REPÚBLICA DE COLOMBIA

Libertad y Orden

MINISTERIO DE TRANSPORTE

SUPERINTENDENCIA DE PUERTOS Y TRANSPORTE

RESOLUCIÓN No. DE

(006832) 04 NOV 2016

Por la cual se expide al anexo técnico para la implementación del Sistema de Control y Vigilancia de que trata la Resolución 05790 de 2016.

EL SUPERINTENDENTE DE PUERTOS Y TRANSPORTE

En ejercicio de las facultades constitucionales y legales, en especial las que le confiere el parágrafo 3 del artículo 3 de la Ley 769 de 2002, modificado por la Ley 1383 de 2010, los artículos 41, 42 y 44 del Decreto 101 de 2000, Modificado Parcialmente por los Decretos 2053 de 2003, 2741 de 2001 y adicionado por el Decreto 540 de 2000 y 1479 de 2014.

CONSIDERANDO

Que el artículo 41 del Decreto 101 de 2000, modificado por el artículo 4 del Decreto 2741 de 2001 y el artículo 3 del Decreto 1016 de 2000, establece dentro del objeto de la delegación que el Presidente de la República le hiciere a la Superintendencia de Puertos y Transporte, respecto a las funciones de inspección, vigilancia y control que le corresponden como suprema autoridad administrativa en materia de tránsito: "*1. Inspeccionar, vigilar y controlar la aplicación y el cumplimiento de las normas que rigen el sistema de tránsito y transporte*".

Que el artículo 44 del Decreto 101 de 2000, le asignó a la Superintendencia de puertos y Transporte, entre otras, las funciones de: "*3. Inspeccionar, vigilar y controlar el cumplimiento de las normas nacionales de tránsito, y aplicar las sanciones correspondientes, en los casos en que tal función no esté atribuida a otra autoridad*", "*10. Solicitar a las entidades públicas que conforman el Sistema Nacional de Transporte la información que estime conveniente para evaluar periódicamente el cumplimiento de las normas de tránsito, transporte e infraestructura*", "*11. Solicitar documentos e información general, incluyendo los libros de comercio, así como practicar las visitas, inspecciones y pruebas que sean necesarias para el cumplimiento de sus funciones*".

Que el parágrafo 1 del artículo 44 del Decreto 101 de 2000, establece "*Sin perjuicio de la conformación de sus propios sistemas de información, la Supertransporte utilizará los registros y demás bases de datos que estén a cargo del Ministerio del Transporte y las demás entidades del sector*".

Que el artículo 4 del Decreto 1016 de 2000, modificado por el artículo 6 del Decreto 2741 de 2001, le asigna como funciones a la Superintendencia de Puertos y Transporte, entre otras, las siguientes: "*4. Inspeccionar, vigilar y controlar el*

1/4 8

Por la cual se expide al anexo técnico para la implementación de los Sistemas de Control y Vigilancia de que trata la Resolución la Resolución 05790 de 2016.

cumplimiento de las normas nacionales de tránsito, y sancionar y aplicar las sanciones correspondientes salvo en materia de tránsito terrestre automotor, aéreo y marítimo", "14. Solicitar a las entidades públicas que conforman el Sistema Nacional de Transporte la información que estime conveniente para evaluar periódicamente el cumplimiento de las normas de tránsito, transporte e infraestructura", "15. Solicitar documentos e información general, inclusive los libros de comercio, así como practicar las visitas, inspecciones y pruebas que sean necesarias para el cumplimiento del objeto de su delegación y funciones", "19. Establecer mediante actos de carácter general las metodologías, criterios y demás elementos o instrumentos técnicos específicos necesarios para el cumplimiento de sus funciones dentro del marco que éstas establecen".

Que el Código Nacional de Tránsito en el parágrafo 3 del artículo 3, modificado por el artículo 2 de la Ley 1383 de 2010, dispone que: "*Las autoridades, los organismos de tránsito, las entidades públicas o privadas que constituyan organismos de apoyo, serán vigiladas y controladas por la Superintendencia de Puertos y Transporte*"; previendo en el Parágrafo 1 de la misma disposición que "*Las entidades públicas o privadas a las que mediante delegación o convenio les sean asignadas determinadas funciones de tránsito, constituirán organismos de apoyo a las autoridades de tránsito*".

Que el parágrafo 1 del artículo 14 de la Ley 769 de 2002, le otorgó a la Superintendencia de Puertos y Transporte la competencia de vigilar y supervisar los centros de enseñanza automovilística.

Que el artículo 2 de la misma Ley define los Centros de enseñanza para conductores como *"establecimiento docente de naturaleza pública, privada o mixtos que tenga como actividad permanente la capacitación de personas que aspiran a conducir vehículos automotores y motocicletas*" y precisa que los Centros Integrales de Atención son aquellos establecimientos donde se presta el servicio de escuela y casa cárcel para la rehabilitación de los infractores a las normas del Código de Tránsito que puede ser operado por el Estado o por entes privados que a través del cobro de las tarifas por los servicios allí prestados, garantizarán su autosostenibilidad.

Que el artículo 2 de la Ley 769 de 2002, "Código Nacional de Tránsito", define a la licencia de conducción como *"el documento público de carácter personal e intransferible expedido por autoridad competente, el cual autoriza a una persona para la conducción de vehículos con validez en todo el territorio nacional".*

Que de conformidad con lo anterior, las actividades desarrolladas por los Centros de Enseñanza Automovilística y los Centros Integrales de Atención, consisten en la capacitación y reeducación de los conductores, lo cual garantiza la idoneidad de los mismos, así como la seguridad de peatones, usuarios, pasajeros, conductores, motociclistas, ciclistas, etc.

Que la Ley 769 de 2002, establece como principios rectores del Tránsito Terrestre, la seguridad de los usuarios, la calidad, la oportunidad, el cubrimiento, la libertad de acceso, la plena identificación, la libre circulación, la educación y la descentralización, los cuales son plenamente aplicables en el desarrollo de las actividades que deben ejecutarse en los Centros de Enseñanza Automovilística y en los Centros Integrales de Atención.

Que de acuerdo a los requisitos establecidos en el artículo 19 de la Ley 769 de 2002, modificado por el artículo 5 de la Ley 1383 de 2010, por el artículo 3 de la Ley 1397

2/18

Por la cual se expide al anexo técnico para la implementación de los Sistemas de Control y Vigilancia de que trata la Resolución la Resolución 05790 de 2016.

de 2010 y por el artículo 196 del Decreto Ley 019 de 2012, para la obtención de la licencia de conducción para vehículos automotores se requiere, entre otros requisitos, el siguiente:

> *"d. Obtener un certificado de aptitud en conducción otorgado por un Centro de Enseñanza Automovilística habilitado por el Ministerio de Transporte e inscrito ante el RUNT".*

Que la Superintendencia de Puertos y Transporte expidió la Resolución 05790 del 12 de febrero de 2016, mediante la cual se reglamentan las características técnicas del Sistema de Control y Vigilancia, de los Centros de Enseñanza Automovilística – CEA y de los Centros Integrales de Atención – CIA.

Que el Decreto 1479 de 2014, por el cual se reglamenta el artículo 19 de la Ley 1702 de 2013 y se dictan otras disposiciones, establece el procedimiento de intervención a los Organismos de Tránsito, así como el procedimiento para la suspensión preventiva, suspensión o cancelación de la habilitación de los organismos de apoyo al tránsito.

Que en el marco de las funciones atribuidas a la Superintendencia de Puertos y Transporte, es deber de la entidad, verificar el cumplimiento de las condiciones, requisitos y procedimientos establecidos en las normas legales y reglamentarias, expedidas por Ley o por el Ministerio de Transporte y cualquier otra disposición que las modifiquen, sustituyan, deroguen o adicionen, para lo cual debe contar con mecanismos de prevención.

Que la función de vigilancia, inspección y control tiene por objeto establecer orden en las actividades que se desarrollan en el sector del transporte, incluidas las actividades de apoyo al tránsito y el mejoramiento de la vigilancia y el control, a través de mecanismos sistematizados, para el desarrollo de tales actividades.

Que además del desarrollo de procesos sancionatorios, la Superintendencia debe generar modelos de supervisión de carácter preventivo, que le permitan generar impacto en beneficio de la movilidad y la seguridad vial.

Que en cumplimiento del numeral 8 del artículo 8, del Código de Administrativo y de lo Contencioso Administrativo, el proyecto de acto administrativo fue publicado en la página WEB de la Superintendencia de Puertos y Transporte, se recibieron los respectivos comentarios y sugerencias, los cuales fueron tenidos en cuenta previa la evaluación de su pertinencia.

En mérito de lo expuesto el Superintendente de Puertos y Transporte,

RESUELVE

Artículo 1. Objeto. El objeto del presente acto administrativo, es expedir el anexo técnico para la implementación del Sistema de Control y Vigilancia de que trata la Resolución 05790 de 2016, proferida por la Superintendencia de Puertos y Transporte, que está contenido en el anexo único de la presente Resolución y hace parte integral del presente acto administrativo.

Artículo 2. Exigibilidad. Las disposiciones contenidas en la presente Resolución serán exigibles de la siguiente manera:

3/9

Por la cual se expide al anexo técnico para la implementación de los Sistemas de Control y Vigilancia de que trata la Resolución la Resolución 05790 de 2016.

2.1. Para los proveedores: Los operadores/proveedores interesados en obtener autorización para prestar el servicio del sistema de control y vigilancia para los Centros de Enseñanza Automovilística – CEA y los Centros Integrales de Atención – CIA y de los Organismos de Tránsito que realicen cursos para obtener descuentos, solo podrán prestar el servicio una vez cuenten con la Homologación por parte de la Superintendencia de Puertos y Transporte, demostrando el cumplimiento de las disposiciones adoptadas mediante el presente acto administrativo.

2.2. Para los de los Centros de Enseñanza Automovilística – CEA y de los Centros Integrales de Atención – CIA y los Organismos de Tránsito que realicen cursos para obtener descuentos. Deberán dar cumplimiento de las disposiciones aquí contenidas, dentro de los dos (2) meses siguientes a que se les comunique que efectivamente por lo menos dos (2) proveedores autorizados, cumplen la totalidad de los requisitos previstos en el presente acto administrativo.

2.3. La implementación del Sistema se realizará de forma gradual y no generará cargas a la operación de los CEAS y CIAS. Los costos de implementación del sistema como software y de equipos necesarios, estarán incluidos en la tarifa establecida por los proveedores homologados del Sistema de Control y Vigilancia para los CEAs y CIAS.

Artículo 3. Vigencia. La presente resolución rige a partir de la fecha de su expedición y será publicada en la página WEB de la Superintendencia de Puertos y Transporte y en el Diario ficial.

06832 04 NOV 2016

PUBLÍQUESE Y CÚMPLASE

JAVIER JARAMILLO RAMÍREZ
Superintendente de Puertos y Transporte

Proyectó: Lina Huari.

a/a

Por la cual se expide al anexo técnico para la implementación del Sistema de Control y Vigilancia de que trata la Resolución 05790 de 2016.

ANEXO TÉCNICO PARA LA IMPLEMENTACIÓN DEL SISTEMA DE CONTROL Y VIGILANCIA DE QUE TRATA LA RESOLUCIÓN 05790 DE 2016.

INTRODUCCIÓN

El presente documento define los requerimientos que deben cumplir aquellos aspirantes a proveedores del Sistema de Control y Vigilancia para los Centros de Enseñanza Automovilística y para los Centros Integrales de Atención. El documento se estructura de la siguiente manera:

El título 1 describe el objetivo del documento, el Sistema de Control y Vigilancia, el marco legal sobre el cual se desarrolla todo el proceso, así como el alcance del presente documento.

