ANEXO TÉCNICO DEL SICOV PARA CENTROS DE APOYO LOGÍSTICO DE EVALUACIÓN

Este es el Anexo Técnico del Sistema de Control y Vigilancia para Centros de Apoyo Logístico de Evaluación del que trata la Resolución 8150 del 10 de junio 2026.

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 operación del SICOV: Detalla los requisitos de carácter administrativo, técnico y tecnológico que debe satisfacer el SICOV para CALE.

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

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 de los Centros de Apoyo Logístico de Evaluación frente al funcionamiento del Sistema.

TÍTULO 1

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 debe garantizar la infraestructura tecnológica del Sistema de Control y Vigilancia para los Centros de Apoyo Logístico de Evaluación (CALE).

Su objetivo primordial es garantizar que la infraestructura tecnológica de soporte asegure la integridad, calidad y seguridad en la prestación del servicio de evaluación teórico-práctico.

1.2. Objetivo del documento

El presente Anexo Técnico tiene como objetivo principal establecer los requerimientos técnicos y operativos que deben reunir los sistemas, componentes y servicios que conforman el Sistema de Control y Vigilancia.

1.3. Marco normativo

La existencia y funcionamiento de la infraestructura tecnológica del Sistema de Control y Vigilancia se fundamenta en primera medida en la necesidad de garantizar la transparencia en la evaluación de conductores, constituyendo. Su existencia se fundamenta principalmente 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 189, en virtud del cual le corresponde al Presidente de la República el ejercicio de las atribuciones de inspección y vigilancia de los servicios públicos y las actividades de que tratan los numerales 22, 24 y 25.
- La Constitución Política, en su artículo 150, que dicta que le corresponde al Congreso de la República expedir las normas a las cuales debe sujetarse el Gobierno para el ejercicio de las funciones de inspección y vigilancia que le señala la Constitución.
- 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 489 de 1998, en sus artículos 66 y 82, norma en la que el Legislador dispuso que las Superintendencias son organismos creados por la ley que cumplen funciones de inspección y vigilancia atribuidas por la ley o mediante delegación que haga el Presidente de la República.
- 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.
- 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.
- 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.
- 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.
- 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.
- Resolución número 20253040037125 de 2025 del Ministerio de Transporte, que reglamentó los requisitos de registro de los Centros de Apoyo Logístico de Evaluación (CALE) en el Registro Único Nacional de Tránsito (RUNT) y estableció las condiciones para la realización de los exámenes teórico y práctico de conducción que deben presentar los aspirantes para el otorgamiento de la licencia de conducción y su recategorización.

1.4. Alcance del documento

El presente Anexo Técnico define los requisitos a nivel técnico y operativo que debe reunir la infraestructura tecnológica de los sistemas que se implementen en los CALE.

TÍTULO 2

2. REQUERIMIENTOS PARA LA OPERACIÓN DEL SICOV PARA CALE

2.1. Requerimientos de recaudo y validación de identidad contra la RNEC

2.1.1. Aliado u operador de recaudo

El proveedor del sistema tecnológico contratado para operar el Sistema de Control y Vigilancia deberá garantizar el servicio de recaudo a través de operadores de recaudo que cumplan con los siguientes requisitos:

- 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.

- 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

- El aliado de recaudo deberá generar un número de identificación único de pago (PIN) a través de un proceso seguro que se realice a través de un algoritmo que concatene diferentes campos de información de la transacción, que culmine con un consecutivo secuencial, único e irrepetible.

  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, y 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, sean precisos.

- Encriptación de los datos que viajan a través de la red.

- Actualización en línea de lo recaudado.

- Debe tener constituido un esquema de replicación en línea de los datos.
- Debe emitir o generar comprobantes de recaudo, con posibilidades de emitir las copias que sean necesarias.

- Contar con redundancia de un CPD principal y un CAPD, que garantice la continuidad del servicio.

- Debe contar con dispositivos de seguridad perimetral en la red.

- Disponer de un canal de atención inmediata para los usuarios y/o clientes.

- Deber 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.

- 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.

- Debe contar con procedimiento para evitar que traten de falsificar comprobantes de recaudo.

- Debe suministrar la información requerida de la trazabilidad de cada operación de recaudo.

- Debe 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.

- Los aliados de recaudo deberán garantizar atención para resolver cualquier novedad, atender cualquier petición, reclamo o denuncia, por parte de cualquiera de los CALE a los que el proveedor tecnológico 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.

- El aliado de recaudo debe brindar la opción de pago a través de diferentes medios, tales como: pagos a través de internet, datáfonos o dispositivos satélites.

- El aliado de recaudo debe estar integrado con el CALE, a fin de que este 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.

- El aliado de recaudo debe 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.

- 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.

- El operador de recaudo debe constituir una póliza de cumplimiento a favor de cada CALE al que preste el servicio, por el buen manejo del dinero recaudado.

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

El proveedor del sistema tecnológico contratado para operar el Sistema de Control y Vigilancia deberá garantizar la autenticación biométrica contra las réplicas de las bases de datos de la Registraduría Nacional del Estado Civil, a fin de validar la identidad de los usuarios de los servicios prestados por los CALE.

Para ello, será necesario que las validaciones se hagan a través de un operador biométrico habilitado por la RNEC, de conformidad con la normatividad vigente aplicable.

2.2. REQUERIMIENTOS TÉCNICOS Y TECNOLÓGICOS

Este capítulo establece los requerimientos técnicos y tecnológicos mínimos del SICOV para CALE que deben ser garantizados.

A través de los distintos componentes que se desarrollan en este documento, se deberá garantizar la operación del Sistema y el óptimo desempeño de la totalidad de sus funcionalidades.

Los requerimientos y condiciones del Sistema, en razón de su naturaleza tecnológica, están sujetos a modificaciones.

Para la operación del SICOV, el proveedor de la solución tecnológica deberá garantizar el funcionamiento de los siguientes componentes:

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.

   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.

   El CPD provee la infraestructura fundamental para el almacenamiento seguro y el procesamiento de la información del SICOV, que se alimenta de la información de la Plataforma Tecnológica de los CALE, permitiendo la fiabilidad, seguridad, redundancia y diversificación de los datos y servicios.

2. **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).

3. **Red de Comunicaciones.** Se refiere a la infraestructura necesaria para interconectar los componentes que permiten el funcionamiento del Sistema de Control y Vigilancia en los Centros de Apoyo Logístico de Evaluación.

   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 (del recaudo, validaciones de identidad, gestión de recursos, etc.), pueda fluir desde los CALE hacia los servidores centrales en los que se alojan los componentes de software del SICOV, así como para la comunicación con sistemas externos de terceros involucrados con la operación. Permite la conectividad y el acceso a las redes de área extensa (WAN) e internet.

4. **Hardware y software requerido.** La operación del SICOV requerirá de la adquisición, disposición e instalación de dispositivos hardware (a nivel centralizado y descentralizado) y software que faciliten la integración con los operadores de recaudo, los operadores biométricos de RNEC, la plataforma tecnológica de los CALE y las herramientas propias del SICOV.

2.2.1. 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 CALE (CPD, CAPD) 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. En consecuencia, la infraestructura tecnológica deberá estar soportada por equipos de cómputo robustos, con alto poder de procesamiento y capacidad para ejecutar cargas operativas intensivas.

4. **Almacenamiento y conectividad resilientes:** Se requerirán sistemas de almacenamiento de alto rendimiento, capaces de soportar tanto las operaciones activas como los periodos de reposo de datos, incorporando esquemas de redundancia y tolerancia a fallos para asegurar la continuidad e integridad del servicio. La solución deberá incluir también equipos de comunicación como switches, routers y balanceadores de carga que garanticen la conectividad eficiente, segura y de alta disponibilidad entre todos los componentes del sistema.

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 de la operación del CALE.

   Para ello, se deberá contar con un Plan de Recuperación de Desastres (DRP) debidamente documentado y probado periódicamente, y un Plan de Continuidad del Negocio (BCP) que asegure la resiliencia de los servicios esenciales.

8. **Provisión de hardware:** El hardware necesario para el funcionamiento del Sistema de Control y Vigilancia en las sedes de los CALE así como aquellos componentes que deban ser instalados en los vehículos dispuestos para la evaluación.

   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 la sedes de los CALE y en los vehículos dispuestos para la evaluación.

2.2.2. Plan de Recuperación de Desastres (DRP)

La operación del SICOV exige que el proveedor tecnológico cuente 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.

El DRP deberá ser remitido a la Superintendencia de Transporte.

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

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

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

El Objetivo de Tiempo de Recuperación para el Sistema de Control y Vigilancia será de treinta (30) minutos. Esto significa que, ante cualquier interrupción o desastre que afecte la operación del SICOV, 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. Para sus estaciones remotas será de cuatro (4) horas.

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

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

2.2.3.3. Plataforma de Disaster Recovery

Los proveedores tecnológicos deberán incorporar dentro de su solución tecnológica una herramientas de recuperación crítica, que permitan cumplir con políticas de *Backup* de los servidores, almacenamiento y ambientes virtualizados.

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

2.2.4.1. Objetivo y estructura

Se 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.

2.2.4.2. Requisitos generales y certificación

El CPD y CAPD 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.

Lo anterior, por cuanto la disponibilidad exigida puede acreditarse mediante un mecanismo de verificación que reúna cuatro condiciones indispensables para que la Superintendencia de pueda verificar el cumplimiento de los requisitos a nivel de la infraestructura, como sucede con esta certificación:

- En primer lugar, la verificación debe realizarse por un organismo independiente del propio proveedor.
- En segundo lugar, la verificación debe ser física, esto es, realizada sobre la instalación real y no sobre sus especificaciones en papel o sus métricas históricas de disponibilidad.
- Los criterios de evaluación deben ser uniformes y aplicables de igual manera.
- El proceso de certificación debe ser realizado por un organismo técnico independiente con protocolos estandarizados internacionalmente reconocidos, cuya aplicación no dependa de la capacidad técnica propia de la Superintendencia para evaluar cada propuesta.

Estos recursos, cuyas características se detallan a continuación, deben ser de uso exclusivo para la operación del Sistema de Control y Vigilancia para CALE.

Es necesario advertir que la definición de Acuerdos de Nivel de Servicio (SLA) contractuales que comprometa porcentajes de disponibilidad equivalentes al

99,982% no es visto como una solución aceptable, en tanto que constituye un compromiso entre partes privadas verificable únicamente de manera retrospectiva, esto es, una vez que la falla ya ha ocurrido, mediante el análisis de logs, métricas históricas y reportes del propio proveedor. La Superintendencia de Transporte no cuenta con la capacidad técnica, humana ni presupuestal para auditar de manera permanente y uniforme la infraestructura de todos los proveedores tecnológicos del SICOV.

