878 de 2026 y su Anexo Técnico, se ajustan disposiciones relativas al periodo de implementación del Sistema de Control y Vigilancia para los CDA, y se dictan otras disposiciones"

ante la presencia y detección de personas (rostros) no identificadas o no registradas en el subsistema ABIS que se encuentren en la pista, dejando trazabilidad precisa de tales circunstancias a través del registro de eventos y notificación al CDA y al CPD Analítico y de Información de la Superintendencia para la gestión oportuna de situaciones de riesgo.

3. Validación de identidad del personal que valida el FUR: La validación de la identidad del (los) ingeniero(s) designado(s) y registrado(s) en el SICOV por el CDA para validar los resultados consignados en el FUR y constatar que la RTMyEC se haya hecho completa y satisfactoriamente, se realizará obligatoriamente en la etapa final del proceso. Esta validación se efectuará con tecnología de reconocimiento facial 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 CDA sobre cualquier indisponibilidad del servicio, sus causas y el plan de contingencia. Cuando la indisponibilidad sea del servicio de consulta contra las réplicas de las bases de datos de la RNEC, la comunicación a través de la cual se brinde esta información deberá ir suscrita conjuntamente con el operador biométrico autorizado por esa entidad, cuando estos dos sean personas distintas."

Artículo 9. Modifíquese el literal h) del numeral 2.5.8.11. del Anexo Técnico adoptado a través de la Resolución 2878 de 2026, el cual quedará así:

"h) Reporte de novedad por reingreso a pista o reversa en pista: En el registro deberá quedar traza y reporte de novedad asociada al momento en que un mismo vehículo sea detectado ingresando más de una vez a la pista en un lapso de dos horas desde el primer ingreso y/o cuando de reversa en la pista.

Cada servicio en el que ocurra esto será marcado automáticamente en el Sistema y generará una alerta para su análisis posterior por parte de la Superintendencia de Transporte a través del operador homologado.

Todo reingreso a pista deberá ser solicitado por el Centro de Diagnóstico Automotor (CDA) al operador homologado del SICOV mediante mesa de servicio, dejando registro de la justificación técnica que motiva la solicitud y de la autorización otorgada.

RESOLUCIÓN No 009981 DE 6 agosto 2026

"Por medio de la cual se modifica la Resolución 2878 de 2026 y su Anexo Técnico, se ajustan disposiciones relativas al periodo de implementación del Sistema de Control y Vigilancia para los CDA, y se dictan otras disposiciones"

El reingreso a pista únicamente procederá cuando se configure alguna de las siguientes circunstancias:

- a) Se evidencie la omisión involuntaria de una o varias actividades o pruebas que hagan parte del procedimiento de inspección.
- b) Exista imposibilidad de culminar una o varias pruebas como consecuencia de una falla súbita del vehículo inspeccionado.
- c) Se presente una falla en alguno de los equipos de inspección del CDA que afecte la confiabilidad o validez de la prueba realizada.
- d) El usuario desista de continuar con la inspección antes de la realización de cualquiera de las pruebas, sin que se haya emitido un resultado final.
- e) Se presente una contingencia externa que impida la culminación normal del servicio, tales como indisponibilidad del RUNT, del SICOV, de la plataforma de recaudo o de otros sistemas indispensables para la prestación del servicio.
- f) Cualquier otro evento excepcional previamente autorizado por la Superintendencia de Transporte o definido por el Comité Técnico Operativo.

El operador homologado del SICOV deberá validar que la causal invocada corresponda con la evidencia técnica disponible, dejando trazabilidad y registros históricos por cada Centro de Diagnostico Automotor que realice estas solicitudes.

Cuando el operador homologado evidencie que existe información suficiente para concluir que la inspección fue ejecutada correctamente y, aun así, el CDA solicite un reingreso a pista sin una justificación técnica válida, el SICOV generará una marcación de irregularidad del servicio, dejando la respectiva alerta visible en el MOCVI para la Superintendencia de Transporte.