El título 2, define los requerimientos técnicos, administrativos, financieros y jurídicos para la homologación de los aspirantes a proveedores del Sistema de Control y Vigilancia, así como los procesos de verificación que cada uno de ellos debe cumplir.

Por la cual se expide al anexo técnico para la implementación del Sistema de Control y Vigilancia de que trata la Resolución 05790 de 2016.

TÍTULO 1 - INFORMACIÓN GENERAL.

En este título se describe los lineamientos que se tienen en cuenta para la construcción de este documento.

1.1 OBJETIVO DEL DOCUMENTO

El presente documento tiene por objetivo definir los requerimientos que deben cumplir y por los cuales se evaluarán a los aspirantes a proveedores del Sistema de Control y Vigilancia de los Centros de Enseñanza Automovilística y los Centros Integrales de Atención

1.2 SISTEMA DE CONTROL Y VIGILANCIA DE LOS CENTROS DE ENSEÑANZA AUTOMOVILISTICA Y DE LOS CENTROS INTEGRALES DE ATENCIÓN.

El Sistema de Control y Vigilancia es una infraestructura tecnológica operada por cualquier ente público o privado que el Centro de Enseñanza Automovilística (en adelante CEA) y el Centro Integral de Atención (en adelante CIA), contrate y que será previamente homologado por la Superintendencia de Puertos y Transporte o por quien esta delegue, para asegurar el cumplimiento de los parámetros establecidos en el presente anexo y de los que se fijen posteriormente, que le permita prestar con calidad el servicio para garantizar:

- La expedición segura del certificado; la identidad y presencia del aspirante/solicitante y de los capacitadores e instructores en el Centro de Enseñanza Automovilística y en el Centro Integral de Atención
- La asistencia y realización de cada una las formaciones teóricas, prácticas y capacitaciones.
- Que el certificado se expida desde la ubicación geográfica del CEA y del CIA.
- Que las pruebas se hagan desde los computadores de los CEA y CIA, con el fin de evitar un posible fraude en la expedición del mencionado certificado.
- El registro del pago.
- La correlación o trazabilidad para el cruce de información.
- Que los CEA y CIA estén conectados con el centro de monitoreo de la Superintendencia de Puertos y Transporte y el RUNT.

Con lo anterior se pretende vigilar y contar la suficiente información que permita establecer que el examen de aptitud para conducir y la asistencia al curso de capacitación, reeducación y/o rehabilitación, se expidió bajo el cumplimiento de los requerimientos y condiciones fijados en las normas vigentes para el tema. Para ello, se hará uso de los medios tecnológicos sistematizados y digitalizados requeridos, para obtener, renovar o recategorizar la licencia de conducción, ante las autoridades de tránsito.

A partir de la anterior definición, se evidencia que el Sistema de Control y Vigilancia para los CEA y CIA, buscan esencialmente garantizar la legitimidad a través de la realización del proceso de aptitud para conducir y de capacitación para el infractor, con el fin de proteger al usuario de la ilegalidad en el proceso de evaluación y certificación, a través de la implementación de características técnicas y de seguridad adecuadas.

1.3 MARCO LEGAL

En concordancia con las facultades otorgadas al Presidente de la República de acuerdo al numeral 16 del artículo 189 de la Constitución Política y desarrolladas por el artículo 37 de

la ley 105 de 1993 y por el artículo 54 de la Ley 489 de 1998, se delegaron las funciones de control, inspección y vigilancia otorgadas al Presidente de la República, contenidas en el numeral 22 del artículo 189 de la Constitución Política de Colombia, a la Superintendencia de Puertos y Transporte con el objeto de inspeccionar, vigilar y controlar la aplicación y el cumplimiento de las normas que rigen el sistema de tránsito y transporte. De la misma manera, inspeccionar vigilar y controlar la permanente, eficiente y segura prestación del servicio de transporte. De esta manera mediante los Decretos 101 de 2000, 1016 de 2000 y 2741 de 2001. Se otorgaron facultades a la Superintendencia de Puertos y Transporte.

En el mismo sentido, el artículo 4 del Decreto 2741 de 2001 determinó que los sujetos de control y vigilancia pueden ser las personas naturales o jurídicas que las normas determinen. En cuanto a los sujetos objeto de vigilancia de la Superintendencia de Puertos y Transporte, dentro del ejercicio de las funciones delegadas y de las otorgadas en virtud de la ley, la Superintendencia puede, examinar y comprobar la transparencia en el manejo de las distintas operaciones y actividades que desarrolla, en cumplimiento de su objeto social, y de las entidades sometidas a su inspección, vigilancia y control. Es así que la Superintendencia de Puertos y Transporte se encuentra dotada de competencia para reglamentar los aspectos administrativos y los demás aspectos que tengan que ver con el funcionamiento de los sistemas de vigilancia, información y control, bajo el entendido del artículo 66 de la Ley 489 de 1998, que consagra que: "Las superintendencias son organismos creados por la ley, con la autonomía administrativa y financiera que aquella les señale, sin personería jurídica, que cumplen funciones de inspección y vigilancia atribuidas por la ley o mediante delegación que haga el Presidente de la República.

1.4 ALCANCE DEL DOCUMENTO

El alcance de este documento incluye la definición de los requerimientos a nivel jurídico, administrativo, financiero y técnico que deben cumplir las entidades aspirantes a operar el Sistema de Control y Vigilancia para los Centros de Enseñanza Automovilística y para los Centros Integrales de Atención.

Los Requerimientos Administrativos, incluyen mecanismos que permitan la validación de aspectos tales como la trayectoria del aspirante a proveedor, experiencia en proyectos similares de tecnología, experiencia del equipo de trabajo entre otros.

Los Requerimientos Financieros, pretenden garantizar que el operador cuente con el respaldo económico suficiente para que inicie el funcionamiento del Sistema y que una vez puesta en marcha la operación tenga sostenibilidad, garantizando a la Superintendencia de Puertos y Transporte, que las entidades homologadas dispongan de los recursos necesarios sostenibles en el tiempo.

Los Requerimientos Jurídicos, buscan principalmente garantizar la legalidad de las entidades a homologarse, de sus representantes, la capacidad jurídica y la facultad que debe tener una persona para adelantar cualquier tipo de proceso con una Entidad Estatal, es decir (i) obligarse a cumplir el objeto del proceso; y (ii) no estar incursa en inhabilidades o incompatibilidades que impidan el ejercicio de las actividades involucradas en el proceso.

Los Requerimientos Técnicos, garantizan idoneidad en la prestación del servicio, buscando que se utilice la tecnología adecuada y actualizada a las necesidades de seguridad, disponibilidad y calidad del servicio.

Este documento contiene los requerimientos generales que deben seguir las entidades

aspirantes a proveedor para conseguir esta meta, y presenta diferentes alternativas para el cumplimiento de los requerimientos con el fin de garantizar pluralidad de oferentes, es así como se incluye por ejemplo alternativas de conformación de uniones temporales o consorcios entre otras.

Con el fin de evitar un solo tipo de propuesta tecnológica, este documento no detalla la solución como tal, sino da libertad a las entidades que se homologuen para que diseñen e implementen sus propios sistemas, garantizando así diferentes tipos de soluciones que se puedan presentar dentro de un marco general de requerimientos.

Este documento describe los procesos que se deben seguir una vez publicada la resolución con todos los requerimientos y su anexo técnico.

TITULO 2 - REQUERIMIENTOS DOCUMENTALES

A continuación se establecen los Requerimientos que deberán cumplir los aspirantes a proveedor para recibir la evaluación documental, estos se deberán suministrar con el fin de que sean corroboradas sus condiciones jurídicas, administrativas, financieras y técnicas.

2.1. Carta de interés y Radicación de Requerimientos Documentales

La carta de interés y radicación de Requerimientos documentales, permitirá iniciar el proceso de validación de los Requerimientos para homologarse como proveedor del Sistema de Control y Vigilancia para los Centros de Enseñanza Automovilística y para los Centros Integrales de Atención. Ver numeral 2.1.2: Modelo Carta de Interés y Radicación de Requerimientos Documentales.

2.1.1. Especificaciones de la entrega del documento:

A continuación, se aclaran algunos detalles respecto al diligenciamiento del modelo de carta de interés y radicación de Requerimientos documentales, descrito en el numeral 2.1.2.

- Debe imprimirse en tamaño carta.
- Debe ir en papel membrete de la compañía.
- **"[NOMBRES APELLIDOS DEL SUPERINTENDENTE DELEGADO]"** Debe ser reemplazado por los nombres y apellidos del Superintendente Delegado nombrado al momento de presentar este documento.
- [RAZON SOCIAL EMPRESA, CONSORCIO O UNIÓN TEMPORAL], debe ser reemplazado por el nombre o razón social del ente aspirante a proveedor a proveedor.
- [Número del NIT], debe ser reemplazado con el Número de Identificación Tributaria de la Empresa o Consorcio. En caso de Unión Temporal deberá colocar el nombre de la Unión temporal y el nombre o razón social de cada una de las empresas que la conforman con su número de NIT.
- **"Resolución NN de 201X"**, donde NN debe ser reemplazada por el número de Resolución que expida la Superintendencia de Puertos y Transporte con el Anexo Técnico de Requerimientos y Requerimientos para el Sistema de Control y Vigilancia de los CENTROS DE ENSEÑANZA AUTOMOVILISTICA Y/O CENTROS INTEGRALES DE ATENCION.
- "NN Folios" donde NN debe ser reemplazado por el número de folios entregados en el medio
físico.

- "NN KBytes" donde NN debe ser reemplazado por el número de Kbytes entregados en el medio electrónico.

2.1.2. Modelo Carta de Interés y Radicación de Requerimientos Documentales.

Ciudad, Fecha (dd/mm/aaaa)

Doctor (a)
[NOMBRES APELLIDOS DEL SUPERINTENDENTE DELEGADO]
Superintendente Delegado de Tránsito y Transporte Terrestre
Automotor SUPERINTENDENCIA DE PUERTOS Y TRANSPORTE
Calle 63 No. 9A – 45. Bogotá. D.C.

REF. Carta de interés para participar en el proceso de validación de Requerimientos para homologarse como proveedor del Sistema de Control y Vigilancia para los CEA y/o CIA

Respetado Doctor,

Mediante el presente oficio deseo manifestar que la empresa (Unión Temporal o Consorcio) [RAZON SOCIAL EMPRESA, CONSORCIO O UNIÓN TEMPORAL] con NIT No. [Número del NIT], la intención de participar en el proceso que adelanta la Superintendencia de Puertos y Transporte para prestar el servicio a los Centros de Enseñanza Automovilística y a los Centros Integrales de Atención como proveedor del Sistema de Control y Vigilancia.

Se anexa los requerimientos documentales exigidos en la Resolución NN de 201X expedida por la Superintendencia de Puertos y Transportes, así:

- Medio Físico, 2 tomos de NN Folios.
- Medio electrónico, 2 CD con NN Kbytes de tamaño.

Agradezco la atención prestada.

Cordialmente,

[NOMBRES APELLIDOS]
REPRESENTANTE LEGAL
[RAZÓN SOCIAL EMPRESA, CONSORCIO O UNIÓN TEMPORAL]

2.2. Requerimientos del aspirante a proveedor.

Este numeral describe la forma como deben ser entregados los documentos con la información que radicará el aspirante a proveedor a ser evaluado como proveedor del Sistema de Control y Vigilancia.