Por otra parte, dada la naturaleza eminentemente técnica de la infraestructura tecnológica, la facultad de decidir caso por caso si una arquitectura particular es equivalente al TIER III introduce un espacio de decisión no reglado que puede ser cuestionado y dar lugar a discusiones de carácter técnico que en el mercado aún no se han cerrado.

La exigencia de un estándar único, objetivamente verificable y aplicable de manera uniforme es, en consecuencia, la solución más consistente con los principios de seguridad jurídica, igualdad de condiciones y transparencia regulatoria que la propia Superintendencia de Industria y Comercio promueve en el ejercicio de la abogacía de la competencia.

Ahora bien, la exigencia de certificación TIER III no impone al proveedor tecnológico la obligación de construir su propia infraestructura certificada. El mercado colombiano cuenta con operadores de centros de datos que ya ostentan esta certificación, lo que permite a cualquier proveedor tecnológico acceder a infraestructura TIER III mediante modelos de arrendamiento de espacio, práctica que constituye un estándar en la industria TI a nivel global y en Colombia.

Esta circunstancia implica dos consecuencias relevantes desde la perspectiva de la proporcionalidad: en primer lugar, que los costos asociados a cumplir esta exigencia son los propios del arrendamiento de servicios de infraestructura ya existentes, no los de construir una instalación propia; y en segundo lugar, que la exigencia constituye un estándar mínimo de calidad verificable de manera independiente, uniforme para todos los participantes y accesible en el mercado colombiano a través de proveedores de infraestructura que ya operan en el país.

2.2.4.3. 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.
- **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 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.

2.2.4.4. Requerimientos de almacenamiento

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

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

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

- **Almacenamiento de Información en Reposo (NAS):** El subsistema **NAS** (*Network Attached Storage*) será destinado al almacenamiento de grandes volúmenes de información en reposo, incluyendo registros históricos, datos procesados y respaldos de largo plazo. Sus características clave incluirán:

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

2.2.4.5. Requerimientos de bases de datos

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

- **Arquitectura:** Deberá estar basado en una arquitectura distribuida, desplegable sobre entornos virtualizados y/o contenedorizados (Kubernetes), permitiendo su escalado automático.
- **Tipos de bases de datos:** La plataforma debe soportar bases de datos relacionales (SQL) para garantizar integridad referencial y consistencia ACID, y bases de datos NoSQL para soportar grandes volúmenes de datos semiestructurados y consultas de alta velocidad.
- **Alta disponibilidad y tolerancia a fallos:** Deberá garantizar la disponibilidad continua de los datos mediante mecanismos como

replicación síncrona y/o asíncrona entre nodos, con soporte para recuperación automática ante fallos (*failover* automático).
- **Despliegue y Respaldo:** Debe permitir el despliegue sobre volúmenes persistentes gestionados por Kubernetes.

2.2.4.6. Resiliencia y recuperación

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

- **Respaldo y recuperación:** El sistema debe usar herramientas para realizar copias de seguridad/backups en entornos seguros tales como unidades de cinta, dispositivos NAS, almacenamiento en la nube, o PBBA. Deberá contar con mecanismos de respaldo automatizado y programado con una retención mínima de 90 días hábiles, replicación en el CAPD, y gestión de snapshots y puntos de restauración.
- **Plan de respaldo:** Se 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.

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

2.2.4.8. Soporte remoto y gestión de servicios

Se 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:** 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.

2.2.4.9. 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**.

2.2.5. 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 debe proporcionar respuestas y soluciones a los usuarios finales, clientes o beneficiarios (destinatarios del servicio), y también puede otorgar asesoramiento en relación con una organización o institución, productos y servicios.

El servicio de Mesa de Ayuda debe estar disponible durante los horarios de atención presencial en la sede de los CALE, y desde una hora antes y una después de su apertura y cierre respectivamente

2.2.5.1. Operación técnica de la Mesa de Ayuda

El proveedor tecnológico deberá implementar un Punto Único de Contacto especializado, asegurando su accesibilidad tanto para usuarios técnicos como para usuarios sin conocimientos especializados en tecnología. A través de este mecanismo se deberán gestionar los requerimientos e incidentes técnicos reportados. La operación de este servicio se regirá bajo las siguientes condiciones

- **Herramienta de gestión:** Se deberá contar con un software de gestión de servicios TI que permita la trazabilidad completa del ciclo de vida de cada reporte (apertura, categorización, prioridad, niveles de escalamiento, resolución y cierre). Esta herramienta debe permitir la exportación de logs para auditoría de la Superintendencia de Transporte.
- **Canales de atención:** Se deberán garantizar, como mínimo, dos (2) canales de comunicación efectivos y concurrentes: uno de carácter sincrónico (vía telefónica o chat en tiempo real) y uno **asincrónico** (portal de autogestión o correo electrónico), asegurando la facilidad de uso tanto para perfiles técnicos como para personal administrativo de los CALE.
- **Especialidad del soporte:** El personal de la mesa de ayuda deberá contar con conocimiento específico en los módulos críticos del sistema, especialmente en: (i) procesos de validación biométrica y facial, (ii) gestión de recaudo y (iii) protocolos de interoperabilidad, con el fin de garantizar respuestas resolutivas en el primer nivel de contacto.

2.2.5.2. Procesos y gestión operativa

Se 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 CALE, se creará un ticket en la Mesa de Ayuda, a través de una herramienta de gestión de tickets. Los tickets creados deberán escalar hasta que el proveedor tecnológico brinde una solución o respuesta aceptable y/o cierre el caso luego de haber hecho la gestión correspondiente con el usuario.

2.2.5.3. Gestión del conocimiento y capacitación

Se deberá asegurar la actualización del conocimiento y la capacitación del personal de la Mesa de Ayuda:

Capacitación de analistas: Capacitar permanentemente a los analistas de la Mesa de Ayuda sobre el Sistema de Control y Vigilancia y sobre el uso y soporte de los dispositivos de hardware y software asociados a su operación.

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

Módulo de preguntas frecuentes (FAQ): Disponer de un módulo de preguntas frecuentes y actualizadas, accesible para el personal de los CALE.

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.

2.2.6. Funcionalidades tecnológicas del SICOV para los CALE

Este capítulo describe las funcionalidades y capacidades tecnológicas generales que el Sistema de Control y Vigilancia deberá garantizar en la operación de los Centros de Apoyo Logístico de Evaluación.

Muchas de las funcionalidades que a continuación se describen involucran actividades de registro de información, generación y almacenamiento de logs de la prestación del servicio, que requieren que el CALE parametrice su plataforma tecnológica, de tal manera que asegure su captura, para la consulta y transmisión automatizada que a través de los mecanismos de interoperabilidad se debe garantizar con el proveedor tecnológico del SICOV, conforme a lo que a continuación se describe en detalle.

2.2.6.1. 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 y fidedigna de cada CALE autorizado para operar.

Este registro integral incluirá, como mínimo, los siguientes datos:

a) Identificación legal y comercial: Nombre o razón social completa y/o información del establecimiento de comercio; 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.

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) Información adicional requerida: Cualquier otro dato o documento que la Superintendencia de Transporte determine como necesario.

2.2.6.2. Gestión y registro de pagos de servicios de evaluación del Examen Teórico y Práctico.

El Sistema deberá facilitar y garantizar el registro seguro del pago de la tarifa correspondiente a la prestación del servicio de evaluación de teoría y práctica en los CALE. 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.

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 la aprobación de la transacción por el valor completo del servicio a prestar por parte del CALE, más los valores que correspondan a servicios de terceros.

Adicionalmente, el PIN sólo se generará después de que a través del SICOV se verifique, a través de mecanismos de interoperabilidad, y en tiempo real, que el aspirante cuenta con:

1. 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;
2. Un Certificado de Aptitud en Conducción, expedido por un Centro de Enseñanza Automovilística (CEA) y;

Esta verificación previa se hará a través de mecanismos de interoperabilidad con la infraestructura tecnológica del SICOV para CRC y el SICOV para CEA y/o de interoperabilidad con el Registro Único Nacional de Tránsito (RUNT).

Mientras son implementadas las capacidades de interoperabilidad, el Sistema habilitará que esta información se registre haciendo la consulta directamente y en tiempo real, de forma manual, en el RUNT.

3. Que exista coincidencia territorial en las certificaciones, teniendo en cuenta lo siguiente:

   El SICOV verificará automáticamente que el CALE seleccionado por el aspirante se encuentre ubicado en el mismo departamento o en departamentos geográficamente contiguos al Organismo de Tránsito donde se realizará el trámite de expedición o recategorización de la licencia de conducción.

   Esta validación tiene como fin armonizar la etapa de evaluación con la validez territorial de los certificados de aptitud física, mental y de coordinación motriz definida en la Resolución 217 de 2014 y la Resolución 20253040037125 de 2025 del Ministerio de Transporte (o la norma que las modifique o sustituya), evitando que el ciudadano realice evaluaciones

en sedes que no tengan validez ante el Organismo de Tránsito de su elección.

Para tales efectos, el SICOV implementará un mecanismo de validación automática e inmediata previo a la generación del PIN. El sistema impedirá la transacción si el CALE seleccionado no se encuentra ubicado en el mismo departamento o en departamentos geográficamente contiguos al Organismo de Tránsito en el cual se adelantará el trámite; información que debe ser comunicada por el usuario. Para tales efectos, el proveedor tecnológico deberá integrar una matriz de contigüidad geográfica oficial que impida cualquier excepción manual a esta regla de jurisdicción.

b) Trazabilidad del recaudo: El Sistema deberá registrar la información de la transacción y de la entidad que procesó el recaudo. Para tal efecto, el operador de recaudo deberá transmitir al sistema, de manera inmediata y automatizada, a través de un mecanismo de interoperabilidad, la información precisa del pago recibido por parte del usuario del servicio, discriminando los valores dispersados o a dispersar a cada uno de los terceros, el tipo y número de documento de identidad del usuario que tomará el servicio, fecha y hora del ingreso del pago, tipo y número de documento de identificación de la persona natural o jurídica que realizó el pago y la categoría a la que aplicaría el examen teórico y/o práctico.

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) Integración transaccional para agendamiento en línea: Con el fin de facilitar el comercio electrónico y la autogestión del usuario, se permite el pago del servicio y recaudo de valores a terceros desde las plataformas o servicios de agendamiento que utilicen los CALE.

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, 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.

2.2.6.3. 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 CALE (personal administrativo, instructores, evaluadores) que interactúen con el Sistema.

Este registro, que realizará el CALE 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.