Los operadores homologados deberán consolidar y reportar mensualmente a la Superintendencia de Transporte, a través del MOCVI, un informe con las estadísticas de reingresos a pista, discriminadas por CDA, causal invocada, línea de inspección, tipo de vehículo y demás variables que se lleguen a determinar, con el fin de identificar patrones de comportamiento, riesgos operacionales o posibles mecanismos de alteración de los procesos de inspección."

Artículo 10. Modifíquese el numeral 2.5.8.14. del Anexo Técnico adoptado a través de la Resolución 2878 de 2026, el cual quedará así:

"2.5.8.14. Integración/interoperabilidad con el software y tecnología de generación de resultados del CDA.

El Sistema de Control y Vigilancia deberá facilitar un mecanismo de integración y/o consulta que le permita recibir y consultar en tiempo real los resultados de las pruebas de RTMyEC que se realicen con apoyo en equipos especializados (frenómetro, luxómetro, detector de holguras, analizador de gases, etc.) de manera inmediata una vez estos se encuentren disponibles de manera parcial y total para su registro en el SICOV, y de las pruebas visuales y sensoriales de manera directa y de primera mano, sin intervención de cualquier tipo que ponga en riesgo la integridad de la información.

Para ello, el CDA deberá asegurarse de que su software y tecnología de generación de resultados garantice la transmisión de los resultados de las

RESOLUCIÓN No 009981 DE 6 agosto 2026

"Por medio de la cual se modifica la Resolución 2878 de 2026 y su Anexo Técnico, se ajustan disposiciones relativas al periodo de implementación del Sistema de Control y Vigilancia para los CDA, y se dictan otras disposiciones"

pruebas realizadas con sus equipos, de manera inmediata y automatizada, sin intervención humana y sin retraso de tiempo, justo en el momento en que estos resultados estén disponibles, luego de ser realizadas las pruebas parciales y totales durante el proceso de inspección.

En cualquier caso, los resultados parciales y totales deben estar disponibles lo antes posible para permitir una sincronización con el video capturado por el homologado SICOV con no más de 3 segundos de retraso o diferencia. Para lograr este propósito, el operador homologado definirá un protocolo para la entrega de los resultados. Cada transmisión deberá indicar, como mínimo, la siguiente información:

- a) ID de la inspección.
- b) Placa del vehículo.
- c) Prueba.
- d) Paso o identificación de la secuencia del resultado durante la prueba.
- e) Datos del resultado.
- f) Si está repitiendo un paso (o toda la prueba) ya ejecutado (indicando el motivo, por ejemplo datos incoherentes o fallas del operario o equipo durante la ejecución).

En caso de que el software y tecnología de generación de resultados de un CDA no cuente con la capacidad de entregar de manera inmediata los datos parciales de las pruebas que se realizan, por depender de la entrega de resultados totales por parte de los equipos al finalizar la prueba, será el SICOV quien defina el procedimiento bien sea que tome los datos directamente de los equipos o por medio de requerimientos de ciberseguridad como requisito de seguridad e inalterabilidad de los resultados.

Entre el momento de inicio y finalización de las siguientes pruebas, se deben remitir los siguientes resultados parciales al homologado SICOV:

g) Prueba visual:	- Defectos encontrados en cada sección visual correspondiente de acuerdo con la configuración adoptada por el CDA conforme a las instrucciones impartidas en el presente Anexo (inferior, exterior, motor, interior, etc).
h) Prueba de frenos:	- Cero de sensores e inicio de la prueba. - Pesos al finalizar la medición en cada rueda por eje (puede provenir de báscula integrada, báscula externa o del probador de suspensión). - Fuerzas registradas en cada rueda por eje del vehículo, tanto para freno de servicio como para freno auxiliar o de parqueo.
i) Prueba de suspensión:	- Peso estático al finalizar la medición de cada rueda por eje. - Adherencia al finalizar la vibración de la placa por cada rueda por eje.
j) Prueba de Alineación al paso:	- Desviación lateral reportada al terminar cada eje.
k) Prueba de	- Resultados de error en distancia al finalizar el recorrido