2.2.1. Instrucciones de la presentación del Documento con los Requerimientos del aspirante a proveedor.

Con el fin de estandarizar la entrega de documentos se define a continuación las

características como deben ser presentados:

- ✓ Técnica de empaste: Unibind
- ✓ Color de las Tapas: Transparentes
- ✓ Foliación: El foliado debe quedar en un lugar visible, y que no quede cubierto por ningún texto o membrete.
- ✓ Idioma: El idioma para presentación de los Requerimientos documentales debe ser en español.
- ✓ Papel: Tamaño carta 8.1/2"x11"

2.2.2. Portada

La portada es la primera página y servirá para identificar claramente al aspirante a proveedor que anexa los Requerimientos documentales, esta hoja debe contener el número 1 en área de foliación. Ver numeral 2.2.4 Modelo de la portada general.

2.2.2.1. Especificaciones de la entrega del documento.

A continuación se aclaran algunos detalles respecto al diligenciamiento del modelo de portada, descrito en el numeral 2.2.2.2.

- ✓ Debe colocarse al inicio del documento.
- ✓ Su número de Folio debe ser 1.
- ✓ "RESOLUCION NN DEL **DD** DEL MES DE **MM** DE 2015", debe colocarse el número de la resolución y la fecha de cuando se expida por parte de la Superintendencia de Puertos y Transporte la reglamentación para el proceso de evaluación y homologación de los aspirantes a proveedor del Sistema de Control y Vigilancia para los CEA Y CIA, donde "NN" es el número de la resolución, "DD" es el día y "MM" es el Mes de expedición de la resolución.
- ✓ [RAZON SOCIAL EMPRESA, CONSORCIO O UNIÓN TEMPORAL], debe ser reemplazado por el nombre o razón social del ente aspirante a proveedor a proveedor.
- ✓ [CIUDAD] Ciudad donde se origina la documentación.
- ✓ "201**N**", donde "N" es el último dígito del año en el que se radican los documentos.

2.2.2.2. Modelo de la Portada General.

PRESENTACIÓN DE REQUERIMIENTOS DOCUMENTALES SEGÚN RESOLUCIÓN
NN DEL **DD** DEL MES **MM** DE 2015
EXPEDIDA POR LA SUPERINTENDENCIA DE PUERTOS Y TRANSPORTE

ASPIRANTE:
[RAZÓN SOCIAL EMPRESA, CONSORCIO O UNIÓN TEMPORAL]

CIUDAD]
201**N**

2.2.3. Índice General

El índice general permite organizar el documento en el orden en que se debe entregar, dependiendo de si el aspirante a proveedor es una empresa, una Unión Temporal o un

Consorcio, su contenido puede variar según los Requerimientos específicos para cada caso. Ver numeral 2.2.3.2 Modelo del índice general (Empresa, Unión Temporal o Consorcio).

2.2.3.1. Especificaciones de la entrega del Documento.

- ✓ **"#"** significa que se debe colocar el número de folio en donde se encuentra ubicado.
- ✓ Requerimiento técnico AAA: significa que se debe reemplazar con el nombre del requerimiento
- ✓ **"n"** significa el consecutivo del requerimiento.

2.2.3.2. Modelo del índice general (Empresa, Unión Temporal o Consorcio)

INDICE GENERAL

2.3. LISTA DE REQUERIMIENTOS JURÍDICOS

Los Requerimientos Jurídicos buscan principalmente garantizar la legalidad de las entidades a homologarse y de sus representantes, además validar la capacidad jurídica y la facultad que debe tener una persona para adelantar cualquier tipo de proceso con una Entidad Estatal, es decir (i) obligarse a cumplir el objeto del proceso; y (ii) no estar incursa en inhabilidades o incompatibilidades que impidan el ejercicio de las actividades involucradas en el proceso. Se presenta a continuación algunas consideraciones que se deben tener en cuenta.

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

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

C. Inhabilidades e incompatibilidades:
Las inhabilidades e incompatibilidades están establecidas para asegurar los intereses públicos y proteger la transparencia, objetividad e imparcialidad en las relaciones entre el Estado y los particulares.
El régimen de inhabilidades e incompatibilidades es de aplicación restrictiva, por lo cual cuando existen varias interpretaciones posibles sobre una inhabilidad o incompatibilidad, debe preferirse la que menos limita los derechos de las personas.

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

Las inhabilidades son una limitación a la capacidad de contratar o participar con Entidades
Estatales y están expresamente señaladas en la ley 80 de 1993, la cual establece:

I. Que no son hábiles para participar en Procesos de Contratación, además de quienes están en las siguientes situaciones:
   a. Las personas que se hallen inhabilitadas para contratar por la Constitución y las leyes.
   b. Quienes participaron en las licitaciones o celebraron los contratos de que trata el literal anterior estando inhabilitados. Esta inhabilidad se extenderá por el término de 5 años a partir de la participación en la licitación, o de la celebración del contrato o de la expiración del plazo para su firma.
   c. Quienes dieron lugar a la declaratoria de caducidad. Esta inhabilidad se extenderá por el término de 5 años contados a partir de la fecha de declaratoria del acto de caducidad de quienes han sido condenados por sentencia judicial a la pena accesoria de interdicción de derechos y funciones públicas y quienes hayan sido sancionados disciplinariamente con destitución. Esta inhabilidad se extenderá por el término de 5 años contados a partir de la ejecutoria de la sentencia que impuso la pena, o del acto que dispuso la destitución de quienes sin justa causa se abstengan de suscribir el contrato estatal adjudicado. Esta inhabilidad se extenderá por el término de 5 años a partir de la fecha en que expiró el

plazo para la firma.

d. Los servidores públicos.
e. Quienes sean cónyuges o compañeros permanentes y quienes se encuentren dentro del segundo grado de consanguinidad o segundo de afinidad con cualquier otra persona que formalmente haya presentado propuesta para una misma licitación.
f. Las sociedades distintas de las anónimas abiertas, en las cuales el representante legal o cualquiera de sus socios tenga parentesco en segundo grado de consanguinidad o segundo de afinidad con el representante legal o con cualquiera de los socios de una sociedad que formalmente haya presentado propuesta, para una misma licitación.
g. Los socios de sociedades de personas a las cuales se haya declarado la caducidad, así como las sociedades de personas de las que aquéllos formen parte con posterioridad a dicha declaratoria.
h. Las personas naturales que hayan sido declaradas responsables judicialmente por la comisión de delitos contra la administración pública cuya pena sea privativa de la libertad, o soborno trasnacional, con excepción de delitos culposos. Esta inhabilidad se extenderá a las sociedades de que sean socias tales personas, sus matrices y a sus subordinadas, con excepción de las sociedades anónimas abiertas. La inhabilidad prevista en este literal, se extenderá por un término de veinte (20) años.
i. Las personas que hayan financiado campañas políticas a la Presidencia de la República, a las gobernaciones o a las alcaldías con aportes superiores al dos punto cinco por ciento (2.5%) de las sumas máximas a invertir por los candidatos en las campañas electorales en cada circunscripción electoral, quienes no podrán celebrar contratos con las entidades públicas, incluso descentralizadas, del respectivo nivel administrativo para el cual fue elegido el candidato. La inhabilidad se extenderá por todo el período para el cual el candidato fue elegido. Esta causal también operará para las personas que se encuentren dentro del segundo grado de consanguinidad, segundo de afinidad, o primero civil de la persona que ha financiado la campaña política. Esta inhabilidad comprenderá también a las sociedades existentes o que llegaren a constituirse distintas de las anónimas abiertas, en las cuales el representante legal o cualquiera de sus socios hayan financiado directamente o por interpuesta persona campañas políticas a la Presidencia de la República, a las gobernaciones y las alcaldías.

II. Tampoco podrán participar en licitaciones ni celebrar contratos estatales con la entidad respectiva:

a. Quienes fueron miembros de la junta o consejo directivo o servidores públicos de la entidad contratante. Esta incompatibilidad sólo comprende a quienes desempeñaron funciones en los niveles directivo, asesor o ejecutivo y se extiende por el término de un (1) año, contado a partir de la fecha del retiro.
b. Las personas que tengan vínculos de parentesco, hasta el segundo grado de consanguinidad, segundo de afinidad o primero civil con los servidores públicos de los niveles directivo, asesor ejecutivo o con los miembros de la junta o consejo directivo, o con las personas que ejerzan el control interno o fiscal de la entidad contratante.
c. El cónyuge compañero o compañera permanente del servidor público en los niveles directivo, asesor, ejecutivo, o de un miembro de la junta o consejo directivo, o de quien ejerza funciones de control interno o de control fiscal.

d. Las corporaciones, asociaciones, fundaciones y las sociedades anónimas que no tengan el carácter de abiertas, así como las sociedades de responsabilidad limitada y las demás sociedades de personas en las que el servidor público en los niveles directivo, asesor o ejecutivo, o el miembro de la junta o consejo directivo, o el cónyuge, compañero o compañera permanente o los parientes hasta el segundo grado de consanguinidad, afinidad o civil de cualquiera de ellos, tenga participación o desempeñe cargos de dirección o manejo. Esta inhabilidad no se aplicará en relación con las corporaciones, asociaciones, fundaciones y sociedades allí mencionadas, cuando por disposición legal o estatutaria el servidor público en los niveles referidos debe desempeñar en ellas cargos de dirección o manejo.
e. Los miembros de las juntas o consejos directivos. Esta incompatibilidad sólo se predica respecto de la entidad a la cual prestan sus servicios y de las del sector administrativo al que la misma esté adscrita o vinculada.
f. Directa o indirectamente las personas que hayan ejercido cargos en el nivel directivo en entidades del Estado y las sociedades en las cuales estos hagan parte o estén vinculados a cualquier título, durante los dos (2) años siguientes al retiro del ejercicio del cargo público, cuando el objeto que desarrollen tenga relación con el sector al cual prestaron sus servicios.

   Esta incompatibilidad también operará para las personas que se encuentren dentro del primer grado de consanguinidad, primero de afinidad, o primero civil del ex empleado público.

   De igual forma la Ley 80 de 1993 prevé las inhabilidades e incompatibilidades sobrevinientes, estableciendo que de llegar a sobrevenir inhabilidad o incompatibilidad en el contratista, este cederá el contrato previa autorización escrita de la entidad contratante o, si ello no fuere posible, renunciará a su ejecución. Cuando la inhabilidad o incompatibilidad sobrevenga en un proponente dentro de una licitación, se entenderá que renuncia a la participación en el proceso de selección y a los derechos surgidos del mismo.

   Si la inhabilidad o incompatibilidad sobreviene en uno de los miembros de un consorcio o unión temporal, éste cederá su participación a un tercero previa autorización escrita de la entidad contratante. En ningún caso podrá haber cesión del contrato entre quienes integran el consorcio o unión temporal.

2.3.1. Certificado de existencia y representación, expedido por la Cámara de Comercio.

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

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

2.3.1.1. Especificaciones de la entrega del documento.

- ✓ Se debe presentar en original.
- ✓ Su expedición debe ser igual o inferior a 30 días calendario al de la fecha de radicación.
- ✓ Si la propuesta es presentada en Unión Temporal o en Consorcio, se debe adicionar el certificado de cámara de comercio de cada una de la personas naturales y/o jurídicas que lo(a) conformen.

2.3.2. Registro Único Tributario

Es el mecanismo único para identificar, ubicar y clasificar a las personas y entidades que tengan la calidad de contribuyentes declarantes del impuesto sobre la renta y no contribuyentes declarantes de ingresos y patrimonio; los responsables del régimen común y los pertenecientes al régimen simplificado; los agentes retenedores; los importadores, exportadores y demás usuarios aduaneros, y los demás sujetos de obligaciones administradas por la U.A.E. Dirección de Impuestos y Aduanas Nacionales DIAN, respecto de los cuales esta requiera su inscripción. Sirve para cerciorarse e identificar la actividad económica ante terceros con quienes sostenga una relación comercial, laboral o económica en general y ante los diferentes entes de supervisión y control, a su vez, este documento le señala sus obligaciones frente al Estado Colombiano.