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 la 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 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 (al inicio, durante y después de la finalización de cada evaluación) de ese ciclo evaluativo específico, como se detalla más adelante.

c) Gestión de templates de referencia y trazabilidad histórica

Aunque dicho template será la referencia única para todas las validaciones de identidad dentro de ese ciclo evaluativo, el SICOV deberá implementar un versionamiento lógico de identidad bajo las siguientes reglas:

Archivo histórico de templates: Cada vez que un ciudadano inicie un nuevo proceso de evaluación (asociado a un nuevo pago o PIN), el sistema capturará un nuevo template de referencia, pero conservará de manera obligatoria los registros anteriores (imágenes) en un histórico vinculado al número de identificación.

Metadatos de Control: Por cada captura de referencia, el sistema almacenará metadatos de trazabilidad (fecha, hora y dispositivo utilizado).

Análisis de consistencia: El Sistema realizará comparaciones automáticas entre el nuevo template y los históricos. Si se detecta una diferencia biométrica con la tecnología de reconocimiento facial, el sistema disparará una alerta de "Posible irregularidad" por dicho servicio específico, la cual será visible en el Módulo de Supervisión y Control que se habilitará para el acceso de la Superintendencia de Transporte.

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

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

El proceso de registro de los usuarios del servicio y del personal vinculado al CALE se realizará en el área de recepción a través de los equipos de cómputo y los dispositivos periféricos dispuestos para dicho proceso (cámara fija o web, lector biométrico dactilar especializado, pad de firmas) o en los puntos de auto-registro ubicados en los CALE a través de kioscos o torres equipadas con los dispositivos periféricos necesarios.

Regla para el cotejo con reconocimiento facial

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

1. El proveedor tecnológico debe respetar obligatoriamente dichos niveles. Cualquier ajuste no autorizado será considerado una falta grave a la seguridad del sistema.

2. No se permiten aprobaciones manuales de identidad

2.2.6.4. Autenticación y verificación 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 CALE 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.

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.

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

- Fundamentalmente, por parte de todos los usuarios del servicio y miembros del personal directivo y operativo del CALE, **al momento del primer acceso o enrolamiento formal** en el Sistema, conforme a lo desarrollado en el presente Anexo.

- Por parte de todos los usuarios y personal de instructores y evaluadores de los CALE (según aplique), así:

    - Al inicio y al final de la realización de cada evaluación.

- Cuando lo requiera el Sistema, por indisponibilidad de la tecnología de reconocimiento facial, de acuerdo con las especificaciones y condiciones que llegue a definir 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 autorizados por la RNEC, los cuales deberán contar con funcionalidad certificada de detección de vida (liveness detection) de conformidad con lo establecido por esa entidad.

   b) Reconocimiento facial (mecanismo 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.

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

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

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

   El CALE 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).

   El proceso de evaluación quedará suspendido. No se permitirá al usuario avanzar en las fases de evaluación teórica ni práctica. Solo una vez que el ciudadano haya actualizado su información ante la autoridad competente y el SICOV logre una validación exitosa con el nuevo documento de identidad, podrá retomar el servicio.

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

2.2.6.5. Gestión del registro y control de información del personal vinculado a los CALE.

El Sistema deberá disponer de funcionalidades para llevar un registro detallado que se actualizase de manera permanente con la información de todo el personal vinculado a los CALE, incluyendo evaluadores, instructores, personal administrativo y directivo. 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. Al ser el CALE el responsable del registro directo de la información, el SICOV capturará automáticamente dicha información del CALE y con ella mantendrá actualizado el registro al que aquí se hace referencia.

1. **Registro inicial y estado del personal:**

a) Todo miembro del personal deberá ser registrado en el CALE previo al inicio de sus labores. Este registro inicial estará condicionado a la superación exitosa del procedimiento de enrolamiento y verificación de identidad contra las bases de datos de la RNEC, conforme a lo detallado en los numerales anteriores de este Anexo.

b) El CALE deberá llevar registro de la fecha de vinculación y, cuando ocurra, la fecha de desvinculación efectiva del personal, información que deberá ser actualizada diligentemente por el CALE.

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

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

a) Inactivación temporal por inactividad prolongada: El SICOV identificará automáticamente a aquellos instructores y evaluadores para los cuales no se registre actividad en la plataforma del CALE durante un periodo consecutivo de treinta (30) días calendario. En tal caso, el Sistema modificará el estado del evaluador o instructor a "inactivo temporalmente". El instructor o evaluador deberá realizar 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 o evaluador no ha hecho una nueva validación de su identidad en el CALE ante la RNEC, el Sistema cambiará su estado a "inactivo definitivamente". Para que el instructor o evaluador en este estado pueda volver a participar en evaluaciones, el CALE deberá realizar un nuevo proceso de registro inicial completo. La Plataforma tecnologógica dejará traza de dicho procedimiento.

c) Módulo de información detallada del personal: El Sistema deberá contar con un módulo específico para la consulta actualizada de la información detallada

del personal de instructores y evaluadores vinculado al CALE. Este módulo deberá permitir, como mínimo, el registro de:

- Tipo de vinculación contractual.
- Cargo o rol desempeñado. Para los instructores, las categorías para las cuales está autorizado.
- Número, categoría, fecha de expedición y vigencia de la licencia de conducción.
- Para los evaluadores, información de su licencia o certificado de idoneidad, con su respectiva vigencia.
- Certificados de títulos académicos y de formación relevantes para el desarrollo de sus actividades.
- Información sobre comparendos por infracciones a las normas de tránsito. En el caso en que hubiera registro de estas, deberá almacenarse obligatoriamente el paz y salvo del SIMIT. El proveedor verificará cada seis (6) meses en el RUNT que los instructores tengan vigente su licencia de conducción.

2.2.6.6. Interoperabilidad con otras infraestructuras SICOV.

Indistintamente de que la información que a continuación se indica pueda consultarse a través del mecanismo de interoperabilidad que se implemente con el RUNT, el proveedor tecnológico del SICOV debe también implementar mecanismos de interoperabilidad para el intercambio seguro de información con:

El SICOV para CRC y sus operadores homologados: Para la verificación de la vigencia y la categoría del certificado de aptitud física, mental y de coordinación motriz para conducir expedido por un Centro de Reconocimiento de Conductores.

EL SICOV para CEA y sus operadores homologados: Para la verificación de la vigencia y la categoría de la licencia en el certificado de aptitud en conducción expedido por un Centro de Enseñanza Automovilística debidamente registrado.

2.2.6.7. Validación continua de identidad de los participantes en el proceso de evaluación.

El SICOV de los CALE requiere implementar y ejecutar un proceso robusto y continuo de validación de la identidad de los usuarios del servicio y de los instructores y evaluadores durante las distintas etapas del proceso de evaluación.

1. **Mecanismos biométricos de validación:** El SICOV utilizará una combinación de los siguientes mecanismos biométricos para las validaciones de identidad en los CALE:

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

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

2. **Momentos y mecanismos específicos de validación de identidad:** El Sistema deberá exigir y registrar la validación de identidad tanto de usuarios, como de instructores y evaluadores en los siguientes tres momentos clave de cada evaluación: al inicio, durante (para verificación de permanencia) y al finalizar, con los siguientes mecanismos específicos:

   a) Validación de identidad en la evaluación teórica

El Sistema validará la identidad de los usuarios **antes** del inicio de la evaluación teórica, a través de la tecnología de reconocimiento facial (Selfie vs Template) o a través del cotejo de las huellas dactilares contra la base de datos de la RNEC. Sólo cuando resulte exitosa la validación de identidad, el usuario podrá ser ubicado en el cubículo que le asigne el CALE.

Durante la prueba teórica, el Sistema deberá validar la identidad del usuario a través de tecnología de reconocimiento facial (Selfie vs Template), con el cotejo de al menos cinco (5) fotografías capturadas en diferentes momentos aleatorios durante la prueba. El resultado de estos intentos de validación de identidad deberá ser informado al CALE a través de su plataforma tecnológica. La validación exitosa será requisito para la aprobación de la evaluación, además de lo exigido en cuanto al acierto en las respuestas.

Al finalizar la prueba (con la confirmación de envío de las respuestas en la plataforma del CALE), el Sistema requerirá un nuevo intento de validación de identidad que deberá efectuarse a través de la tecnología de reconocimiento facial (Selfie vs Template) o a través del cotejo de las huellas dactilares contra la base de datos de la RNEC.

b) Validación de identidad en la evaluación práctica

Como condicionante para el inicio de la prueba, el Sistema verificará que el aspirante haya aprobado previamente el examen teórico.

De comprobarse lo anterior, el Sistema validará la identidad de los usuarios **antes** del inicio de cada evaluación práctica, tanto de la prueba de destreza individual en pista, como la prueba en vía pública, a través del mecanismo de reconocimiento facial (Selfie vs Template) y/o a través del cotejo de las huellas dactilares contra la base de datos de la RNEC. Sólo cuando resulte exitosa la validación de identidad, se podrá dar inicio a cada prueba.

Durante el desarrollo de la **prueba de destreza individual** y de la **prueba en vía pública**, el Sistema deberá capturar al menos cinco (5) fotografías de manera aleatoria que se utilizarán para validar la identidad del usuario a través de la tecnología de reconocimiento facial (Selfie vs Template).

Al finalizar ambas pruebas, el Sistema requerirá un nuevo intento de validación de identidad que podrá efectuarse ser a través del mecanismo de reconocimiento facial o, en su defecto, a través del cotejo de las huellas dactilares contra la base de datos de la RNEC.

3. **Alerta por no detección de permanencia:** Cuando, durante una evaluación teórica o práctica, el sistema de verificación de permanencia no logre validar la identidad de un aspirante o instructor, el sistema de validación de identidad deberá enviar una alerta automática de manera inmediata al CALE y deberá quedar trazabilidad en los registros (logs) de tal situación, para consulta del SICOV.

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

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

El Sistema de Control y Vigilancia deberá incorporar funcionalidades para el almacenamiento seguro y el procesamiento analítico de los datos derivados del proceso de validación de identidad de los usuarios del servicio, instructores y evaluadores. 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 evaluación.

a) El SICOV deberá garantizar el registro y mantenimiento de trazabilidad completa y auditable de todos los intentos de validación de identidad (exitosos y fallidos) realizados por usuarios, instructores y evaluadores, la cual deberá ser capturada por el CALE. Este registro detallado deberá incluir, como mínimo: el mecanismo de validación empleado, el resultado de cada validación, el dispositivo empleado, la fecha y hora exactas, la identificación del usuario, instructor y evaluador involucrados en la respectiva sesión, la información del CALE evaluador, el aula o vehículo asociado y la tipificación del fallo en la validación de identidad. Estos datos deberán alojarse y procesarse en el CPD.