RESOLUCIÓN No 009981 DE 6 agosto 2026

"Por medio de la cual se modifica la Resolución 2878 de 2026 y su Anexo Técnico, se ajustan disposiciones relativas al periodo de implementación del Sistema de Control y Vigilancia para los CDA, y se dictan otras disposiciones"

Taxímetro:	- Resultados de error en tiempo al finalizar el paso.
l) Prueba de Luces:	- Resultado de intensidad de luz baja por cada faro correspondiente. - Resultado de inclinación de luz baja por cada faro correspondiente. - Resultado de intensidad de luz alta por cada faro correspondiente. - Resultado de intensidad de luz antiniebla por cada faro correspondiente. - Resultado de inclinación de luz antiniebla por cada faro correspondiente. - Sumatoria de la intensidad de luces que se pueden encender simultáneamente en el vehículo (cuando aplique) - Simultaneidad de las luces de acuerdo con la configuración aplicable a cada vehículo.
m) Prueba de sonido:	- Resultados parciales de sonido de acuerdo con el procedimiento del CDA.
n) Prueba de gases:	- Paso de condiciones iniciales y lecturas del Termohigrómetro - Resultados de la comprobación visual previa del vehículo. - Datos leídos por el equipo una vez terminada la prueba de residuos. - Momento en el que se detecta el gas circulando por el equipo (CO2 >1% y O2 < 20%) - v) RMP, temperatura (si aplica) y datos de gases al inicio de los 30s en ralentí. - Datos arrojados por el equipo durante todo el ciclo de aceleración a velocidad crucero y ralentí. - Consolidado (promedio de los últimos 5 segundos) de RPM, temperatura y datos de gases al finalizar los 30s en ralentí. - RMP, temperatura y datos de gases al inicio de los 30s en crucero (si aplica). Consolidado (promedio de los últimos 5 segundos) de RPM, temperatura y datos de gases al finalizar los 30s en crucero (si aplica)
o) Prueba Diesel:	- Paso de condiciones iniciales y lecturas del Termohigrómetro. - Resultados de la comprobación inicial previa del vehículo. - RPM y temperatura inicial y final del motor (según aplique) en ralentí - RPM en crucero cuando se haga la aceleración súbita de prueba. - Resultado de limpieza y por aceleración y resultado total.

Para cualquiera de las pruebas, el proveedor tecnológico del software y tecnología de generación de resultados debe informar de manera inmediata al operador homologado SICOV siempre que se modifiquen los valores de ajuste, tanto para valores almacenados en el mismo sistema de inspección como para

RESOLUCIÓN No 009981 DE 6 agosto 2026

"Por medio de la cual se modifica la Resolución 2878 de 2026 y su Anexo Técnico, se ajustan disposiciones relativas al periodo de implementación del Sistema de Control y Vigilancia para los CDA, y se dictan otras disposiciones"

ajustes hechos con el software de inspección propiamente en el hardware de los equipos.

Para asegurar el cumplimiento de lo aquí previsto, se debe garantizar la sincronización precisa de horarios de los sistemas, lo cual es necesario para garantizar consistencia y trazabilidad de los datos.

En los eventos en que se repitan pruebas totales o parciales, el SICOV deberá registrar todas las ejecuciones y sus respectivos resultados, preservando el histórico completo para efectos de auditoría y control.

El SICOV deberá permitir la visualización y consulta de esta información en el Módulo de consulta, IVC e inteligencia de negocio (MOCVI) del CPD-Analítico.

(...)"

Artículo 11. Modifíquese el ordinal 4 del numeral 2.5.8.19. del Anexo Técnico adoptado a través de la Resolución 2878 de 2026, el cual quedará así:

"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 CDA 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 activará el mecanismo escalonado de respuesta previsto en los literales (c) y (h) del presente numeral. 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 registrado 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 CDA preste y registre en el SICOV 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.