El aspirante a proveedor debe presentar dentro de su propuesta fotocopia legible del Registro Único Tributario – RUT expedido por la DIAN. La información contentiva en el R.U.T. deberá encontrarse actualizada conforme a los datos reales del aspirante a proveedor, acorde con lo dispuesto en las Resoluciones 139 y 154 de 2012, emitidas por la Dirección General de Impuestos y Aduanas Nacionales y las normas posteriores que las modifiquen y/o adicionen.

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

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

2.3.2.1. Especificaciones de la entrega del documento.

- ✓ Se debe presentar copia del RUT (Registro Único Tributario).

✓ Si la propuesta es presentada en Unión Temporal o en Consorcio, se debe adicionar el Registro Único Tributario de cada una de la personas naturales y/o jurídicas que lo(a) conformen.

✓ Deben estar presentes los códigos CIIU de la actividad económica, con la versión vigente.

Las siguientes son las actividades económicas según el CIIU en su última versión consolidadas por grupo, división y clase que serán la base de este requisito, los aspirantes a proveedor deberán tener al menos una de las siguientes actividades:

☐ **6201:** Actividades de Desarrollo de sistemas informáticos, consultoría informática y actividades relacionadas.

Esta clase comprende el análisis, el diseño, la escritura, pruebas, modificación y suministro de asistencia en relación con programas informáticos.

Esta clase incluye:

- El análisis, diseño de la estructura, el contenido y/o escritura del código informático necesario para crear y poner en práctica programas de sistemas operativos, aplicaciones de programas informáticos (incluyendo actualizaciones y parches de corrección), también bases de datos.
- El desarrollo de soluciones web (sitios y páginas web) y personalización de programas informáticos a clientes, es decir, modificar y configurar una aplicación existente a fin de que sea funcional con los sistemas de información de que dispone el cliente.

Esta clase excluye:

- La edición de paquetes de software o programas informáticos comerciales. Se incluye en la clase 5820, «Edición de programas de informática (software)».
- La planificación y diseño de sistemas que integren el equipo de hardware, software y tecnologías de la comunicación, aunque el suministro del software se constituya como una parte integral del servicio. Se incluye en la clase 6202, «Actividades de consultoría de informática y actividades de administración de instalaciones informáticas».

☐ **6202:** Actividades de consultoría informática y actividades de administración de instalaciones informáticas.

Esta clase incluye:

- La planificación y el diseño de los sistemas informáticos que integran el equipo (hardware), programas informáticos (software) y tecnologías de las comunicaciones (incluye redes de área local [LAN], red de área extensa [WAN], entre otras).
- Las unidades clasificadas en esta clase pueden proporcionar los componentes de soporte físico y lógico (como pueden ser el hardware y software) como parte de sus servicios integrados o estos componentes pueden ser proporcionados por terceras partes o vendedores. En muchos casos las unidades clasificadas en esta clase suelen instalar el sistema, capacitar y apoyar a los usuarios del sistema.
- Los servicios de gerencia y operación en sitio, de sistemas informáticos y/o instalaciones informáticas de procesamiento de datos de los clientes, así como también servicios de soporte relacionados.
- Los servicios de consultoría en el diseño de sistemas de administración de información y en equipos de informática.

- Los servicios de consultoría para sistemas de ingeniería y fabricación asistida por computador.
- El servicio de análisis de requerimientos para la instalación de equipos informáticos.

Esta clase excluye:

- La venta por separado de equipos o programas informáticos. Se incluye en la clase 4651, «Comercio al por mayor de computadores, equipo periférico y programas de informática» y en la clase 4741, «Comercio al por menor de computadores, equipos periféricos, programas de informática y equipos de telecomunicaciones en establecimientos especializados», según corresponda.
- La instalación de computadores centrales y equipos similares. Se incluye en la clase 3320, «Instalación especializada de maquinaria y equipo industrial».
- La instalación por separado (configuración) de los computadores personales e instalación por separado de software. Se incluye en la clase 6209, «Otras actividades de tecnologías de información y actividades de servicios informáticos».

6311: Procesamiento de datos, alojamiento (hosting) y actividades relacionadas

Esta clase incluye:

- El suministro de infraestructura para servicios de hosting, servicios de procesamiento de datos y actividades conexas relacionadas.
- Las actividades especializadas en alojamiento de: sitios web, servicios de transmisión de secuencias de video por internet (streaming), aplicaciones, entre otros.
- El suministro de servicios de aplicación.
- El suministro a los clientes de acceso en tiempo compartido a servicios centrales.
- Las actividades de procesamiento de datos: elaboración completa de datos facilitados por los clientes y generación de informes especializados a partir de los datos facilitados por los clientes.
- El suministro de servicio de registro de datos.
- La tabulación y la digitación de todo tipo de datos.
- El escaneo óptico de datos y de documentos.
- El funcionamiento de oficinas de servicio de informática dedicadas al procesamiento de datos y alojamiento web.

Esta clase excluye:

- La explotación de los sitios web. Se incluye en la clase 6312, «Portales web».

2.3.3. Copia de Documento de Identidad del Representante Legal.

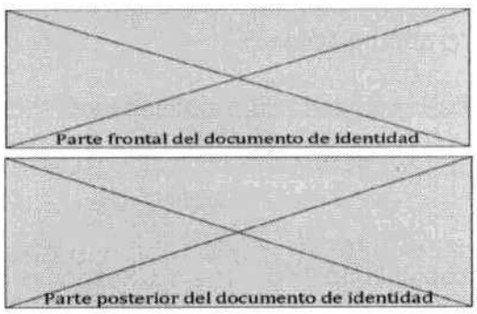
El documento de identidad es llamado Cédula de Ciudadanía o C.C., para el caso de los ciudadanos colombianos mayores de edad. Éste es el único documento de identificación válido para todos los actos civiles, políticos, administrativos y judiciales según la ley 39 de 1961. Se expide para los ciudadanos colombianos al cumplir los 18 años de edad (mayoría de edad en Colombia). El organismo encargado para realizar las tareas de expedición de cédulas es la Registraduría Nacional del Estado Civil de Colombia. En el caso de los extranjeros, existe la Cédula de Extranjería que expide Migración de Colombia a manera de documento de identificación, con los mismos efectos que la Cédula de Ciudadanía.

Por la cual se expide al anexo técnico para la implementación del Sistema de Control y Vigilancia de que trata la Resolución 05790 de 2016.

Ver Numeral 2.3.3.1: Modelo Copia de Documento de Identidad del Representante Legal.

2.3.3.1. Modelo Copia de Documento de Identidad del Representante Legal.

Esta copia está dirigida al archivo de los Requerimientos documentales presentados por [RAZÓN SOCIAL EMPRESA, CONSORCIO O UNIÓN TEMPORAL], para presentar propuesta como proveedor del Sistema de Control y Vigilancia de la Superintendencia de Puertos y Transporte.



Firma.

VÁLIDA ÚNICAMENTE COMO REQUISITO DOCUMENTAL PARA PROCESO DE EVALUACIÓN SUPERTRANSPORTE.

2.3.3.2. Especificaciones de la entrega del documento.

La copia del documento de identidad debe estar a una ampliación de 150%. La firma es de la persona que aparece en el documento de identidad.
En caso de ser el representante legal de una persona parte de una Unión Temporal o Consorcio debe escribir: [RAZÓN SOCIAL UNIÓN TEMPORAL O CONSORCIO (RAZÓN SOCIAL EMPRESA)]

2.3.4. Certificado del Pago de aportes parafiscales.

Toda empresa o unidad productiva que tenga trabajadores vinculados mediante Contrato de trabajo debe hacer un aporte equivalente al 9% de su Nómina por concepto de los llamados aportes parafiscales, los cuales se distribuirán de la siguiente forma: 4% para el subsidio familiar (Cajas de Compensación Familiar), 3% para el Instituto Colombiano de Bienestar Familiar (ICBF) y 2% para el Servicio Nacional de Aprendizaje (SENA), o la normatividad vigente.

Acorde con lo señalado en el artículo 50 de la Ley 789 de 2002 y en el artículo 23 de la Ley 1150 de 2007 el aspirante a proveedor, deberá entregar una certificación de cumplimiento de sus obligaciones con los sistemas de salud, riesgos profesionales, pensiones y aportes a las Cajas de Compensación Familiar, Instituto Colombiano de Bienestar Familiar y Servicio Nacional de Aprendizaje, expedida por el Revisor Fiscal, cuando exista según los requerimientos de Ley, o por el Representante Legal de la sociedad interesada, en la que se acredite que dicha compañía se encuentra al día en el pago de aportes al Sistema de Seguridad Social Integral (E.P.S, AFP, ARP, Caja de Compensación familiar, ICBF y SENA).

2.3.4.1. Especificaciones de la entrega del documento.

- ✓ Certificado emitido por revisor fiscal o representante legal según corresponda, basado en el tipo Certificado de persona.
- ✓ Su expedición debe ser igual o inferior a 30 días calendario al de la fecha de radicación.
- ✓ Si la propuesta es presentada en Unión Temporal o en Consorcio, se debe adicionar el certificado de pago de aportes parafiscales de cada una de la personas naturales y/o jurídicas que lo(a) conformen.
- ✓ En caso de ser un revisor fiscal el obligado a emitir el certificado deberá anexar fotocopia de la cédula de ciudadanía, fotocopia de la tarjeta profesional y antecedentes disciplinarios de la Junta Nacional de Contadores.

2.3.5. Certificación de composición de socios o accionistas.

Certificado firmado por el Representante Legal o el Revisor Fiscal dependiendo del tipo de empresa, en el que se relacionan los socios y/o accionistas o asociados que tengan directa o indirectamente el 5% o más del capital social, aporte o participación. Cuando esta información no conste en el certificado de existencia o representación expedido por la Cámara de Comercio. La certificación debe tener corte de la información en un término no superior a treinta (30) días de la fecha de presentación de la propuesta. Si dentro de la composición accionaria de la empresa se encuentra una Persona Jurídica cuya participación sea igual o superior al 5% del capital, esta debe aportar la composición de participación accionaria, proceso que debe repetirse hasta que los accionistas sean personas naturales. De cada accionista se debe incluir: Nombre o razón social, identificación y porcentaje de participación, siempre y cuando esta sea igual o superior al 5%. Ver numeral 2.3.5.2: Modelo de Certificación de Composición Accionaria.

2.3.5.1. Especificaciones de la entrega del documento.

El certificado de composición de socios o accionistas deberá ser emitido por el Revisor Fiscal de la empresa o consorcio. En el caso de Unión Temporal se deberá presentar un certificado de composición de socios o accionistas de cada una de las empresas que conforman la Unión Temporal. En caso de no presentar la composición accionaria por su naturaleza jurídica, el Representante Legal del aspirante a proveedor deberá presentar una declaración juramentada, con reconocimiento de texto, firma y huella en Notaría, de que no participará en más de una propuesta para el presente proceso.

El certificado deberá ser autenticado con firma y huella.
[RAZÓN SOCIAL EMPRESA, CONSORCIO O UNIÓN TEMPORAL], deberá reemplazarse por el nombre del ente.
[Número de NIT], debe ser reemplazado con el Número de Identificación Tributaria de la Empresa o Consorcio. En caso de Unión Temporal deberá colocar el nombre de la Unión Temporal y el nombre o razón social de cada una de las empresas que la conforman con su número de NIT, el Revisor Fiscal de cada empresa deberá expedir el certificado de la

composición accionaria.
Deberá certificar el 100% de las acciones de la compañía.
[NN], debe reemplazarse por el día en número que se expide el certificado
[Mes en Letras], debe reemplazarse por el mes que se expide el certificado, descrito en letras. [AAAA], debe reemplazarse por el año en que se expide el certificado, descrito en cuatro dígitos. [Número de la Tarjeta Profesional], debe reemplazarse por el número de la Tarjeta Profesional del Revisor Fiscal Vigente.
Huella del Revisor Fiscal o Representante Legal dependiendo el tipo de empresa, debe colocarse la huella del Revisor Fiscal la cual debe ir autenticada.