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 proveedor tecnológico y la Superintendencia de Transporte. Los hallazgos relevantes deberán generar alertas automáticas para revisión por parte de la Superintendencia y del CALE, según corresponda.

2.2.6.9. Registro de resultados evaluaciones teórico prácticas y metadatos de sesión.

El Sistema deberá gestionar y mantener un registro actualizado y detallado de los resultados de las evaluaciones teórico-prácticas realizadas a los usuarios, que incluya los pormenores de los resultados obtenidos en la prueba y el dato de si fue aprobada o no. El CALE deberá garantizar la captura y almacenamiento automático de dichos registros.

Para garantizar la integridad y el cumplimiento de la estructura definida por el Ministerio de Transporte, la plataforma tecnológica del CALE deberá transmitir a la infraestructura del SICOV, de manera automática, al término de cada día en el que preste servicios, un archivo de metadatos de la evaluación, firmado digitalmente, que contenga como mínimo la siguiente información:

a) Identificación de la sesión: ID único de la evaluación, fecha, hora de inicio y hora de finalización (marca de tiempo).
b) Estructura del examen: Verificación del cumplimiento del número total de preguntas aplicadas (40 preguntas) y su distribución por núcleos temáticos: doce (12) de tipo actitudinal y veintiocho (28) de conocimiento, estas últimas discriminadas por los cuatro (4) núcleos reglamentarios.
c) Trazabilidad de la evaluación: Tiempo de respuesta registrado por cada pregunta.
d) Resultados detallados: Calificación obtenida por el aspirante en cada núcleo temático y el resultado final consolidado.

Control de tiempos de ejecución y permanencia

El SICOV guardará trazabilidad de la duración de cada sesión evaluativa de la siguiente manera:

- El sistema registrará una estampa de tiempo de inicio tras la validación biométrica exitosa de inicio y de cierre.
- El sistema verificará, mediante el análisis de los datos de geolocalización, que la prueba en vía pública haya tenido una duración mínima de 20 minutos de conducción efectiva.

Validación de la calificación

El SICOV funcionará como un validador de la lógica de calificación establecida por el Ministerio de Transporte. Para cada examen práctico, el software del CALE deberá transmitir los códigos específicos de los errores cometidos (Clase I, II o III) conforme al catálogo oficial.

2.2.6.10. Control de reintentos y flujo de vigencias.

El Sistema integrará la lógica de reintentos establecida por el Ministerio de Transporte:

Validación de gratuidad: El sistema identificará automáticamente los casos de reprobación y habilitará un (1) reintento sin costo asociado al mismo PIN, siempre que se agende y realice dentro de los diez (10) días calendario posteriores.

Bloqueo de caducidad: El SICOV restringirá el inicio de cualquier prueba práctica si detecta que han transcurrido más de treinta (30) días calendario desde la aprobación del examen teórico sin que se haya completado el proceso.

Prelación de agenda: El subsistema de gestión del SICOV deberá corroborar el funcionamiento del algoritmo de asignación de turnos del CALE, que priorice a los aspirantes en proceso de reintento de evaluación sobre las solicitudes iniciales.

2.2.6.11. Gestión y control de vehículos de evaluación.

El Sistema deberá gestionar y mantener un registro actualizado y detallado de cada vehículo vinculado a los CALE para la impartición de las evaluaciones prácticas.

Esta funcionalidad se basará primordialmente en la información disponible y actualizada en el Registro Único Nacional de Tránsito (RUNT) e incluirá, como mínimo, los siguientes datos por vehículo:

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

b) Documentación legal y de operación:

- Información de la licencia de tránsito.
- Fecha de expedición y vigencia de la póliza del Seguro Obligatorio de Accidentes de Tránsito (SOAT).
- Fecha de expedición y vigencia del Certificado de Revisión Técnico-Mecánica y de Emisiones Contaminantes (RTMyEC) y de adaptaciones, así como la identificación del Centro de Diagnóstico Automotor (CDA) que lo expidió, en los casos que aplique.
- Para vehículos adaptados para la enseñanza o evaluación a personas con discapacidad, información del certificado de adaptación correspondiente.

1. **Registro de novedades por parte del CALE:** El CALE deberá, para tal efecto, registrar en su plataforma de forma oportuna las siguientes novedades asociadas a sus vehículos vinculados:

    - 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 CALE y la fecha de su desvinculación definitiva.

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

   a) El Sistema deberá generar alertas automáticas dirigidas al CALE con antelación de treinta (30) días hábiles sobre el próximo vencimiento de la póliza SOAT y/o del certificado de RTMyEC de los vehículos registrados.

2.2.6.12. Monitoreo de actividad en vehículos de evaluación.

El Sistema de Control y Vigilancia deberá registrar y validar la ubicación geográfica y el recorrido de los vehículos de evaluación vinculados al CALE durante la impartición de cada evaluación práctica en vía pública. Esta función tiene como objetivo verificar la realización efectiva de la evaluación práctica.

1. **Dispositivo de geolocalización vehicular y transmisión de datos:**

a) Para cumplir con esta función, cada vehículo de enseñanza debe 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 CALE.

b) El dispositivo deberá ser instalado y 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.

c) La ubicación del dispositivo en el vehículo deberá permitir su eventual inspección por parte de la Superintendencia de Transporte.

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

a) El Sistema de Control y Vigilancia consultará y hará la ingesta de dicha información desde el CPD del CALE o la infraestructura dispuesta para ello, al final de cada día de prestación del servicio, y con ello registrará el historial completo de ubicación y recorrido de cada vehículo durante las pruebas en pista y en vía pública.

b) El Sistema debe permitir a la Superintendencia de Transporte la visualización de la ubicación de los vehículos que se utilicen para realizar las evaluaciones prácticas. Para ello, el Sistema tomará la información de la plataforma del CALE.

c) La información de geolocalización y recorridos servirá como insumo para la generación de reportes, la atención de quejas o reclamos, y acciones de IVC que adelante la Superintendencia de Transporte.

2.2.6.13. Verificación continua de la permanencia de los participantes.

El Sistema deberá implementar mecanismos tecnológicos para verificar la permanencia continua de los usuarios del servicio y los evaluadores durante el desarrollo completo de cada evaluación, tanto en modalidad presencial, como virtual, en este último caso mientras las condiciones técnicas y regulatorias así lo permitan. Esta función es crucial para asegurar la participación efectiva en el proceso de evaluación y prevenir el fraude.

1. **Mecanismo general de verificación:** El Sistema validará en tiempo real la identidad de los usuarios presentes durante la realización de las pruebas en las aulas y vehículos, realizando, como mínimo, cinco (5) procedimientos de comprobación de permanencia por cada evaluación realizada. El mecanismo principal para esta verificación será la tecnología de reconocimiento facial, que procesará las capturas de fotografías

tomadas en momentos aleatorios durante el transcurso de cada evaluación.

2. **Alerta por no detección:** Si como resultado del procedimiento automático de verificación de permanencia, el Sistema no logra identificar o detectar a un usuario que se registró al inicio, se activará de inmediato una alerta que informará en tiempo real al CALE sobre la no detección del(os) usuario(s). El Sistema guardará trazabilidad precisa de los servicios en que esto ocurra. Esta información estará disponible para consulta de la Superintendencia de Transporte, a través del MSC, y será objeto de análisis con herramientas de analítica de datos por parte del proveedor tecnológico del SICOV.
3. **Infraestructura descentralizada y software requerido:** La implementación de esta funcionalidad requerirá la instalación de hardware en la sede de los CALE (como cámaras en aulas, dispositivos móviles en vehículos e infraestructura de procesamiento descentralizada), así como el uso de servicios tecnológicos de reconocimiento facial. Más adelante se describen los estándares mínimos exigidos para esta infraestructura y software.

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

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

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 se realicen únicamente desde las sedes, vehículos y ubicaciones físicas autorizadas por el Ministerio de Transporte y debidamente registradas en el RUNT. 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.

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

El Sistema de Control y Vigilancia deberá llevar un registro actualizado con la información de la capacidad instalada y operativa real de cada CALE. Esta capacidad determinará el volumen máximo de servicios (capacidad de las aulas, total de vehículos, horario de atención y cupos) que el CALE puede programar y prestar simultáneamente.

2.2.6.16. Clasificación automática de cada evaluación según el estado de validación de identidad.

El Sistema deberá clasificar de manera automática cada evaluación registrada para un usuario según el resultado de los intentos de validación en los distintos momentos del proceso, como: "Prueba con validación de identidad realizada satisfactoriamente" o "Prueba con validación de identidad no realizada satisfactoriamente", o “Evaluación suspendida”.

Esta clasificación se basará estrictamente en el cumplimiento de los requisitos de validación de identidad y de verificación de permanencia, del usuario en el caso de la prueba de destreza individual en vía pública, y del usuario y el instructor o evaluador cuando aplique, conforme a los procedimientos detallados en los numerales correspondientes de este Anexo Técnico.

1. **Criterios para clasificación como "Prueba con validación de identidad realizada satisfactoriamente":** Una evaluación se clasificará automáticamente con la etiqueta de "Prueba con validación de identidad

realizada satisfactoriamente" si, y solo si, el Sistema registra que se cumplieron de manera acumulativa y satisfactoria todos los puntos de control de identidad y permanencia establecidos para dicha evaluación (ej. al inicio, durante y al finalizar). El Sistema registrará esta clasificación de forma inmediata y automatizada una vez se confirmen todas las validaciones requeridas.

2. **Criterios para clasificación como "Prueba con validación de identidad no realizada satisfactoriamente":** Cualquier evaluación en la que se presenten inconvenientes que impidan la validación de identidad satisfactoria de los intervinientes, por cualquier motivo, será clasificada automáticamente como "Prueba con validación de identidad no realizada satisfactoriamente". El Sistema deberá registrar el motivo específico de esta clasificación (ej. inconsistencia en la validación inicial del usuario, inconvenientes en la detección de permanencia, etc.).
3. **Criterios para clasificación como "Evaluación suspendida".** Si se suspende la prueba de destreza individual o la prueba de maniobras en vía pública por motivos atribuibles al Centro de Apoyo Logístico de Evaluación, o por un caso fortuito o de fuerza mayor, el Sistema debe dejar traza del servicio con dicha etiqueta en el registro histórico.

Para que un CALE pueda reportar la aprobación de los exámenes teórico y práctico en el RUNT, a fin de que se registre allí su certificación, ambos procesos de evaluación deben estar clasificados con la etiqueta de "Prueba con validación de identidad realizada satisfactoriamente".