Esta marcación operará desde el instante mismo del vencimiento del documento crítico, sin perjuicio de lo previsto en el literal (h) del presente numeral respecto de la ventana de operación de cuatro (4) horas."

d) Categorización de la revisión como "No realizada". Las inspecciones que generen la marcación de irregularidad por los motivos aquí expuestos se

RESOLUCIÓN No 009981 DE 6 agosto 2026

"Por medio de la cual se modifica la Resolución 2878 de 2026 y su Anexo Técnico, se ajustan disposiciones relativas al periodo de implementación del Sistema de Control y Vigilancia para los CDA, y se dictan otras disposiciones"

clasificarán automáticamente como "No realizadas" conforme a lo desarrollado en el presente Anexo.

e) Registro detallado del incumplimiento: El SICOV registrará y mantendrá un historial detallado de cada alerta generada por incumplimiento documental, incluyendo la fecha y hora de la detección, el documento específico faltante o vencido, y el estado de la evidencia enviada al CDA.

f) 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 que le permitirán visualizar en línea, entre otras cosas, las alertas activas por CDA, así como cuantificar y detallar el número de servicios y certificados de RTMyEC "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, el servicio afectado, información del(los) inspector(es), certificador(es), y del tenedor del vehículo para la RTMyEC específica.

g) 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, apoyándose en el proveedor homologado del Sistema, de los documentos cargados en un plazo máximo de cinco (5) días hábiles con el apoyo de los proveedores homologados del Sistema.
3. Una vez validada satisfactoriamente la subsanación por parte del CDA, se procederá al cese de la alerta en el Sistema. 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.

h) Restricción progresiva del uso de recursos del SICOV ante el vencimiento de documentos críticos:

Desde el momento exacto del vencimiento de un documento crítico, el SICOV activará simultáneamente la alerta temprana por incumplimiento y la marcación de irregularidad sobre todos los servicios que se presten bajo esa condición, conforme a lo previsto en los literales (b) y (c) del presente numeral.

RESOLUCIÓN No 009981 DE 6 agosto 2026

"Por medio de la cual se modifica la Resolución 2878 de 2026 y su Anexo Técnico, se ajustan disposiciones relativas al periodo de implementación del Sistema de Control y Vigilancia para los CDA, y se dictan otras disposiciones"

Sin perjuicio de lo anterior, el SICOV permitirá al organismo de apoyo continuar utilizando los recursos del sistema durante las cuatro (4) horas calendario siguientes a la fecha exacta del vencimiento.

Vencidas las cuatro (4) horas sin que el CDA haya cargado en el SICOV el documento actualizado que subsane el incumplimiento, para dar trámite a la verificación descrita en el literal (g), el Sistema activará automáticamente una restricción de uso de recursos, que restringirá al organismo de apoyo utilizar las funcionalidades del SICOV para realizar las validaciones de identidad del personal, asignar agenda, y en general para realizar otras operaciones que impliquen el uso de los recursos del sistema, hasta tanto cargue y se valide el documento actualizado que acredite el cumplimiento vigente del requisito crítico vencido, conforme a lo previsto en el literal (g). El cese de la restricción de uso de recursos operará una vez el organismo de apoyo cargue el documento actualizado y se verifique en el Sistema, por parte del operador homologado, su vigencia formal, conforme a lo previsto en el literal (g).

El sistema comunicará de manera inmediata al organismo de apoyo, a través de su correo electrónico, sobre: el vencimiento detectado y el documento específico que debe actualizarse; la activación de la alerta temprana y la marcación de irregularidad sobre los servicios prestados desde el vencimiento; el tiempo restante de la ventana de cuatro (4) horas antes de la activación de la restricción de recursos; y la activación de la restricción de recursos al vencimiento del plazo, con indicación del procedimiento para subsanar el incumplimiento y restablecer el acceso a los recursos del sistema."