1. En el caso de ser una sociedad por acciones simplificadas SAS, podrá participar siempre y cuando presente la composición. En caso de no presentar la composición accionaria por su naturaleza jurídica, el Representante Legal del aspirante a proveedor deberá presentar una declaración juramentada, con reconocimiento de texto, firma y huella en Notaría, de que no participará en más de una propuesta para el presente proceso.

2.3.5.2. Modelo de Certificación de Composición Accionaria

Ciudad, Fecha (dd/mm/aaaa)

Composición accionaria
CERTIFICACIÓN DEL REVISOR FISCAL

El suscrito Revisor Fiscal de [RAZÓN SOCIAL EMPRESA, CONSORCIO O UNIÓN TEMPORAL]., identificada con NIT No. [Número de NIT], hace constar que de acuerdo con el libro oficial de registro de accionistas, inscrito en el registro mercantil, de conformidad con las normas de auditoría generalmente aceptadas en Colombia.

CERTIFICA QUE:
La composición accionaria es la siguiente:

CC/NIT	**ACCIONISTA**	**ACCIONISTAS [RAZÓN SOCIAL EMPRESA, CONSORCIO] AL CORTE DE [DD/MM/AA]**		**%**
		No. DE ACCIONES	**VALOR NOMINAL**	
[Número]	[RAZÓN SOCIAL O NOMBRE]	NNN	$$$,00 COP	NN%
[Número]	[RAZÓN SOCIAL O NOMBRE]	NNN	$$$,00 COP	NN%
. . .				
TOTALES		**No. Total de acciones**	**$$$,00 COP**	**100,00000 %**

Se expide a los [NN] días del mes de [Mes en Letras] de [AAAA], con destino a proceso de evaluación y homologación como aspirante a proveedor del Sistema de Control y Vigilancia para los CEA Y CIA.

Cordialmente,

Huella del Revisor Fiscal

[NOMBRES Y APELLIDOS DEL REVISOR FISCAL] Revisor Fiscal
T.P. [Número de la Tarjeta Profesional]
[RAZÓN SOCIAL O NOMBRE DE LA EMPRESA O CONSORCIO]

2.4. LISTA DE REQUERIMIENTOS ADMINISTRATIVOS.

Los Requerimientos Administrativos incluyen mecanismos que permitan la validación de aspectos tales como la trayectoria del aspirante a proveedor, experiencia en proyectos similares de tecnología, experiencia del equipo de trabajo entre otros.

2.4.1. Experiencia de la Compañía.

La experiencia es el conocimiento del aspirante a proveedor derivado de su participación previa en actividades iguales o similares a las previstas en el objeto del contrato.

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

La experiencia requerida debe ser adecuada y proporcional a la naturaleza del contrato o actividad y su valor. La experiencia es adecuada cuando es afín al tipo de actividades previstas en el objeto del contrato o actividad a celebrar. La experiencia es proporcional cuando tiene relación con el alcance, la cuantía y complejidad del contrato o actividad a celebrar.

La experiencia del Oferente Plural (Unión Temporal, Consorcio y promesa de Sociedad Futura) corresponde a la suma de la experiencia que acredite cada uno de los integrantes del aspirante a proveedor plural.

Por otra parte, cuando un aspirante a proveedor adquiere experiencia en un contrato o actividad como integrante de un Contratista Plural, la experiencia derivada de ese contrato o actividad corresponde a la ponderación del valor del contrato por el porcentaje de participación.

La experiencia a acreditar debe estar compuesta de una combinación de actividades que garantice la cobertura de todos los aspectos que intervienen en la conformación del Sistema de Control y Vigilancia para los Centros de Enseñanza Automovilística y los Centros Integrales de Atención.

Conforme a lo establecido en el MANUAL PARA DETERMINAR Y VERIFICAR LOS REQUERIMIENTOS HABILITANTES EN LOS PROCESOS DE CONTRATACIÓN-VERSIÓN M- DVRHPC-04 DE COLOMBIA COMPRA EFICIENTE: "Si en el Proceso de Contratación no es obligatorio que los oferentes cuenten con RUP, la Entidad Estatal de forma autónoma debe definir la forma de acreditar los Requerimientos habilitantes de experiencia, capacidad jurídica, capacidad financiera y capacidad organizacional". En este caso, la Entidad considera que los Requerimientos exigidos a continuación aseguren la idoneidad de los posibles proveedores.

1) Cuantía total de la experiencia requerida. La cuantía de la experiencia debe ser igual o superior a 7.759 SMMLV (salarios mínimos mensuales legales vigentes).

2) Cuando las certificaciones expresen su valor en dólares, se tendrá en cuenta la

TRM a la fecha en que se celebró el contrato certificado.

3) En caso de presentar certificaciones globales. Deberán desglosar el monto o porcentaje y objeto para el cual aplica dicha certificación.

4) Número de contratos a certificar: Los aspirantes deberán acreditar experiencia mediante certificación firmada por los contratantes o entes gubernamentales en máximo seis (6) certificaciones.

5) Antigüedad en celebración de contratos: Las certificaciones de experiencia ejecutada deberán tener una antigüedad máxima de cinco (5) años a la fecha de radicación de la carta de interés.

6) Acreditación de la experiencia: Acreditar experiencia mediante certificación firmada por los clientes o entidades gubernamentales en por lo menos un proyecto en sistemas que incluyan alguna de las siguientes funcionalidades:

   a) Seguridad Informática y/o Seguridad de la Información: Manejo de Riesgo, Protección de Datos, Cifrado de Información, Auditoria de Bases de Datos, Centro de Operaciones de Seguridad (SOC), Correlación de Eventos.

   b) Software: Desarrollo y/o Implantación de Software.

7) Cumplimiento de contratos: Aquellas certificaciones de experiencia que califiquen el cumplimiento del contrato como "malo", "regular", o expresiones similares que demuestren el cumplimiento no satisfactorio del mismo o que indiquen que durante su ejecución fueron sujetas a multas o sanciones debidamente impuestas por la administración o que a las mismas se les haya hecho efectiva la cláusula penal estipuladas en los contratos, no se aceptarán por el ente evaluador.

El aspirante a proveedor acreditará la experiencia requerida para este proceso de evaluación a través de los siguientes pasos: a) mediante el diligenciamiento del Modelo de Certificaciones de Experiencia del Aspirante, numeral 2.4.1.2; y, b) mediante la presentación de certificaciones expedidas por quien otorga la misma. En caso de que el comité evaluador requiera información adicional, se solicitará la copia del contrato.

2.4.1.1. Especificaciones de la entrega del documento.

Cada formato de certificaciones de experiencia del aspirante a proveedor deberá estar firmado y con huella legible por el Representante Legal del aspirante a proveedor debidamente autenticado en Notaría con firma y huella.

Deberá aportar adicionalmente una certificación firmada por parte del cliente con el objeto del contrato, monto, la fecha de inicio del contrato, la fecha de finalización del contrato, calificación del cumplimiento o porcentaje de ejecución.

Si la propuesta es presentada en Unión Temporal o en Consorcio, se debe presentar el Modelo de
Certificaciones de Experiencia del aspirante a proveedor de cada una de las empresas que lo(a) conformen.

2.4.1.2. Modelo de Certificaciones de Experiencia del Aspirante

MODELO DE CERTIFICACIONES DE EXPERIENCIA DEL ASPIRANTE

EMPRESA QUE CERTIFICA	
FECHA DE EXPEDICIÓN DE LA CERTIFICACIÓN	DD/MM/AAAA
NOMBRE O RAZÓN SOCIAL DEL CLIENTE	
NIT DEL CLIENTE	
OBJETO DEL CONTRATO – (SOLO SI APLICA)	
NOMBRES Y APELLIDOS DE QUIEN EXPIDE LA CERTIFICACIÓN	
Grupo y Actividad al que pertenece esta experiencia	• Seguridad Informática y/o Seguridad de la Información: Manejo de Riesgo, Protección de Datos, Cifrado de Información, Auditoria de Bases de Datos, Centro de Operaciones de Seguridad (SOC), Correlación de Eventos. • Software: Desarrollo y/o Implantación de Software.
FECHA DE INICIO	MM/AAAA
SI ACTÚA EN UNIÓN TEMPORAL O CONSORCIO INDICAR EL % DE PARTICIPACIÓN	
FECHA TERMINACIÓN	MM/AAAA
VALOR – (SOLO SI APLICA)	COP vigencia 2015 – SMMLV vigencias posteriores.
PORCENTAJE DE EJECUCIÓN	
PÁGINA WEB DEL CLIENTE	
CORREO ELECTRÓNICO DEL CONTACTO-CLIENTE	
TELÉFONO DEL CONTACTO-CLIENTE	
CIUDAD Y DIRECCIÓN DEL CLIENTE	
Firma y Huella Representante Legal del Aspirante	

2.4.2. Certificaciones exigibles a la Compañía.

El aspirante a proveedor del Sistema de Control y Vigilancia deberá contar con certificación de Sistema de Gestión de la Calidad. En caso de Unión Temporal o Consorcio al menos una de las sociedades deberá contar con la certificación de calidad. La certificación deberá estar vigente a la fecha de evaluación.

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

  El aspirante a proveedor del Sistema de Control y Vigilancia deberá contar por lo menos con una de las siguientes certificaciones: CMMI nivel 3 o superior en cualquier de sus áreas, IT MARK, ISO 27001 (una vez la Superintendencia Financiera lo exija a sus vigilados y según el numeral 2.4.4 del presente anexo), ISO 20000, ISO 15504.

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

  Las mejores prácticas CMMI se publican en los documentos llamados modelos. En la actualidad hay tres áreas de interés cubiertas por los modelos de CMMI: Desarrollo, Adquisición y Servicios. El Modelo presenta 5 Niveles de Madurez. Para ser evaluado en determinado nivel, se debe implementar un conjunto determinado de Prácticas (requeridas).

  A grandes rasgos, estas son las características de cada nivel:
  NIVEL 1: En este Nivel se encuentra la mayoría de las organizaciones. Los procesos son impredecibles, pobremente controlados y reactivos.
  NIVEL 2: Las áreas de proceso de este Nivel están orientadas a la gestión. Los procesos son definidos, documentados, utilizados y medidos.
  NIVEL 3: En este Nivel los procesos se encuentran estandarizados y documentados a nivel organizacional. Las áreas de proceso que se incorporan están orientadas a la ingeniería. NIVEL 4: En este Nivel los procesos son Predecibles Medibles y Controlables. La Calidad y productividad son predecibles cuantitativamente.
  NIVEL 5: Las organizaciones que se encuentran en este Nivel ponen foco en el mejoramiento continuo de sus procesos.

- **IT MARK:** Es una certificación en métodos técnicos y de negocio, enfocado hacia la mejora de procesos en Pymes del sector de tecnologías de información. IT Mark trabaja en componentes tales como la gestión de negocios que desarrollan estrategias comercial, financiera y de mercado. Además evalúa las inversiones de capital de riesgo, la gestión de seguridad de la información y finalmente, la implementación de procesos de software y sistema. De acuerdo al Ministerio TIC, las empresas que implementan IT Mark, tienen mejoras representativas en el desempeño empresarial, logran enormes avances hacia la calidad, eficiencia, productividad y competitividad, hasta lograr la madurez de sus organizaciones.