2.2.6.17. Gestión del registro histórico de certificados expedidos.

El Sistema deberá llevar un registro histórico, detallado, cronológico, seguro e inalterable de todas las evaluaciones teórico prácticas aprobadas en cada CALE y de los certificados por estos expedidos y cargados en el RUNT. Este registro histórico deberá incluir, como mínimo, la siguiente información por cada certificado:

a) Número único de identificación del certificado generado.
b) Identificación del CALE que expidió el certificado.
c) Identificación del usuario a quien se le expidió el certificado (tipo y número de documento de identidad, nombres y apellidos).
d) Fecha de la expedición del certificado en el SICOV.
e) Resultado obtenido en las evaluaciones teórico-prácticas.
f) Nombre del Centro de Enseñanza Automovilística que emitió previamente el certificado de aptitud tras la capacitación en conducción y del Centro de Reconocimiento de Conductores que emitió el certificado de aptitud física, mental y de coordinación motriz.

Este registro histórico se deberá guardar por un periodo de cinco (5) años.

2.2.6.18. Registro y actualización de tarifas de servicios.

El Sistema llevará un registro actualizado con la información detallada de las tarifas que ofrece al público por los servicios de evaluación teórica y práctica. Cualquier modificación de las tarifas deberá verse reflejada en el Sistema automáticamente de manera inmediata.

2.2.6.19. Gestión y control de suspensiones, medidas cautelares y usuarios activos.

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 de la infraestructura del SICOV cada vez que adopte una medida de suspensión en

contra de un CALE, así como la información precisa sobre el momento (fecha y hora) exacto en que la medida de suspensión se haga efectiva en el Registro Único Nacional de Tránsito, así como el momento de su levantamiento.

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

Contabilización precisa: El SICOV llevará un registro exacto del tiempo transcurrido de ejecución de cada 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 y para garantizar los derechos de los usuarios del CALE que al momento de ejecución de la medida ya hubieran pagado por el servicio y generado un PIN.

Esta capacidad se activará para dar estricto cumplimiento a:

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

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

Usuarios activos: Como medida especial de protección del usuario y de la continuidad del servicio, cada vez que se haga efectiva una medida de suspensión de un CALE, el sistema guardará un registro con la información de todos los usuarios activos del servicio a los que no se les hubiera terminado de prestar el servicio (quienes hayan pagado se les haya generado un PIN antes de la adopción de la medida y a quienes no se les hayan realizado los exámenes teórico y práctico), usuarios a los que el CALE tendrá la obligación de garantizar la culminación del servicio.

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

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

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

2.2.6.20. Registro y monitoreo continuo de cumplimiento.

El Sistema llevará un registro que permita monitorear continuamente el cumplimiento de obligaciones exigibles a los CALE. El sistema **contará con la** capacidad de generación de alertas ante las siguientes situaciones:

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 CALE no ha subsanado el vencimiento o la ausencia de documentos críticos para su operación, como son aquellos que dieron lugar a la autorización de su registro en el RUNT. Esta alerta llevará a la marcación de irregularidad de todos los servicios que se presten bajo esa condición.
- **Uso de vehículos sobrepasando la antigüedad permitida, sin SOAT y/o RTMyEC:** Se generará una alerta de restricción automática si detecta, bien por cuenta de la información registrada por el CALE y disponible en el Sistema; o como resultado de la consulta que se realice en el RUNT, que un vehículo utilizado para la evaluación práctica excede la antigüedad máxima permitida por categoría de licencia de conducción, o si no cuenta con SOAT o con el certificado de revisión técnico-mecánica y de emisiones contaminantes (RTMyEC) y de adaptaciones vigentes.

Alertas por posible manipulación de dispositivos y suplantación de identidad:

- **Manipulación de dispositivos:** Se activará una alerta si se detecta la manipulación, alteración, desinstalación o daño de los equipos del Sistema de Control y Vigilancia instalados en las sedes o vehículos de los CALE.
- **Intentos fallidos consecutivos de validación de identidad:** Se registrará una alerta 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 evaluación teórica y práctica (inicio, durante, cierre). Para el caso del personal, la alerta se activará si estos fallos se presentan consecutivamente en tres o más pruebas seguidas.

Alertas de operación e infraestructura:

- **Interrupciones en la transmisión de datos:** Cualquier interrupción, retención indebida o disposición no autorizada de la información esencial del Sistema generará una alerta.
- **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 altas y bajas:** El SICOV podrá generar alertas si se detectan patrones de calificaciones consistentemente altas o bajas en las evaluaciones realizadas a los usuarios del servicio.

a) Trazabilidad de las actuaciones:

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

Con estas evidencias, disponibles en el Módulo de Supervisión y Control, la Superintendencia de Transporte podrá visualizar y descargar información de la operación de los CALE en todo el país.

b) 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.

2.2.6.21. Módulo de Supervisión y Control (MSC) para el acceso de la Superintendencia de Transporte.

El Sistema deberá garantizar un módulo de acceso restringido para la Superintendencia de Transporte. Este módulo permitirá a la entidad consultar, visualizar, leer análisis e indicadores del proveedor, analizar y solicitar información consolidada y detallada, en tiempo real, tanto de la operación general del SICOV CALE, como de la prestación de servicios por parte de los Centros de Apoyo Logístico de Evaluación.

En este módulo, la Superintendencia podrá filtrar y visualizar las alertas por irregularidades y anomalías de cada CALE, discriminando si su origen fue específico o estructural.

1. Por causal específica: Cuando la anomalía se detecta únicamente en el desarrollo de ese servicio particular (ej. presunto intento de suplantación de identidad en una evaluación).

2. Por causal estructural: Cuando la anomalía proviene de un incumplimiento de los requisitos de operación del Organismo de Apoyo (ej. documentos que soportan requisitos críticos). En este escenario, el SICOV aplicará la marcación de manera masiva y automática a todos los servicios que se gestionen bajo la vigencia de dicha irregularidad.

Este módulo deberá proveer, como mínimo, las siguientes funcionalidades e información:

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 (especialmente del servicio de recaudo y de autenticación biométrica a través de operador autorizado por la RNEC); acceso a reportes detallados sobre incidentes técnicos que se presenten y/o hayan presentado en la operación, y la duración de estas interrupciones o fallas y el número de servicios y usuarios afectados; así como un tablero de seguimiento del cumplimiento de los Acuerdos de Nivel de Servicio (ANS) definidos para la operación del Sistema.

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

   - Los datos extraídos deben permitir la construcción y visualización de la totalidad de los indicadores exigidos por la Entidad (disponibilidad por componente, latencia de respuesta, estado Up/Down, entre otros).
   - No se aceptará el cargue manual de reportes de disponibilidad. El flujo de datos entre las herramientas de observabilidad del operador y el Módulo de Supervisión y Control de la Superintendencia debe ser automático y mediante servicios web.
   - La Superintendencia se reserva el derecho de auditar las fuentes primarias de estas herramientas de monitoreo para asegurar que los datos reportados coincidan con la realidad operativa del sistema. Si los servicios de infraestructura están subcontratados, se debe advertir esta situación al tercero que preste el servicio al proveedor.
   - Independientemente de la herramienta de origen, la información deberá visualizarse de manera consolidada en el tablero de control de la Superintendencia para verificar en tiempo real el estado del Sistema y sus componentes.

2. **Gestión de peticiones, quejas, reclamos y sugerencias (PQRSD) relacionadas con el CALE y el SICOV:** Visualización de estadísticas actualizadas sobre las PQRSD recibidas y gestionadas por el CALE, con

corte al día anterior del mes en el que se realiza la consulta. Esta información también se podrá consultar por mes y año, y los datos históricos generales. El sistema, además, permitirá consultar tiempos promedio de respuesta por cada PQRSD. Para tal efecto, el proveedor tecnológico del SICOV deberá consultar y descargar automáticamente, al cierre de cada jornada de atención, la información respectiva de cada CALE.

Por otra parte, se debe permitir la visualización de estas mismas estadísticas actualizadas sobre las PQRSD recibidas y gestionadas por el proveedor tecnológico de la infraestructura del SICOV para CALE.

3. **Consulta de datos operativos históricos de los CALE:** Capacidad para que la Superintendencia de Transporte consulte información específica y agregada de los CALE, utilizando diversos criterios de búsqueda. Para la consulta de la información específica de cada sede de CALE en el país, el módulo debe ofrecer la opción de consulta por perfil individualizado, en donde podrá encontrar toda la información asociada a su operación incluidas las capacidades de análisis estadístico y tendencias.

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.

5. **Alertas:** Información de los alertas generadas en el Sistema, con toda la información asociada al respecto (CALE, fecha, hora, motivo de generación de la alerta, entre otros).

6. **Trazabilidad y auditoría de la interoperabilidad:** Acceso a los registros (logs) detallados de la interoperabilidad.

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.

2.2.7. Estándares generales de interoperabilidad

La infraestructura tecnológica del Sistema de Control y Vigilancia para CALE debe garantizar la interoperabilidad obligatoria con los CALE y con los Sistemas de Control y Vigilancia de los Centros de Enseñanza Automovilística (SICOV-CEA) y de los Centros de Reconocimiento de Conductores (SICOV-CRC).

Con el fin de asegurar que dicha integración sea técnica y operativamente viable, y responda a la realidad de los sistemas existentes, los protocolos de comunicación y demás condiciones mínimas aplicables a la interoperabilidad con los SICOV-CEA y el SICOV-CRC serán definidos posteriormente por la Superintendencia.

Sin perjuicio de lo anterior, los proveedores deberán certificar que su arquitectura base cumple con lo siguiente:

- Seguridad en el tránsito: Uso de estándares abiertos y protocolos de comunicación cifrados mediante TLS 1.2 o superior. Adicionalmente, toda la información sensible (biometría, registros audiovisuales y trazas de geolocalización) deberá almacenarse con cifrado en reposo mediante algoritmos de grado industrial (mínimo AES-256 o superior).
- Trazabilidad y no repudio: Capacidad de generar logs de auditoría inalterables por cada transacción o intento de conexión, registrando marca de tiempo, origen, destino y resultado de la operación. Para los casos de recepción de paquetes de datos de operación (incluyendo

coordenadas GPS y eventos de biometría) deberá contar con un mecanismo de verificación de integridad mediante funciones Hash (SHA-256 o superior) o firma electrónica, que impida la alteración de la evidencia tras su generación.
- Disponibilidad: Las interfaces de comunicación deben estar diseñadas para operar de manera continua, alineadas con los niveles de servicio establecidos.
- Autenticación robusta: Implementación de mecanismos seguros para el consumo de servicios conforme a las políticas de seguridad del sistema.