Artículo 12. Modifíquese el numeral 2.5.11.1.1.1. del Anexo Técnico adoptado a través de la Resolución 2878 de 2026, el cual quedará así:

"2.5.11.1.1.1. Rack de equipos

Debe tener las siguientes características mínimas:

- Rack de piso, tipo metálico con pintura electrostática, con llave y con rodachinas.
- Altura mínimo de 1.80 metros, 38 Unidades de Rack.
- Tendrán mínimo dos extractores de desempeño industrial debidamente conectados a un circuito normal.
- Serán armados con sus respectivos organizadores y cuatro (4) rieles ajustables para equipos
- de 19" de ancho, además debe incluir un barraje de puesta a tierra (TGB).
- Tendrán vidrio templado en la parte frontal de la puerta con posibilidad de desmontar sus
- tapas laterales y traseras.
- El rack suministrará las multi-tomas con supresor de transientes y protección para aislamiento de circuitos, cuando se presente sobre corrientes en la red. Estas multi-tomas deberán estar conectadas a la UPS a través de un circuito independiente de la red regulada, realizando las adecuaciones eléctricas requeridas.
- Debe llevar bandejas porta equipos según la necesidad del sitio.
- Se tendrá una alerta por apertura y movimientos del rack, para monitoreo desde el SOC.

RESOLUCIÓN No 009981 DE 6 agosto 2026

"Por medio de la cual se modifica la Resolución 2878 de 2026 y su Anexo Técnico, se ajustan disposiciones relativas al periodo de implementación del Sistema de Control y Vigilancia para los CDA, y se dictan otras disposiciones"

Se dispondrá de una cámara IP para el monitoreo permanente del rack de comunicaciones y la generación de evidencia visual ante eventos de apertura, manipulación o acceso no autorizado. Esta cámara deberá cumplir como mínimo con las siguientes características:

- Tipo domo IP.
- Resolución mínima 1920 x 1080 (2 MP).
- Sensor CMOS de escaneo progresivo. Compresión H.265/H.264.
- Día/Noche con filtro IR mecánico (ICR).
- Iluminación infrarroja integrada con alcance mínimo de 20 m.
- Lente varifocal motorizado, con distancia focal aproximada entre 2.8 y 12 mm o equivalente.
- Ajuste remoto de zoom y enfoque desde la interfaz web o VMS, sin necesidad de desmontar la cámara.
- Alimentación PoE conforme IEEE 802.3af o 802.3at.
- WDR mínimo de 120 dB.
- Clasificación IP66 o superior.
- Clasificación IK10 (deseable).
- Al menos una entrada y una salida de alarma (opcional según la arquitectura del proyecto).
- Compatible con ONVIF Profile S y Profile T. El Rack deberá estar protegido a través de un sistema de cierre electrónico mediante un token con el fin de garantizar la seguridad de los equipos SICOV."

Artículo 13. Modifíquese el numeral 2.5.11.1.2. del Anexo Técnico adoptado a través de la Resolución 2878 de 2026, el cual quedará así:

"2.5.11.1.2. Lectores biométricos especializados de huellas

Los lectores de huellas especializados que se utilizarán para validar biométricamente la identidad de usuarios y personal del CDA deberán contar con homologación por parte de la Registraduría Nacional del Estado Civil (RNEC) bajo los estándares de la última versión del Anexo Técnico expedido por esa entidad.

Ubicación: Estos dispositivos deberán estar instalados (i) en la recepción de los CDA para el enrolamiento inicial del personal y los usuarios del servicio, así como (ii) en las líneas de inspección, para garantizar que se puedan realizar validaciones de identidad contra las réplicas de las bases de datos de la RNEC en caso de no resultar validada exitosamente la identidad del personal técnico con la tecnología de reconocimiento facial (selfie vs. Template), o en caso de indisponibilidad o falla de este servicio.