- **ISO 27001:** Es una certificación define cómo organizar la seguridad de la información en cualquier tipo de organización, con o sin fines de lucro, privada o pública, pequeña o grande. Es posible afirmar que esta norma constituye la base para la gestión de la seguridad de la información. La ISO 27001 es para la seguridad de la información lo mismo que la ISO 9001 es para la calidad: es una norma redactada por los mejores especialistas del mundo en el campo de seguridad de la información y su objetivo es proporcionar una metodología para la implementación de la seguridad de la información en una organización. También permite que una organización sea certificada, lo cual significa que una entidad de certificación independiente ha confirmado que la seguridad de la información se ha implementado en esa organización de la mejor forma posible.

A raíz de la importancia de la norma ISO 27001, muchas legislaturas han tomado esta norma como base para confeccionar las diferentes normativas en el campo de la protección de datos personales, protección de información confidencial, protección de sistemas de información, gestión de riesgos operativos en instituciones financieras, etc.

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

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

- **ISO 15504:** Es un estándar internacional de evaluación y determinación de la capacidad y mejora continua de procesos de ingeniería del software, con la filosofía de desarrollar un conjunto de medidas de capacidad estructuradas para todos los procesos del ciclo de vida y para todos los participantes. Es el resultado de un esfuerzo internacional de trabajo y colaboración y tiene la innovación, en comparación con otros modelos, del proceso paralelo de evaluación empírica del resultado. Norma que trata los procesos de ingeniería, gestión, relación cliente-proveedor, de la organización y del soporte. Se creó por la alta competencia del mercado de desarrollo de software, a la difícil tarea de identificar los riesgos, cumplir con el calendario, controlar los costos y mejorar la eficiencia y calidad. Este engloba un modelo de referencia para los procesos y sus potencialidades sobre la base de la experiencia de compañías grandes, medianas y pequeñas.

En caso de Unión Temporal o Consorcio al menos una de las sociedades debe contar con la certificación en sistema de gestión de la calidad ISO 9001 y por lo menos uno de los miembros deberá contar con alguna de las certificaciones solicitadas (CMMI Nivel 3 o superior, IT MARK, ISO 27001 (una vez la Superintendencia Financiera lo exija a sus vigilados y según el numeral 2.4.4 del presente anexo), ISO 20000 o ISO 15504. La certificación deberá estar vigente a la fecha de evaluación.

El aspirante a proveedor acreditará las certificaciones requeridas para este proceso de evaluación a través de los siguientes pasos: a) mediante el diligenciamiento del Modelo de Certificaciones Exigibles a la compañía, numeral 2.4.2.2.; y, b) mediante la presentación de certificaciones expedidas por quien otorga la misma. En caso de que el comité evaluador requiera información adicional, se le solicitará a la compañía aspirante.

2.4.2.1. Especificaciones de la entrega del documento.

Cada formato de certificaciones exigibles a la compañía del aspirante a proveedor deberá estar diligenciado y también firmado con huella legible por el Representante Legal del

aspirante a proveedor debidamente autenticado en Notaría con firma y huella.

Deberá aportar la(s) certificación(es) en ISO 9001 expedidas por las entidades certificadoras autorizadas y alguna de las siguientes certificaciones solicitadas: IT MARK, CMMI nivel 3 o superior, ISO 27001, ISO 20000 o ISO 15504. Si la propuesta es presentada en Unión Temporal o en Consorcio, se debe presentar el Modelo de certificaciones exigibles a la compañía de cada una de las empresas que lo(a) conformen y al menos una compañía o sociedad deberá cumplir con el certificado de calidad ISO 9001.

Marque con una X en los cuadros de diálogo donde cumpla y aporte los Requerimientos.

2.4.2.2. M o d e l o de Certificaciones Exigibles a la compañía del aspirante

MODELO DE CERTIFICACIONES EXIGIBLES A LA COMPAÑÍA DEL ASPIRANTE	
NOMBRE O RAZÓN SOCIAL DE LA COMPAÑÍA DEL ASPIRANTE	
NIT DE LA COMPAÑÍA DEL ASPIRANTE	
NOMBRES Y APELLIDOS DEL REPRESENTANTE LEGAL DE LA COMPAÑÍA DEL ASPIRANTE	
CERTIFICACIONES APORTADAS	Sistema Gestión de la Calidad: • ISO-9001 • GP-1000 entidades públicas Alguna o Varias de las siguientes Certificaciones: • ISO 27001 • ISO 20000 • ISO 15504 • CMMI • IT MARK
Certificación **ISO 9001** Certificado No._____ Fecha de Expedición: DDMMAAAA Fecha de Vencimiento: DDMMAAAA Entidad Certificadora: _____ Teléfono Contacto Ent. Certificadora:_____ Web Consulta Ent. Certificadora:_____ e-mail contacto Ent. Certificadora:_____	Certificación **ISO 27001** Certificado No._____ Fecha de Expedición: DDMMAAAA Fecha de Vencimiento: DDMMAAAA Entidad Certificadora: _____ Teléfono Contacto Ent. Certificadora:_____ Web Consulta Ent. Certificadora:_____ e-mail contacto Ent. Certificadora:_____

Certificación **ISO 20000** Certificado No._____ Fecha de Expedición: DDMMAAAA Fecha de Vencimiento: DDMMAAAA Entidad Certificadora: Teléfono Contacto Ent. Certificadora:_____ Web Consulta Ent. Certificadora:_____ e-mail contacto Ent. Certificadora:_____	Certificación **ISO 15504** Certificado No._____ Fecha de Expedición: DDMMAAAA Fecha de Vencimiento: DDMMAAAA Entidad Certificadora: Teléfono Contacto Ent. Certificadora:_____ Web Consulta Ent. Certificadora:_____ e-mail contacto Ent. Certificadora:_____
Certificación **CMMI** Nivel_____ Certificado No._____ Fecha de Expedición: DDMMAAAA Fecha de Vencimiento: DDMMAAAA Entidad Certificadora: Teléfono Contacto Ent. Certificadora: _____ Web Consulta Ent. Certificadora: _____ e-mail contacto Ent. Certificadora: _____	Certificación **IT MARK** Certificado No._____ Fecha de Expedición: DDMMAAAA Fecha de Vencimiento: DDMMAAAA Entidad Certificadora: Teléfono Contacto Ent. Certificadora: _____ Web Consulta Ent. Certificadora: _____ e-mail Contacto Ent. Certificadora: _____
_____ Firma y Huella Representante Legal del Aspirante	

2.4.3. Equipo de Trabajo exigible a la compañía

El equipo de trabajo es el personal mínimo idóneo que debe tener la compañía para la ejecución del proyecto garantizando la atención suficiente y oportuna a todos los frentes operacionales involucrados dentro del funcionamiento del Sistema de Control y Vigilancia.

2.4.3.1. Equipo de Dirección

2.4.3.1.1. Gerente de Proyectos.

El Gerente de Proyectos tiene a su cargo la planificación, dirección y coordinación del proyecto en todos sus aspectos, definiendo y concretando los objetivos, identificando las actividades a realizar, los recursos técnicos y de personal, los plazos y los costos requeridos para la ejecución del mismo. Se encargará de mantener permanente contacto con las Directivas de la Entidad, el Supervisor del Sistema y demás personal que se requiera durante la ejecución del proyecto, y tomará las medidas preventivas y correctivas pertinentes para contrarrestar los riesgos que se detecten.

Se requerirá 1 (un) profesional en Ingeniería de Sistemas, Industrial, Electrónica o carreras afines, con posgrado en Gerencia de Proyectos o Maestría en Ingeniería de Sistemas o con certificación de PMP y experiencia certificada en la Dirección de Proyectos en los últimos dos (2) años. Con el fin de asegurar la idoneidad y estabilidad del equipo de

trabajo se deberá adjuntar copia de título profesional, matrícula profesional vigente, certificaciones y demostrar que tienen algún tipo de contrato con el aspirante a proveedor.

2.4.3.2. Equipo de Trabajo de Seguridad

Los aspirantes a proveedor deberán contar con los perfiles solicitados en los numerales subsiguientes y, en caso de subcontratar el servicio de SOC, se deberá anexar el contrato con la empresa que presta el servicio y las hojas de vida del personal solicitado.

2.4.3.2.1. Gerente de SOC.

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

1 (un) profesional en Ingeniería de Sistemas, Industrial, Electrónica o carreras afines, con especialización o Maestría en Seguridad Informática o certificación como Auditor Interno de ISO- 27001. Con el fin de asegurar la idoneidad y estabilidad del equipo de trabajo se deberá adjuntar copia de título profesional, matrícula profesional vigente, certificaciones y demostrar que tienen algún tipo de contrato con el aspirante a proveedor.

2.4.3.2.2. Oficial de Seguridad.

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

1 (un) profesional en Ingeniería de Sistemas, Industrial, Electrónica o carreras afines, con especialización o Maestría en Seguridad Informática o certificado como CISSP o CISM. Con el fin de asegurar la idoneidad y estabilidad del equipo de trabajo se deberá adjuntar copia de título profesional, matrícula profesional vigente, certificaciones y demostrar que tienen algún tipo de contrato con el aspirante a proveedor.

.

2.4.3.2.3. Especialista DBA.

El Especialista es el encargado de establecer las políticas de acceso a las Bases de Datos y monitorear los eventos presentados en tiempo real, esta tarea la podrá realizar a través de herramientas de monitoreo activo de bases de datos o través de la activación y monitoreo de los logs de las bases de datos.

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

2.4.3.2.4. Especialista en Ethical Hacking.

Tiene a su cargo adelantar las actividades tendientes a detectar las debilidades y vulnerabilidades en los sistemas, utilizando para ello, el mismo conocimiento y herramientas de un hacker malicioso, con el fin de generar las herramientas de prevención que requiere el sistema.
Se requerirá 1 (un) profesional en Ingeniería de Sistemas, Industrial, Electrónica o carreras afines, certificado como CEH y/o CISSP, o contrato con una compañía para la prestación de Servicios de Ethical Hacking que tenga personal certificado como CEH y/o CISSP. Con

el fin de asegurar la idoneidad y estabilidad del equipo de trabajo se deberá adjuntar copia de título profesional, matrícula profesional vigente, certificaciones y demostrar que tienen algún tipo de contrato con el aspirante a proveedor o con la compañía contratada para la prestación de servicios de Ethical Hacking.

2.4.3.3. Equipo de Trabajo de Desarrollo.

2.4.3.3.1. Gerente de Operaciones.

El Gerente de Operaciones tiene a su cargo el diseño, la planificación, dirección y coordinación del desarrollo, pruebas, integraciones y la operación de una solución tecnológica, sistema o Software de Gestión.

Se requerirá un (1) profesional en ingeniería de sistemas, industrial, electrónica, de redes o afines, con posgrado o certificación en ITIL o COBIT, con experiencia laboral como gerente, líder o coordinador en los últimos dos (2) años. Con el fin de asegurar la idoneidad y estabilidad del equipo de trabajo se deberá adjuntar copia de título profesional, matrícula profesional vigente, certificaciones y demostrar que tienen algún tipo de contrato con el aspirante a proveedor.

2.4.3.3.2. Gerente de Desarrollo

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

Se requerirá un (1) profesional en ingeniería de sistemas, electrónica, de redes o afines, con Posgrado en Arquitectura, Construcción o Ingeniería de Software y experiencia laboral certificada como Líder, Coordinador o Gerente de Desarrollo en los últimos dos (2) años. Con el fin debe asegurar la idoneidad y estabilidad del equipo de trabajo se deberá adjuntar copia de título profesional, matrícula profesional vigente y demostrar que tienen algún tipo de contrato con el aspirante a proveedor. Con el fin de asegurar la idoneidad y estabilidad del equipo de trabajo se deberá adjuntar copia de título profesional, matrícula profesional vigente, certificaciones y demostrar que tienen algún tipo de contrato con el aspirante a proveedor.