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

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

2.2.8.1. 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:

2.2.8.1.1. Monitoreo y gestión centralizada de la infraestructura.

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

Para ello, deberá:

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

2.2.8.1.2. 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.

2.2.8.1.2.1. **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.

2.2.8.1.2.2. **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.

2.2.8.1.2.3. 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.

2.2.8.1.3. Seguridad de endpoints y correo electrónico

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

Esto incluye:

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

2.2.8.1.4. 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-activo).

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).

2.2.8.1.5. Herramientas de seguridad lógica y operación

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

- **SIEM (Security Information and Event Management):** Para la correlación y análisis de eventos de seguridad.
- **Monitor de Infraestructura y Servicios (NOC):** Para la supervisión del estado y disponibilidad de activos de red y sistemas.
- **Sistema de Gestión de Incidentes (ITSM):** Para el registro, seguimiento y resolución de eventos, con *ticketing* automatizado y escalamiento por criticidad.
- **Plataforma de Automatización de Seguridad (SOAR):** Para la respuesta automatizada ante incidentes, con *playbooks* de respuesta y automatización de acciones.
- **Analizador de Vulnerabilidades:** Para la identificación proactiva de debilidades técnicas.

- **Detección y Respuesta en Endpoints (EDR):** Para la supervisión y protección de dispositivos finales, con análisis de comportamiento y aislamiento remoto.
- **Gestión de Identidades (IAM):** Para el control de acceso a recursos críticos, con autenticación multifactor y gestión de privilegios.
- **Monitor de Bases de Datos y Aplicaciones:** Para la protección de operaciones y datos en sistemas críticos.
- **CMDB (Configuration Management Database):** Para el inventario y la relación de activos tecnológicos.
- **Plataforma de Inteligencia de Amenazas:** Para la contextualización de riesgos externos conocidos.

2.2.8.1.6. Desarrollo de aplicaciones y entornos de prueba

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

2.2.9. Infraestructura tecnológica en los CALE para el funcionamiento del SICOV

Los Centros de Apoyo Logístico de Evaluación deberán garantizar la correcta operación del Sistema en sus instalaciones, por lo que deberán permitir el suministro, instalación, configuración, mantenimiento y soporte de todos los equipos, dispositivos y periféricos mínimos necesarios por parte del proveedor tecnológico, así como el adecuado funcionamiento del software necesario para dar cumplimiento a todo lo previsto en este Anexo.

Los requisitos que se establecen a continuación son de carácter mínimo. El proveedor tecnológico que se seleccione deberá garantizar que el hardware y software suministrados y operados estén en capacidad de soportar todas las funcionalidades establecidas por la Superintendencia de Transporte.

Ante la aparición de nuevas y mejores tecnologías, la infraestructura deberá ser actualizada para evitar la obsolescencia tecnológica y garantizar la mejora continua del sistema, conforme a los lineamientos de la Superintendencia.

Los proveedores tecnológicos tendrán libertad para adquirir los equipos de hardware y soluciones tecnológicas especializadas de cualquier marca o proveedor, siempre que estas cumplan con las condiciones y funcionalidades mínimas exigidas por la Superintendencia en este acápite.

Será responsabilidad del proveedor tecnológico garantizar la correcta integración de su software con los equipos adquiridos y/o empleados por el CALE para prestar el servicio y brindar soporte técnico sobre dicha integración.

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

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

2.2.9.1. Hardware para el funcionamiento del Sistema

Se deberán suministrar y soportar dispositivos y periféricos, con las características y funcionalidades mínimas que a continuación se detallan:

2.2.9.1.1. Lectores biométricos especializados de huellas

Los lectores de huellas especializados que se utilizarán para validar biométricamente la identidad de usuarios y personal del CALE deberán reunir, como mínimo, las características y condiciones que se mencionan a continuación:

Lector de huella multiespectral

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

Lector de huella óptico infrarrojo

FUNCIONES Y CARÁCTERÍSTICAS	
Tecnología	Optical technology que cuentes con Diodos emisores de luz (LED) infrarroja
Template Extractor y Matcher	MINEX III Certificado
Resolución de imagen de salida / Profundidad de bits	500 dpi / 8-bit, 256 escala de grises
Formato de salida de imagen	Imágenes sin comprimir o comprimidas WSQ (certificadas por el FBI)

Formato de salida de plantilla	ANSI 378 / ISO 19794-2 / ISO-19784 (MINEX III certificado)
Match sobre dispositivo	Entradas de plantilla ANSI 378 / ISO 19794-2
Adquisición de imágenes	Adquisición de imágenes estructuradas (SIA) para mayor velocidad, rechazo de la luz ambiental y calificación de la posición de los dedos
USB	USB 2.0 alta velocidad (480 Mbps)
Sistemas Operativos	Windows 10/11; Linux x86/x64
SEGURIDAD	
Detección de Ataques de Presentación (PAD) / Detección de Dedos en Vivo (LFD)	-ISO/IEC 30107-3, Level 2 Presentation Attack Detection (PAD) Certificado / Live Finger Detection (LFD)
Protección física contra manipulaciones	Actualizaciones de firmware cifradas Elemento seguro con borrado de clave activa
Criptografía	AES 128/256, TDES 2/3 Key, SHA-256, RSA-2048
Número de claves simétricas de usuario	10
ID estática única	64 bits
Generador de bits aleatorios determinista (DRBG)	NIST CAVP Certificado
SOPORTE DEL MODELO DE TRANSACCIÓN	
Inyección de llave de fábrica	Soportado
Sesión maestro/esclavo	Soportado
Remote Key Load (RKL)	Soportado

Adicionalmente, los lectores biométricos de huellas dactilares que se utilicen deberán estar homologados por la RNEC conforme a la Resolución vigente aplicable por esa entidad y la última versión del anexo técnico.

Ubicación: Estos dispositivos deberán estar instalados **(i)** en la(s) recepción(es) de los CALE 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 realicen las evaluaciones teóricas, conforme a lo previsto en este Anexo y **(iii)** en los dispositivos instalados en los vehículos en que se realicen las evaluaciones de la fase de evaluación práctica.

2.2.9.1.2. Cámara o dispositivo fijo de captura de fotografía:

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

Especificaciones técnicas mínimas:

- Resolución Mínima: Full HD (1080p)
- FPS: Mínimo 25fps en 1080
- Enfoque Automático
- Corrección de Iluminación automática
- Compresión de Video .H264
- Deberá soportar el estándar de reconocimiento facial ISO/IEC 19794-5 a través de software.

Ubicación: Estos dispositivos deberán estar instalados en cada cubículo empleado para la realización de las evaluaciones teóricas y servirán para la captura de las fotografías de los usuarios en momentos aleatorios durante el

desarrollo de la evaluación teórica a fin de validar la identidad del usuario con la tecnología de reconocimiento facial.

2.2.9.1.3. Dispositivos móviles para la validación de identidad en vehículos:

El proveedor tecnológico deberá disponer de e instalar dispositivos móviles (tipo tablet o móvil) que permitan la validación de identidad a través de los dos mecanismos previstos en este Anexo, lo que implica que estos tengan capacidad de captura de fotografías y la realización de procesos de validación de identidad con tecnología de reconocimiento facial, así como también la captura de las minucias de las huellas dactilares con los lectores de huella especializados. Estos dispositivos deberán ser instalados o ubicados de la siguiente manera:

Ubicación:

- **En los vehículos de evaluación dispuestos para las pruebas en pista y en vía pública:** Para la validación de identidad durante las actividades en movimiento.

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 reconocimiento facial.** Conforme a lo descrito en el acápite de software que se encuentra más adelante.

- **Tecnología de GPS:** Integrada para georreferenciación de los dispositivos móviles para la validación de identidad.

- **Lector de huella dactilar:** Estos dispositivos móviles deberán contar con los lectores biométricos especializados integrados de forma segura y deberán cumplir con los requerimientos mínimos descritos en los numerales correspondientes del presente Anexo, para realizar las validaciones aleatorias contra la RNEC en las pruebas de Pista cuando así se requiera.

  Los dispositivos móviles para la identificación en vehículos deberán garantizar:

  - 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.
  - Capacidad para realizar reconocimiento facial, compatible con la tecnología de reconocimiento facial descrita en este Anexo Técnico.

2.2.9.1.4. Pad de firmas digitalizador

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

El pad de firmas servirá para obtener la autorización previa, expresa e informada del personal del CALE y de los usuarios del servicio, para el tratamiento de sus datos personales y biométricos a través del Sistema, 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.

Ubicación: Estos dispositivos deberán estar ubicados en la(s) recepción(es) del CALE.

2.2.9.1.5. Infraestructura descentralizada para el reconocimiento facial

El proveedor del Sistema deberá instalar infraestructura descentralizada en la sede de los CALE a fin de permitir el funcionamiento eficiente de los equipos, componentes y la tecnología de reconocimiento facial (SDK de captura, liveness y margen). La infraestructura debe contar con lo mínimo exigido por el fabricante, incluida la GPU o CPU que se requiera para su adecuado funcionamiento.

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 de operación del CALE, atendiendo la política de conservación de información indicada por la Superintendencia de Transporte.

Para estos efectos, deberá disponerse 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.

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:

2.2.9.1.5.1. Workstation

Requisitos mínimos:

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

2.2.9.1.5.2. NAS

Requisitos mínimos:

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

2.2.9.1.5.3. Switches de red administrables

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

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

Capacidades de enrutamiento

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

2.2.9.1.5.4. SAI o UPS

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

A 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 CALE.

2.2.9.1.5.5. Rack de equipos

Con las siguientes características mínimas:

- Rack de piso, tipo metálico con pintura electrostática, con llave y con rodachinas.
- Altura 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.

2.2.9.2. Software y componentes de software especializados requeridos para el funcionamiento del software SICOV para los CALE

El proveedor tecnológico deberá disponer del software y/o componentes de software necesarios que garanticen que el Sistema cumpla con cada una de las funcionalidades tecnológicas descritas en este Anexo.

Por lo tanto, será responsable de configurar, mantener y soportar el software y componentes de software que a continuación se describen, así como de asegurar su compatibilidad y adecuado funcionamiento:

2.2.9.2.1. Software de reconocimiento facial para validación de identidad.

El Sistema deberá contar con 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.

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

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

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:

Para la validación de identidad de los usuarios antes y después de las evaluaciones teóricas y prácticas, 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) que demuestre conformidad con el estándar ISO/IEC 30107-3 Niveles 1 y 2 en materia de detección de ataques de presentación, certificada por el NIST a través del programa FATE PAD o por un laboratorio acreditado bajo el programa NIST/NVLAP —entre ellos iBeta Quality Assurance (código NVLAP 200962-0) o BixeLab—, con fecha de presentación de la prueba de certificación no mayor a dos (2) 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 ΔT ≥ 12 YRS debe ser menor o igual a 0.0040 puntos de precisión.
    - Galería VISA Prueba Border. El resultado debe ser menor o igual a 0.0040 puntos precisión.