Estos lectores biométricos podrán estar incorporados/integrados en tabletas u otros dispositivos móviles que se utilicen como puntos de validación de identidad, siempre que esta integración sea segura y facilite la realización del proceso con eficiencia."

Artículo 14. Modifíquese el numeral 2.5.11.1.4. del Anexo Técnico adoptado a través de la Resolución 2878 de 2026, el cual quedará así:

RESOLUCIÓN No 009981 DE 6 agosto 2026

"Por medio de la cual se modifica la Resolución 2878 de 2026 y su Anexo Técnico, se ajustan disposiciones relativas al periodo de implementación del Sistema de Control y Vigilancia para los CDA, y se dictan otras disposiciones"

"2.5.11.1.4. Dispositivos para la validación de identidad en recepción, oficina de verificación de resultados y pista:

En línea con lo dispuesto en el numeral 2.5.11.1.2., los proveedores homologados del SICOV deberán suministrar y soportar dispositivos de ubicación fija o móvil que permitan la validación de identidad con tecnología de reconocimiento facial. Estos dispositivos deberán ser instalados o ubicados de la siguiente manera, según la naturaleza del servicio prestado por el organismo de apoyo:

1. Ubicación:

- La recepción y puntos de validación de los FUR en los CDA deben contar con puntos fijos de validación de identidad de propietarios y tenedores de vehículos y del personal certificador de las RTMyEC.
- Las pistas de los CDA deben contar con puntos móviles o fijos de validación de identidad del personal técnico de inspecciones.

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

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

3. Dispositivos de validación de identidad con biometría dactilar: Los puntos fijos de identificación con que cuente la sede del CDA, deberán contar con lectores biométricos dactilares, preferiblemente integrados de forma segura y dedicada en caso de ir acompañados de dispositivos móviles. Estos dispositivos funcionarán como mecanismo alternativo en caso de que no resulten exitosos los intentos de validación del personal técnico durante las pruebas con la tecnología de reconocimiento facial, o en caso de indisponibilidad o falla de este servicio."

Artículo 15. Modifíquese el numeral 2.5.11.1.7. del Anexo Técnico adoptado a través de la Resolución 2878 de 2026, el cual quedará así:

"2.5.11.1.7. Dispositivo digitalizador de firmas

Es el dispositivo móvil (smartphone o Tablet) o pad de firmas para la captura de la firma manuscrita digitalizada de los usuarios y personal del organismo de apoyo.

Este dispositivo 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."

RESOLUCIÓN No 009981 DE 6 agosto 2026

"Por medio de la cual se modifica la Resolución 2878 de 2026 y su Anexo Técnico, se ajustan disposiciones relativas al periodo de implementación del Sistema de Control y Vigilancia para los CDA, y se dictan otras disposiciones"

Artículo 16. Modifíquese el numeral 2.5.11.1.8. del Anexo Técnico adoptado a través de la Resolución 2878 de 2026, así:

“2.5.11.1.8. Infraestructura descentralizada para el reconocimiento facial.

El proveedor del SICOV deberá 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, tanto para enrolamiento del personal de inspección vehicular y de usuarios del servicio, como para la validación de identidad durante la realización de las RTMyEC.

El sistema debe reconocer sujetos que aparezcan simultáneamente en diversos flujos de video (streams) proporcionados por cámaras IP. Los equipos y la tecnología para el reconocimiento facial deben contar con lo mínimo exigido por fabricante (necesidades de GPU o CPU).

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

Al ser instalado en los centros, deberá disponerse del espacio necesario en el armario o rack de protección **existente** en el CDA y una UPS Online con autonomía de 4 horas para soportar la operación por caída del servicio de energía.

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 CDA.