2.4.3.3.3. Ingenieros o tecnólogos de desarrollo.

Se hace necesario para la integración de los diferentes componentes del Sistema de Control y Vigilancia para los CEA Y CIA, una aplicación o software.
Se requerirá que los aspirantes a proveedores del Sistema de Control y Vigilancia cuenten con:

Dos (2) profesionales en Ingeniería de Sistemas o Tecnólogo en Sistemas con certificación en los lenguajes de programación o experiencia laboral certificada en los últimos tres (3) años donde se encuentran construida la aplicación presentada. Con experiencia laboral certificada en los últimos dos (2) años.

Con el fin de asegurar la idoneidad y estabilidad del equipo de trabajo se deberá adjuntar copia de título profesional, matrícula profesional vigente y demostrar que tienen algún tipo de contrato con el aspirante a proveedor.

En caso que el desarrollo sea de una fábrica de software deberá tener un contrato con dicha fábrica y las licencias de uso.

2.4.3.4. Equipo de trabajo de soporte.

Este equipo de soporte deberá ser el personal necesario para dar cumplimiento a la disponibilidad y continuidad de negocio, deberá estar entrenado para los diferentes casos de uso y niveles de soporte.

2.4.3.4.1. Coordinador de Soporte.

El equipo de soporte requerido será mínimo un profesional en ingeniería de sistemas, industrial, electrónica o carreras afines con posgrado o certificación en ITIL al momento de presentarse al proceso de evaluación de homologación. Con el fin de asegurar la idoneidad y estabilidad del equipo de trabajo se deberá adjuntar copia de título profesional, Matrícula Profesional Vigente, certificaciones y demostrar que tienen algún tipo de contrato con el aspirante a proveedor, además deberá demostrar experiencia como líder de soporte.

2.4.3.4.2. Personal de soporte.

Se requerirá mínimo de dos (2) profesionales en ingeniería de sistemas, electrónica o redes.
Se requerirá mínimo de cuatro (4) Técnicos de soporte. Técnicos, tecnólogos o ingenieros de sistemas, electrónica, redes, telecomunicaciones o afines.

Posteriormente en entrada a operación el personal técnico necesario para cumplir con los ANS (ACUERDO DE NIVELES DE SERVICIO) solicitados de acuerdo al número de CEA Y CIA´s contratados.

2.4.3.5. Mesa de Ayuda.

Como un conjunto de recursos tecnológicos y humanos, 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 o recurso humano encargado de Mesa de Ayuda (MDA) debe proporcionar respuestas y soluciones a los usuarios finales, clientes o beneficiarios (destinatarios del servicio), y también puede otorgar asesoramiento en relación con una organización o institución, productos y servicios. Generalmente, el propósito de MDA es solucionar problemas o para orientar acerca de computadoras, equipos electrónicos o software. El aspirante a proveedor a homologación debe entregar el esquema de atención de la mesa de ayuda firmado por un Ingeniero con ITIL intermedio o superior, quien avale que los procesos de mesa de ayuda han sido diseñados basados en las mejores prácticas de ITIL.
Al entrar en operación, el equipo de mesa de ayuda será el necesario para el cumplimiento de los ANS (ACUERDO DE NIVELES DE SERVICIO) solicitados conforme al número de CEA Y CIA´s contratados.

El aspirante a proveedor aportará el equipo de trabajo exigible para este proceso de evaluación a través de los siguientes pasos: a) mediante el diligenciamiento del Formato Modelo de Equipo de Trabajo Exigible a la compañía, numeral 2.4.3.7.; y, b) mediante la presentación adicional de: Copia de título profesional, título de postgrado, certificaciones, experiencia comprobada y certificada, contrato laboral directo con el aspirante a proveedor y copia de la planilla del último mes en donde se evidencie el pago de los parafiscales de todos los profesionales. En caso de subcontratar el servicio de SOC,

se deberá anexar el contrato con la empresa que presta el servicio y las hojas de vida del personal solicitado, quienes igualmente deben cumplir con los Requerimientos exigidos.

2.4.3.6. Especificaciones de la entrega del documento.

- ✓ Cada Formato Modelo de Equipo de trabajo exigible a la compañía, deberá estar diligenciado y también firmado con huella legible por el Representante Legal del aspirante a proveedor debidamente autenticado en Notaría con firma y huella.
- ✓ Deberá aportar para cada perfil: Cargo, copia de título profesional, título de postgrado, certificaciones, experiencia comprobada y certificada, contrato laboral directo con el aspirante a proveedor y copia de la planilla del último mes en donde se evidencie el pago de los parafiscales de todos los profesionales.
- ✓ En caso de subcontratar el servicio de SOC, se deberá anexar el contrato vigente con la empresa que presta el servicio y las hojas de vida del personal solicitado.

2.4.3.7. Modelo de Certificaciones Exigibles a la compañía del aspirante:

MODELO DE CERTIFICACIONES EXIGIBLES A LA COMPAÑÍA DEL ASPIRANTE	
NOMBRE O RAZÓN SOCIAL DE LA COMPAÑÍA DEL ASPIRANTE	
NIT DE LA COMPAÑÍA DEL ASPIRANTE	
NOMBRES Y APELLIDOS DEL REPRESENTANTE LEGAL DE LA COMPAÑÍA DEL ASPIRANTE	
Equipo de Dirección Gerente de Proyectos.(1)	Título profesional en: (especifique el título de grado) ☐ ingeniería de sistemas, ☐ industrial, ☐ electrónica ☐ carreras afines Posgrado o certificación : (especifique el título de posgrado) ☐ En gerencia de proyectos ☐ Maestría en ingeniería de sistemas
	☐ Certificación de PMP Experiencia: ☐ Dirección de proyectos en los últimos 3 años. Tipo de Contrato: (especifique el tipo de contrato) ☐ Pago de Aportes Parafiscales: (Especifique el o los números de folio donde aporta la planilla con dicho pago)
Equipo de trabajo de seguridad Gerente de SOC.(1)	Título profesional en: (especifique el título de grado) ☐ ingeniería de sistemas, ☐ industrial, ☐ electrónica ☐ carreras afines Posgrado o certificación : (especifique el título de posgrado) ☐ En seguridad informática ☐ Certificación Auditor Interno ISO-27001 Tipo de Contrato: (especifique el tipo de contrato) ☐ Pago de Aportes Parafiscales: (Especifique el o los números de

Equipo de trabajo de seguridad Oficial de Seguridad. (1)	Título profesional en: (especifique el título de grado) ☐ ingeniería de sistemas, ☐ industrial, ☐ electrónica ☐ carreras afines Posgrado o certificación : (especifique el título de posgrado) ☐ En seguridad informática ☐ certificado como CISSP ☐ certificado como CISM Tipo de Contrato: (especifique el tipo de contrato)
Equipo de trabajo de seguridad Especialista DBA. (1)	Título profesional en: (especifique el título de grado) ☐ ingeniería de sistemas, ☐ industrial, ☐ electrónica ☐ carreras afines Certificación técnica: (especifique el fabricante de la Base de Datos) ☐ DBA Tipo de Contrato: (especifique el tipo de contrato) ☐ Pago de Aportes Parafiscales: (Especifique el o los números de folio donde aporta la planilla con dicho pago)
Equipo de trabajo de seguridad Especialista en Ethical Hacking.(1)	Título profesional en: (especifique el título de grado) ☐ ingeniería de sistemas, ☐ industrial, ☐ electrónica ☐ carreras afines Certificación técnica: ☐ CEH y/o CISSP (Adjuntar y especificar Folio) ☐ Contrato con una compañía para la prestación de Servicios de Ethical Hacking. Tipo de Contrato: (especifique el tipo de contrato)
Equipo de trabajo de desarrollo	Título profesional en: (especifique el título de grado)
Gerente de Operaciones	☐ ingenieria de sistemas, ☐ industrial, ☐ electrónica ☐ carreras afines Posgrado o certificación : (especifique el título de posgrado) ☐ ITIL ☐ COBIT Experiencia: ☐ Experiencia como Arquitecto de Software o Gerente de Proyectos en los últimos dos (2) años Tipo de Contrato: (especifique el tipo de contrato) ☐ Pago de Aportes Parafiscales: (Especifique el o los números de folio donde aporta la planilla con dicho pago)
Equipo de Desarrollo Gerente de Desarrollo	Título profesional en: (especifique el título de grado) ☐ ingeniería de sistemas, ☐ electrónica☐ Posgrado: ☐ Arquitectura de Software ☐ Construcción de Software ☐ Ingeniería de Software Experiencia: ☐ Experiencia como Líder, Coordinador o Gerente de Desarrollo en los últimos dos (2) años Tipo de Contrato: (especifique el tipo de contrato) ☐ Pago de Aportes Parafiscales: (Especifique el o los números de folio donde aporta la planilla con dicho pago)

Equipo de trabajo de desarrollo **Ingenieros o tecnólogos de desarrollo. (2 mínimo)**	Título en: (especifique el título de grado) ☐ ingeniería de sistemas - (Especifique Cantidad) ☐ Tecnólogo de Sistemas - (Especifique Cantidad) Posgrado y certificación en: (especifique el título de posgrado) ☐ Construcción de Software ☐ Arquitectura Empresarial de Software ☐ ITIL Foundation versión 3 o superior Certificación técnica o laboral: (especifique el lenguaje de desarrollo en que se encuentra construida la aplicación) ☐ Aplica (deberá adjuntar las respectivas certificaciones) ☐ No aplica Contrato con una fábrica de software: (especifique el contrato con dicha fábrica, licencias de uso) ☐ Aplica (deberá adjuntar el contrato, licencias de uso y certificaciones del personal de la fábrica de software) ☐ No aplica Tipo de Contrato: (especifique el tipo de contrato) ☐ Pago de Aportes Parafiscales: (Especifique el o los números de folio donde aporta la planilla con dicho pago)
Equipo de trabajo de soporte **Coordinador de Soporte. (1)**	Título profesional en: (especifique el título de grado) ☐ ingeniería de sistemas, ☐ industrial, ☐ electrónica ☐ carreras afines Experiencia:
	☐ Experiencia como Líder de Soporte: (especifique el o los números de folio donde aporta la experiencia) Tipo de Contrato: (especifique el tipo de contrato) ☐ Pago de Aportes Parafiscales: (especifique el o los números de folio donde aporta la planilla con dicho pago)
Equipo de trabajo de soporte **Personal de Soporte.** **Ingenieros (2 mínimo)** **Técnicos, tecnólogos o ingenieros (4 mínimo)**	Título profesional en: (especifique cantidad) ☐ ingeniería de sistemas, ☐ industrial, ☐ electrónica ☐ carreras afines Técnicos, Tecnólogos o Ingenieros TTI(especifique cantidad) ☐ TTI 1 ☐ TTI 2 ☐ TTI 3 ☐ TTI 4
Mesa de Ayuda	☐ Esquema de atención de la mesa de ayuda firmado por un Ingeniero con ITIL intermedio o superior, quien avale que los procesos de mesa de ayuda han sido diseñados basados en las mejores prácticas de ITIL. (especifique el o los números de folio donde aporta la experiencia)

Firma y Huella Representante Legal del Aspirante

2.4.4. Aliado u Operador de Recaudo.

El aspirante a proveedor del Sistema de Control y Vigilancia deberá contar con uno o más aliados u operadores de recaudo que deberán cumplir con los siguientes requerimientos:

1. Acreditar experiencia mediante certificación firmada por los clientes en por lo menos un proyecto donde se haya efectuado integración con los sistemas transaccionales de cualquier sector productivo en los últimos tres (3) años.

2. Ser un miembro del Sistema Financiero Colombiano (en el caso de los bancos deberá ser calificado como de bajo riesgo), u operador postal de pago habilitado o autorizado en Colombia y que tenga convenio para este proyecto por lo menos con una entidad financiera vigilada por la Superintendencia Financiera de Colombia.