    La fecha de presentación de las pruebas no puede ser superior a los 2 años y deberán realizarse nuevamente cada 2 años.

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

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

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.

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

El proveedor del Sistema deberá contar con un software de gestión de tickets para la operación de la Mesa de Ayuda.

2.2.9.2.4. Software de Mobile Device Management (MDM).

El operador del Sistema deberá contar con una herramienta que permita administrar, supervisar y proteger los dispositivos móviles y/o equipos de cómputo que sean dispuestos y lleguen a ser entregados a los CALE por parte del proveedor tecnológico.

2.2.10. Gestión de la infraestructura y la obsolescencia tecnológica

Para evitar la obsolescencia tecnológica se deberá:

- Mantener actualizado el inventario del equipamiento tecnológico desplegado en los CALE conforme a las disposiciones técnicas de la Superintendencia de Transporte.
- Actualizar el hardware y software de manera proactiva, incorporando las mejores tecnologías disponibles en el mercado que permitan cumplir los objetivos de seguridad, eficiencia y transparencia. 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, dispositivos y periféricos provistos por el proveedor tecnológico se

deberá realizar cada cuatro (4) años, contabilizados a partir de la fecha de instalación de la infraestructura en los CALE.

TÍTULO 3

3. AUDITORÍA A LA INFRAESTRUCTURA TECNOLÓGICA DEL SICOV PROVISTA POR LOS PROVEEDORES TECNOLÓGICOS

3.1. Objetivo de las auditorías y verificaciones de cumplimiento

Las auditorías de tercera parte y actividades de verificación tienen por objetivo primordial verificar el cumplimiento permanente de los requisitos técnicos, administrativos y de seguridad establecidos en el presente Anexo Técnico y demás disposiciones complementarias.

Buscan asegurar la confiabilidad, integridad, disponibilidad y seguridad de la información capturada de la operación de los CALE, 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. Aspectos generales de auditoría y verificación

La auditoría de tercera parte en el marco del SICOV para CALE debe atender los siguientes criterios:

a. El auditor y empresa auditora deberá auditar todos los requisitos de operación del SICOV para CALE.
b. El auditor y empresa auditora no debe tener conflicto de interés respecto del proveedor tecnológico y la infraestructura objeto de verificación.
c. La Superintendencia de Transporte y el proveedor tecnológico deberán ser informados formalmente sobre los resultados de la auditoría.
d. Deberán identificarse y documentarse oportunidades de mejora relacionadas con la robustez de los componentes de hardware y software empleados en la operación del SICOV.
e. La auditoría deberá ser realizada por una empresa legalmente constituida cuyo objeto social contemple servicios de auditoría en sistemas, seguridad de la información e infraestructura tecnológica.
f. La auditoría de tercera parte deberá demostrar en su informe final que se verificaron todos los requisitos técnicos y operativos aplicables al SICOV, dejando constancia de los resultados en cuanto a su conformidad.

Cualquier acción correctiva derivada de las auditorías de tercera parte deberá implementarse por parte del proveedor tecnológico en un lapso máximo de quince (15) días calendario con el fin de asegurar la integridad y seguridad de la infraestructura tecnológica del SICOV, salvo en aquellos casos que la naturaleza de la acción correctiva implique plazos distintos debidamente justificados, los que en todo caso deben ser puestos en conocimiento y aprobados por parte de la Superintendencia de Transporte.

3.3. Obligaciones del proveedor tecnológico frente a las auditorías y labores de verificación

El proveedor tecnológico tendrá las siguientes obligaciones relacionadas con las auditorías:

1. Brindar todas las facilidades y acceso a la información, sistemas, instalaciones y personal requerido por el auditor para el desarrollo de su labor.

2. Responder de manera oportuna a todos los requerimientos de información, documentación y aclaraciones que sean requeridos.
3. Suministrar a la Superintendencia de Transporte los informes de auditoría en los plazos y formatos que esta determine.

TÍTULO 4

4. ACUERDOS DE NIVELES DE SERVICIO Y OBLIGACIONES DE LAS PARTES

4.1. Acuerdos de Niveles de Servicio

Los proveedor tecnológico del Sistema deberá cumplir con los Acuerdos de Niveles de Servicio de los componentes 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 Supervisión y Control (MSC).

4.1.1. CPD/CPAD

El CPD y CAPD deben garantizar una disponibilidad de, como mínimo 99,9 %.

4.1.2. Mesa de Ayuda

El proveedor tecnológico deberá cumplir con los tiempos máximos de respuesta a los incidentes, solicitudes, quejas y reclamos que presenten los CALE; 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
Superintendencia de Transporte y otras autoridades administrativas/judiciales	5 días	No. días en los cuáles se da respuesta desde el momento de la radicación/5	98 %

4.1.3. Operador de recaudo

El operador de recaudo deberá cumplir con los siguientes Acuerdos de Niveles de servicio.

PETICIONARIO	TIEMPO EN HORAS/DÍAS HÁBILES	INDICADOR DEL SERVICIO	PORCENTAJE DE CUMPLIMIENTO MÍNIMO
Clientes del servicio de recaudo y CALE	24 horas	No. horas en los cuáles se da respuesta desde el momento de	95 %

		la radicación/24	
Superintendencia de Transporte y operador SICOV	5 días	No. días en los cuáles se da respuesta desde el momento de la radicación/5	95 %
Autoridades administrativas y judiciales	7 días	No. días en los cuáles se da respuesta desde el momento de la radicación/5	95 %

4.1.4. Módulo de Supervisión y Control.

El Módulo de Supervisión y Control y todas sus funcionalidades deberá garantizarse con una disponibilidad mínima del software del noventa y nueve punto cuatro por ciento (99,4%), medida mensualmente.

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

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

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

d) El proveedor tecnológico 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 Supervisión y Control al que accederá la Superintendencia de Transporte.

Ventanas de mantenimiento programado: Las ventanas de mantenimiento programado de la plataforma tecnológica del CALE y/o de los componentes del SICOV deben ser informadas a la Superintendencia de Transporte y al público en general con una anticipación mínima de cinco (5) días hábiles, explicando las razones de su realización. En el caso de los usuarios de los CALE, estas deberán informarse a través de avisos visibles en los sitios web oficiales de los CALE.

A la Superintendencia de Transporte deberá transmitirse la información a través del Módulo de Supervisión y Control.

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 CALE y el proveedor de la tecnología del SICOV deberán colocar en conocimiento de la Superintendencia y de los usuarios tales circunstancias de manera inmediata, a través de los canales indicados.

4.2. Política general de tratamiento, conservación y supresión de la información del Sistema.

Los datos personales y la información de la operación de los CALE son recopilados con el fin de garantizar la trazabilidad y validez de los certificados expedidos por los CALE. Así mismo, dicha información permite a la Superintendencia el cumplimiento de sus funciones de supervisión sobre el servicio público a cargo de esos organismos de apoyo al tránsito..

Los proveedores de la infraestructura tecnológica del SICOV para CALE actúan en calidad de Encargados del Tratamiento y custodios temporales de dicha información. En consecuencia, dado que la información operativa soporta una actividad vinculada a un servicio público de tránsito, los proveedores no podrán invocar derechos de propiedad o exclusividad.

El presente numeral establece la política para el archivo, la conservación y la supresión segura de la información y los documentos gestionados por el Sistema de Control y Vigilancia. Esta política se fundamenta en los principios de finalidad, necesidad y temporalidad establecidos en la Ley Estatutaria 1581 de 2012, en las directrices de la Ley General de Archivos (Ley 594 de 2000), y en la consideración de los términos de prescripción de las acciones administrativas, sancionatorias, civiles y penales aplicables.

El proveedor tecnológico del SICOV para CALE será el responsable de implementar y garantizar el cumplimiento de esta política a través de los mecanismos técnicos y procedimientos necesarios, previa aprobación por parte del usuario de los Términos y Condiciones del servicio, así como de la Política de Tratamiento de Datos Personales.

4.2.1. Identificación plena, trazabilidad e integridad para fines de supervisión.

Dada la naturaleza de la información que el Sistema de Control y Vigilancia captura, con base en la cual se pueden desplegar acciones de inspección, vigilancia y control por parte de la Superintendencia de Transporte, el tratamiento de la información se regirá por las siguientes reglas de aseguramiento probatorio:

1. El SICOV garantizará la identificación inequívoca y permanente de todos los intervinientes en el proceso evaluativo (aspirantes, instructores, evaluadores y personal administrativo). Esta información estará disponible de manera clara y precisa para la Entidad, permitiendo la individualización de responsabilidades en el marco de investigaciones administrativas.

2. Toda la información recolectada, incluyendo registros biométricos, resultados de pruebas y metadatos de sesión, constituye prueba documental. El sistema debe asegurar su integridad y disponibilidad para la Superintendencia.

3. El acceso a la información personal identificable estará garantizado para el personal de la Superintendencia de Transporte que desempeñe labores de supervisión, análisis de cumplimiento y procesos administrativos sancionatorios, bajo estrictos protocolos de seguridad y logs de auditoría que registren quién y para qué consultó los datos. Será la Superintendencia quien determine el personal que tendrá los accesos correspondientes y el tipo de perfiles necesarios.

4. Los procesos de analítica e inteligencia de negocio deberán ejecutarse preferiblemente sobre datos seudonimizados o anonimizados, cuando la identidad no resulte ser un dato indispensable –como en aquellos casos en que existan alertas frente a determinados usuarios del Sistema– aplicando los estándares de seguridad definidos por la Superintendencia de Transporte para mitigar riesgos de exposición innecesaria de información personal.

La re-identificación de los titulares solo será procedente cuando sea indispensable para la sustanciación de hallazgos, auditorías técnicas o procesos administrativos, garantizando siempre la trazabilidad de quién accedió al dato.

4.2.2. Categorías de información y plazos de conservación:

a) **Registros y enrolamiento en los procesos de evaluación teórica, práctica y certificación:** Comprende el conjunto de datos que constituyen el expediente electrónico de cada servicio prestado a un usuario, incluyendo su historial de evaluaciones (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 pruebas prácticas en pista y vía pública y el Certificado de aprobación de los exámenes teórico y práctico.

   Plazo de conservación: Esta información deberá conservarse en el Sistema por un término de **diez (10) años**, contados a partir de la fecha de realización de las evaluaciones y/o expedición de los certificados. 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 CALE:** Comprende los documentos cargados por el CALE 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 demás documentos.