La infraestructura debe cumplir con normativa de seguridad informática y protección de datos biométricos, asegurando trazabilidad y auditoría. Se relacionan, a continuación, las características mínimas de cada componente que se deberán garantizar para esta infraestructura específica:

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: 32GB DDR5
- Almacenamiento: Disco de Estado Sólido (SSD) de 1 TB ó Superior
- RAID: 5/6
- Puertos Ethernet RJ45: 2 x 1.5 GbE.
- Ranuras PCIe: 2 para expansión

RESOLUCIÓN No 009981 DE 6 agosto 2026

"Por medio de la cual se modifica la Resolución 2878 de 2026 y su Anexo Técnico, se ajustan disposiciones relativas al periodo de implementación del Sistema de Control y Vigilancia para los CDA, y se dictan otras disposiciones"

- Tarjeta de Video: 1 Unidad de procesamiento gráfico independiente con soporte para librerías de inteligencia artificial. Deberá contar con una memoria de video mínima de 12 GB, capaz de procesar inferencias de modelos biométricos en un tiempo no superior a dos (2) segundos por validación. Debe tener 192 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.

NAS

Requisitos mínimos:

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

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)."

Artículo 17. Modifíquese el numeral 2.5.11.2.1. del Anexo Técnico adoptado a través de la Resolución 2878 de 2026, el cual quedará así:

"2.5.11.2.1. Software de reconocimiento facial para validación de identidad.

a) Reconocimiento facial para enrolamiento y validación de FUR.

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 la comparación selfie vs. Documento y vs. template biométrico.

Este servicio específico será utilizado específicamente para el enrolamiento del personal vinculado al CDA y a los usuarios que presenten los vehículos para la RTMyEC. Así mismo, se utilizará para realizar las validaciones de identidad que deben efectuar los ingenieros certificadores de los resultados de la inspección vehicular.

RESOLUCIÓN No 009981 DE 6 agosto 2026

"Por medio de la cual se modifica la Resolución 2878 de 2026 y su Anexo Técnico, se ajustan disposiciones relativas al periodo de implementación del Sistema de Control y Vigilancia para los CDA, y se dictan otras disposiciones"

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.

El servicio debe tener mínimo las siguientes características:

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

Componentes técnicos:

El software de reconocimiento facial debe contar, como mínimo, 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.

Para el momento del enrolamiento inicial de usuarios y personal del CDA, la captura de fotografía 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).

2. **Algoritmo de reconocimiento de rostro vivo o liveness detection** (activo o pasivo) certificado por el NIST o por un laboratorio autorizado por el NIST en ataques de presentación PAD nivel 1 y 2 con fecha de presentación no mayor a dos años. El 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.

RESOLUCIÓN No 009981 DE 6 agosto 2026

"Por medio de la cual se modifica la Resolución 2878 de 2026 y su Anexo Técnico, se ajustan disposiciones relativas al periodo de implementación del Sistema de Control y Vigilancia para los CDA, y se dictan otras disposiciones"

- 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. Las constancias del cumplimiento de esta obligación se remitirán a la Superintendencia dentro del mes siguiente a la obtención de los resultados.

b) Reconocimiento facial para validación durante la realización de la RTMyEC

Este servicio específico será utilizado específicamente para realizar las validaciones de identidad que debe efectuar el personal de inspección técnica al inicio y al final de cada prueba.

La solución de reconocimiento facial que se debe utilizar en estos casos debe ser capaz de detectar y reconocer continuamente rostros de individuos registrados en el ABIS utilizando cámaras IP, aun cuando los sujetos se encuentren a distancia y en movimiento, y sin requerir ningún tipo de colaboración o asistencia. Deberá reconocer simultáneamente varias caras en el mismo flujo de vídeo, permitiendo el reconocimiento 1:N, y cumpliendo en todo caso los siguientes requisitos:

Velocidad de comparación: El algoritmo deberá tener la capacidad de comparar 100 millones de descriptores biométricos por segundo.

Velocidad de extracción de plantillas faciales: El sistema debe tener el rendimiento para extraer plantillas faciales con una velocidad de 1 milisegundo por rostro.

Formatos de imagen soportados: La solución de reconocimiento facial permitirá el registro de sujetos a partir de formatos de imagen estándares, como JPEG, JPG, PNG o BMP; así como ficheros NIST (estándar (ANSI/NIST-ITL 1-2000).

Formatos de vídeo soportados: La solución debe ser capaz de obtener el flujo de vídeo directamente de cámaras IP, y proporcionará medios para su integración en sistemas de gestión de vídeo (VMS). Será compatible con los protocolos MJPEG, H.264, H.265, RTSP y HTTP (modo snapshot) para la obtención de flujos de vídeo o fotogramas individuales.

Procesamiento de imágenes: La solución debe ser capaz de analizar 600 imágenes por segundo utilizando un sólo servidor mediante tecnologías GPU a una resolución de 1080p, o bien 125 imágenes por segundo en resolución 4K, y 25 fps a 8K. La generación de eventos debe producirse en el espacio de un segundo desde la recepción del frame para al menos el 90% del número total de eventos generados.

Cumplimiento de normas: El algoritmo de matcher debe haber estado en pruebas NIST."

RESOLUCIÓN No 009981 DE 6 agosto 2026

"Por medio de la cual se modifica la Resolución 2878 de 2026 y su Anexo Técnico, se ajustan disposiciones relativas al periodo de implementación del Sistema de Control y Vigilancia para los CDA, y se dictan otras disposiciones"

Artículo 18. Modifíquese el numeral 2.5.13.4. del Anexo Técnico adoptado a través de la Resolución 2878 de 2026, el cual quedará así:

"2.5.13.4. Subsistema ABIS y capacidades de Inteligencia Artificial

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

- 1. Subsistema ABIS (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), 1:1 (uno a uno) y 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."

Artículo 19. Actualización del Plan de Trabajo por los operadores homologados en régimen de transición. Los operadores homologados del Sistema de Control y Vigilancia que a la fecha de entrada en vigencia de la presente resolución se encuentren en régimen de transición presentarán ante la Superintendencia Delegada de Tránsito y Transporte Terrestre, dentro de los diez (10) días siguientes a dicha fecha, un Plan de Trabajo detallado actualizado conforme al nuevo cronograma de fases y fechas establecido en el Artículo 13 de la Resolución 2878 de 2026, modificado mediante la presente resolución.

Dicho plan contendrá como mínimo la desagregación de los hitos técnicos para el cumplimiento de cada fase, el cronograma de desarrollo, pruebas y despliegue de la arquitectura del SICOV para CDA, el plan de migración de datos históricos y la estrategia de socialización y gestión del cambio con los organismos de apoyo vinculados. La Superintendencia de Transporte, a través de esa Superintendencia Delegada, realizará el seguimiento al cumplimiento de los avances con base en este instrumento.

Artículo 20. Vigencia. La presente Resolución rige a partir de la fecha de su publicación en el sitio web de la Superintendencia de Transporte y en el Diario Oficial.

PUBLÍQUESE Y CÚMPLASE

RESOLUCIÓN No 009981 DE 6 agosto 2026

"Por medio de la cual se modifica la Resolución 2878 de 2026 y su Anexo Técnico, se ajustan disposiciones relativas al periodo de implementación del Sistema de Control y Vigilancia para los CDA, y se dictan otras disposiciones"



Alfredo Enrique
Piñeres Olave

ALFREDO ENRIQUE PIÑERES OLAVE
SUPERINTENDENTE

	Nombre del funcionario	Documento Firmado Digitalmente
Proyectó y elaboró	Carlos Daniel González Cervera	carlosgonzalez [27/julio/2026 08:01:52 p. m.]
Revisó	Alberto José Daza Sagbini	albertodaza [03/agosto/2026 05:42:13 p. m.]
Revisó	Luis Gabriel Serna Gámez	luisserna [05/agosto/2026 05:29:17 p. m.]
Aprobó	Alfredo Enrique Piñeres Olave	alfredopineres [06/agosto/2026 12:54:51 p. m.]