   Plazo de conservación: Esta documentación deberá conservarse de forma accesible en el Sistema durante todo el tiempo en que el CALE se encuentre activo en el Sistema y, posteriormente a su cese de operaciones, deberá archivarse por un término adicional de **cinco (5) años** para fines de auditoría histórica.

c) **Datos biométricos primarios (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 deberán conservase por un plazo de **cinco (5) años** contados a partir de la finalización de la prestación del servicio o de la desvinculación en el caso del personal vinculado al CALE, con el fin de atender posibles reclamaciones post-servicio o procesos de cierre administrativo. Los proveedores tecnológicos deberán certificar semestralmente ante la Superintendencia que han ejecutado los procesos de purga y eliminación de datos que han cumplido su ciclo de vida, a partir del momento en que transcurran los primeros cinco (5) años.

d) **Registros y bitácoras de auditoría del Sistema:** Incluye todos los registros técnicos (logs) generados por el Sistema sobre eventos, acciones de los usuarios, accesos, consultas, errores 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 **diez (10) años**, con el fin de permitir la investigación de incidentes de seguridad, el análisis y la auditoría técnica del sistema.

4.2.3. Obligaciones del proveedor tecnológico del Sistema 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.

4.3. Obligaciones de los proveedores tecnológicos del SICOV para CALE.

Son obligaciones indelegables del proveedor tecnológico encargado de implementar, operar y mantener el Sistema de Control y Vigilancia en los Centros de Apoyo Logístico de Evaluación, las siguientes:

1. **Mantenimiento continuo de las condiciones de operación del Sistema:** Cumplir permanentemente con todos los requisitos de operación del Sistema que dieron lugar a su selección para prestar el servicio, 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 Sistema, detallada 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.

4. **Innovación, vigilancia tecnológica y propuestas de mejora continua:** Realizar una vigilancia tecnológica constante sobre avances aplicables a los sistemas de control, inspección, vigilancia y control, y proponer proactivamente a la Superintendencia de Transporte mejoras funcionales, tecnológicas o de seguridad para el Sistema, orientadas a optimizar su efectividad, eficiencia, evitar la obsolescencia tecnológica y adaptarse a nuevas amenazas o requerimientos regulatorios.

Provisión, desarrollo, operación y mantenimiento técnico del Sistema

5. **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 Sistema 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.

6. **Desarrollo y mantenimiento de funcionalidades del Sistema:** Desarrollar, implementar, probar exhaustivamente y mantener actualizadas todas las funcionalidades del software que hace parte de la infraestructura tecnológica del SICOV.

7. **Interoperabilidad:**

   a) Desarrollar y mantener seguras y eficientes todas las integraciones e interfaces necesarias del Sistema con el Registro Único Nacional de Tránsito (RUNT) y con la infraestructura de los Sistemas de Control y Vigilancia para Centros de Reconocimiento de Conductores (SICOV-CRC), y Centros de Enseñanza Automovilística (SICOV-CEA).

   b) Implementar los mecanismos de interoperabilidad y/o integración para el intercambio seguro de información relevante sobre recursos disponibles y servicios prestados con otros proveedores tecnológicos.

   c) Mantener un registro (logs) detallado e inalterable de todas las transacciones, consultas y operaciones de interoperabilidad realizadas con otros proveedores tecnológicos, 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.

8. **Continuidad del negocio y recuperación ante desastres (BCP/DRP):** Diseñar, documentar, implementar, probar periódicamente y mantener actualizados Planes de Continuidad de Negocio (BCP) y Recuperación ante Desastres (DRP) que aseguren la operación ininterrumpida de los componentes críticos del Sistema 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.

9. **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 Sistema, que incluya análisis de impacto, pruebas, documentación, bitácoras de auditoría y comunicación coordinada permanente con la Superintendencia.

Gestión de información, reportes y soporte a la Superintendencia

14. **Provisión de acceso y herramientas de consulta para la Superintendencia:** garantizar a la Superintendencia de Transporte el acceso seguro, continuo y en tiempo real al Módulo de Supervisión y Control (MSC), proveyendo todas las funcionalidades de consulta, visualización, análisis estadístico y descarga de datos históricos y operativos de los CALE y del propio SICOV, conforme a lo detallado en el presente Anexo Técnico y demás 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 Sistema, aplicando herramientas de analítica de datos e inteligencia artificial para identificar patrones, tendencias y generar las alertas sobre posibles incumplimientos, conductas anómalas o riesgos de fraude.

16. **Reporte de alertas y novedades del sistema a la Superintendencia:** Documentar y remitir de forma oportuna, detallada y automática al Módulo de Supervisión y Control 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 o anomalías técnicas reportadas.

17. **Soporte a la verificación documental y de capacidad:** Apoyar a la Superintendencia en la verificación técnica preliminar y gestión documental para el levantamiento de medidas impuestas a los CALE por incumplimientos presuntos, así como en las inspecciones u órdenes administrativa que esta llegue a impartir.

18. **Visitas técnicas de mantenimiento y reporte de anomalías:** Realizar visitas técnicas para verificar condiciones de operación, la instalación, mantenimiento y brindar soporte en los CALE. El objetivo de estas visitas será verificar el correcto estado y funcionamiento de los componentes de hardware y software que integran el Sistema.

    Si durante estas visitas, el personal del proveedor tecnológico 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.

19. **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 Sistema (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 visitas de inspección a los CALE.

20. **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.

21. **Reporte y soporte técnico en incidentes:** Documentar y reportar diligentemente a la Superintendencia de Transporte cualquier falla técnica generalizada o recurrente del Sistema o de sus componentes que afecte la prestación de servicios por parte de los CALE. Proveer a la Superintendencia la información técnica y los registros del sistema que esta requiera para el análisis de casos específicos de incidentes reportados.

Servicio y soporte a los CALE

22. **Calidad del servicio, soporte técnico y capacitación a CALE:** Garantizar la operación del Sistema con los estándares de calidad y disponibilidad requeridos. Esto incluye proveer un servicio de Mesa de Ayuda eficiente y tiempos de respuesta definidos. Suministrar documentación técnica y de usuario clara y actualizada sobre el Sistema, y ofrecer capacitación continua al personal de los CALE para el uso correcto y seguro del sistema.

23. **Gestión del registro de IDClient:** Gestionar activamente el proceso de registro en el Sistema del IDClient asignado por la RNEC a

cada CALE, incluyendo la implementación del mecanismo de verificación para constatar la no duplicidad de IDClient activos 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 CALE frente al SICOV

Además de las obligaciones generales derivadas de la normatividad que rige su actividad y de aquellas específicas contenidas en otros apartados del presente Anexo Técnico, los CALE 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 las funcionalidades del Sistema para la totalidad de los procesos de pago, registro, validación de identidad y permanencia relacionados con la prestación de sus servicios de evaluación, 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 CALE, vehículos y operación general) que registren o carguen en el Sistema.

3. **Mantenimiento de información de habilitación y operación:** Mantener permanentemente actualizada en el Sistema 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 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:** Mantener permanentemente actualizada la información detallada y veraz de todos los recursos humanos (evaluadores, directivos, administrativos), físicos (aulas, computadores, vehículos, periféricos, dispositivos móviles, gps) y tecnológicos propios o vinculados que utiliza para la prestación del servicio. Será responsabilidad exclusiva e indelegable del CALE 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 proveedor tecnológico del SICOV para CALE, el trámite para la obtención y registro en el Sistema de su Identificador Único ante la RNEC (IDClient).

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 (dispositivos biométricos, cámaras, pads de firmas, GPS, computadores y cualquier otro elemento) y software del Sistemas instalado en sus sedes o vehículos.
7. **Disposición y adecuación del espacio para el funcionamiento de la infraestructura descentralizada del SICOV**. Disponer y adecuar, para garantizar el funcionamiento del SICOV, el espacio físico necesario para

la instalación del rack, equipos y dispositivos de infraestructura descentralizada.

8. Se prohíbe de manera expresa el traslado de ubicación de los dispositivos y suministros asignados a un CALE a otro centro o lugar no autorizado. Asimismo, se prohíbe cualquier intento de manipulación, alteración, desinstalación o daño a dichos equipos. El CALE es el custodio directo y responsable de la integridad de los equipos.

9. Reportar de inmediato al proveedor tecnológico cualquier daño, pérdida, hurto, falla, manipulación no autorizada, intento de alteración o funcionamiento anómalo de estos componentes.

10. **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 emitidas por la Superintendencia de Transporte y/o el proveedor tecnológico para el correcto funcionamiento del Sistema y la seguridad de la información.

11. 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 CALE. Esto implica que los equipos deben cumplir con las condiciones mínimas de operación y realizar las actualizaciones por obsolescencia tecnológica.

12. **Reporte de incidentes de seguridad y fraudes:** Reportar de forma inmediata al proveedor tecnológico cualquier incidente de seguridad informática, acceso no autorizado, intento de fraude, suplantación de identidad, vulnerabilidad detectada en el sistema o uso indebido del Sistema del que tengan conocimiento, ya sea por parte de su personal, usuarios o terceros.

Colaboración, transparencia y debida diligencia

13. **Información sobre novedades operativas:** Informar de manera oportuna y veraz al proveedor tecnológico 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.

14. **Capacitación del personal propio:** Asegurar que todo su personal que interactúa con el Sistema 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.

15. **Facilitación de auditorías e inspecciones:** Permitir, facilitar y prestar toda la colaboración necesaria, diligente y oportuna al personal de la Superintendencia de Transporte durante la realización de visitas de inspección 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.

16. **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.

17. **Obtención de autorizaciones para tratamiento de datos:** Obtener y conservar la autorización previa, expresa e informada de sus usuarios y de todo su personal para el tratamiento de sus datos personales y biométricos a través del SICOV, informándoles claramente sobre las finalidades del tratamiento, el uso de tecnologías de reconocimiento facial, 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

18. **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.

19. **Registro de tarifas:** Registrar y mantener actualizadas las tarifas de todos sus servicios de evaluación.

Hasta aquí el Anexo Técnico.

Versión	Fecha	Detalle	Responsables
1.0	09-06-26	Anexo Técnico de requisitos de operación del SICOV para CALE	**Elaboró:** Carlos Daniel González Cervera, Asesor de Despacho. Fabián Andrés Medina Becerra, Contratista experto vinculado al Despacho. **Revisó:** Alberto José Daza Sagbini, Superintendente Delegado de Tránsito y Transporte. Ángela Paola Galindo Nieto, Directora de Promoción y Prevención de Tránsito y Transporte. Gunther Gabriel Ortíz, Jefe Oficina TIC