3. El aliado de recaudo deberá generar un número de identificación único de pago (PIN) a través de un proceso seguro, que se realiza a través de un algoritmo que concatena diferentes campos de información de una transacción, que finalmente se construye con un consecutivo secuencial, único e irrepetible de forma segura y deberá cumplir además con los siguientes criterios:

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

– Actualización en línea de lo recaudado.

– Debe estar constituido un esquema de replicación en línea de los datos.

– Deberá emitir o generar comprobantes de recaudo, con posibilidades de emitir las copias necesarias.

– Contar con redundancia de un datacenter principal y un datacenter alterno, que garantice la continuidad del servicio.

– Deberá contar con dispositivos de seguridad perimetral en la red.

– Disponer de un canal de atención inmediata para los usuarios y/o clientes (P.Q.R).

– Deberá tener restricción en la manipulación técnica de los equipos de cómputo o terminales en los puntos de recaudo.

– Debe permitir obtener datos del recaudo tales como fecha, hora, remitente, Tipo ID del que compra, Número de ID del que compra, y, con estos datos se genera un algoritmo hash cuyo resultado es un número el cual permite realizar verificaciones para cualquier intento de violación o cambio.

– Debe controlar, validar y llevar trazabilidad de los datos de pago tales como: número único de registro o número único de identificación de pago o compra, el valor del pago, el estado (pago o utilizado), fecha del uso del servicio, hora del uso del servicio, número único de uso, entre otros.

– Deberá presentar procedimiento que evite que traten de falsificar comprobantes de recaudo.

4. A través de él o los aliados de recaudo, el aspirante a proveedor deberá garantizar puntos de atención en todos los municipios del país donde se encuentren los Centros de Enseñanza Automovilística y Centros de Integrales de Atención y deberá estar en la disposición de habilitar nuevos puntos de atención cuando queden puntos muy distantes de los CEAS y CIAS.

5. El o los aliados de Recaudo, deberán generar una póliza de cumplimiento a favor de cada Centro de Enseñanza Automovilística/Centros Integrales de Atención y del homologado por el buen manejo del dinero recaudado.

6. El o los aliados de recaudo, deberán brindar diferentes medios de pago como pueden ser: pagos a través de Internet, datafonos, dispositivos satélites ubicados en los CEAS y CIAS, entre otros.

7. El o los aliados de recaudo deberán suscribir un documento de compromiso mediante el cual se obligan a cumplir con niveles de servicios del 99%, en los periodos de atención de los CEAS y CIAS.

8. El aliado de recaudo deberá contar con certificación de calidad.

9. Una vez la Superintendencia Financiera lo exija a sus vigilados, el o los aliados de recaudo deberán contar con alguna de las siguientes certificaciones: ISO 27001, PCI DSS 2.0.

10. El recaudo del pago de la tarifa que adopte en Centro de Enseñanza Automovilística para cada curso de conducción en función de la categoría y tipo de trámite será realizada a través del aliado de recaudo aun cuando dicha tarifa sea diferida en varios pagos, de común acuerdo entre el CEA y el aspirante/solicitante, quien asumirá el costo de cada transacción que genere un número de identificación único de pago (PIN).

En cualquier momento, el aspirante a proveedor o el proveedor autorizado de los Sistemas de Control y Vigilancia de los Centros de Enseñanza Automovilística/Centros Integrales de Atención, podrá solicitar la ampliación del número de aliados de recaudo, cumpliendo con los requisitos antes señalados.

2.4.4.1 COBERTURA Y NIVELES DE SERVICIO

El aliado de recaudo deberá cumplir con lo siguiente:

- Contar con puntos de atención propios o en convenio con otras entidades que cumplan los requerimientos aquí establecidos, en todos los municipios del país donde se encuentren los Centros de enseñanza Automovilística y Centros Integrales de Atención.
- El aliado de recaudo deberá brindar diferentes medios de pago como pueden ser: pagos a través de Internet, datafonos o dispositivos satélites.

2.4.4.2 COMPROMISOS POSTERIORES

- El aliado de Recaudo deberá generar y entregar un oficio a la Superintendencia de Puertos y Transporte comprometiéndose generar una póliza de cumplimiento a favor de cada Centro de Enseñanza Automovilística/Centros Integrales de Atención y del homologado por el buen manejo del dinero recaudado y niveles de servicios del 99% en los periodos de atención de los CEAS y CIAS.
- El operador del recaudo deberá estar integrado con el Sistema de Control y Vigilancia para la consulta, validación y consumo de los Pines y la publicación para la Superintendencia de Puertos y Transporte de:
  - ✓ Pines consumidos por los distintos CEAs y CIAs identificando el número de pin, valor del pago, CEAs y CIAs donde fue consumido el PIN, datos del usuario, fecha y hora.
  - ✓ Pines devueltos y/o Pines no consumidos en un periodo superior a siete (7) días calendario.

2.4.5 Operador Tecnológico del Servicio para la Autenticación Biométrica de la Registraduría Nacional del Estado Civil (RNEC)

El aspirante a proveedor deberá contar con un operador del servicio para autenticación biométrica de las huellas dactilares que cumpla con todos los requerimientos y evaluaciones exigidos por la Registraduria Nacional del Estado Civil RNEC y habilitado por esta. El operador debe cumplir con los siguientes requerimientos:

- ✓ Acreditar cumplimiento de Requerimientos con la RNEC.
- ✓ Deberá tener Infraestructura Tecnológica aprobada, desplegada, auditada por la RNEC y en producción realizando consultas permanentes para por lo menos una entidad pública o con funciones públicas del servicio de Validación de Identidad contra las bases de datos de identificación ciudadana (Biometría), manejando el

estándar ISO 19794-2, conforme a lo dispuesto en la Resolución 3341 del 2013 de la RNEC, su anexo y la normatividad vigente.

- ✓ La validación de identidad biométrica deberá tener características de firma electrónica con validez jurídica y probatoria según el Decreto 2364 de 2012, asegurando la autenticidad, integridad y no repudio de la transacción usando los mecanismos previstos por la ley 527 de 1999.
- ✓ El operador del servicio que cumpla con los anteriores requerimientos deberá establecer un convenio con la Superintendencia de Puertos y Transporte para presentarse como Operador Biométrico Homologado.

2.5. LISTA DE REQUERIMIENTOS FINANCIEROS.

Los Requerimientos Financieros buscan establecer unas mínimas condiciones que reflejan la salud financiera de los proponentes a través de su liquidez y endeudamiento. Estas condiciones muestran la aptitud del aspirante a proveedor para cumplir oportuna y cabalmente el objeto del contrato.

La capacidad financiera requerida en cualquier proceso debe ser adecuada y proporcional a la naturaleza y al valor. En consecuencia, la Entidad Estatal debe establecer los Requerimientos de capacidad financiera con base en su conocimiento del sector relativo al objeto de Proceso Contratación y de los posibles oferentes.

En atención a la naturaleza del contrato a suscribir y de su valor, plazo y forma de pago, la Entidad Estatal debe hacer uso de los indicadores que considere adecuados respecto al objeto del Proceso.

Las Entidades Estatales no deben limitarse a determinar y aplicar de forma mecánica fórmulas financieras para determinar los indicadores. Deben conocer cada indicador, sus fórmulas de cálculo y su interpretación.

Los indicadores de capacidad financiera contenidos en el artículo 10 del Decreto 1510 de 2013 son:

Índice de Liquidez = Activo Corriente / Pasivo Corriente, el cual determina la capacidad que tiene un aspirante a proveedor para cumplir con sus obligaciones de corto plazo. A mayor índice de liquidez, menor es la probabilidad de que el aspirante incumpla sus obligaciones de corto plazo.

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

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

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

Indicador	Si el indicador es mayor, la probabilidad de Riesgo es	Límite
Índice de liquidez	Menor	Mínimo
Índice de Endeudamiento	Mayor	Máximo

Entidades Estatales pueden establecer indicadores adicionales a los establecidos en el numeral 3 del artículo 10 del Decreto 1510 de 2013, solo en aquellos casos en que sea necesario por las características del objeto a contratar, la naturaleza o complejidad del Proceso de Contratación. Es importante tener en cuenta que los indicadores pueden ser índices como en el caso del índice de liquidez (activo corriente dividido por el pasivo corriente) o valores absolutos como el capital de trabajo y el patrimonio.

La siguiente tabla presenta algunos indicadores adicionales de capacidad financiera:

Indicador	Fórmula	Observaciones
Capital de Trabajo	Activo corriente - Pasivo Corriente	Este indicador representa la liquidez operativa del proponente, es decir el remanente del proponente luego de liquidar sus activos corrientes convertidos en efectivo) y pagar el pasivo de corto plazo. Un capital de trabajo positivo contribuye con el desarrollo eficiente de la actividad económica del proponente. Es recomendable su uso cuando la Entidad Estatal requiere analizar el nivel de liquidez en términos absolutos.
Razón de efectivo	Efectivo / Pasivo Corriente	El efectivo es el activo con mayor grado de liquidez que tiene un proponente. La razón de efectivo considera la relación entre la disposición inmediata de recursos y las obligaciones de corto plazo. Es recomendable su uso cuando la liquidez es un factor primordial para lograr con éxito el objeto del Proceso de Contratación.
Prueba ácida	(Activo Corriente - Inventarios) / Pasivo Corriente	Mide la liquidez del proponente de manera más estricta que el índice de liquidez pues no tiene en cuenta su inventario. El inventario es excluido teniendo en cuenta que es la cuenta menos líquida del activo corriente y no debe ser usada para pagar las obligaciones de corto plazo.
Concentración de endeudamiento a corto plazo	Pasivo Corriente / Pasivo Total	Mide la proporción de la deuda del proponente a corto plazo (menor a 1 año) sobre la totalidad de su deuda. Es recomendable incluir este indicador cuando exista un Riesgo asociado al no pago de la deuda de corto plazo, por lo cual un alto nivel de endeudamiento de corto plazo puede afectar la habilidad del proponente para cumplir con el objeto del contrato.
Concentración de endeudamiento a largo plazo	Pasivo no Corriente / Pasivo Total	Mide la proporción de la deuda del proponente a largo plazo (mayor a 1 año) sobre la totalidad de su deuda. Es recomendable incluir este indicador cuando: (i) exista un Riesgo asociado al no pago de la deuda de largo plazo, por lo cual un alto nivel de endeudamiento de largo plazo puede afectar la habilidad del proponente para cumplir con el objeto del contrato; y (ii) el término del contrato es mayor a 1 año.
Patrimonio	Activo Total - Pasivo Total	Mide la cantidad de recursos propios del proponente. Es recomendable su uso cuando la Entidad Estatal requiere analizar la cantidad de recursos propios en términos absolutos cuando el presupuesto del Proceso de Contratación es muy alto y la Entidad Estatal debe asegurar la continuidad del proponente en el tiempo.

El aspirante a proveedor deberá presentar los siguientes Estados Financieros dictaminados de la Sociedad:

a) Balance General, Estado de Resultados y las Notas a los Estados Financieros, con corte al 31 de Diciembre del año inmediatamente anterior a la presentación de la propuesta ante la Superintendencia de Puertos y Transporte, aprobados por el órgano competente, debidamente certificados y dictaminados (Decreto 2649 de 1993, Ley 222 de 1995 y Decreto 1406 de 1999).
El artículo 37 de la Ley 222 de 1995 y la circular externa N° 037 de 2001 de la Junta Central de Contadores establece en relación con los estados financieros certificados que: "El representante legal y el contador público bajo cuya responsabilidad se hubiesen preparado los estados financieros deberán certificar aquellos que se pongan a disposición de los asociados o terceros. La certificación consiste en declarar que se han verificado previamente las afirmaciones contenidas en ellos, conforme al reglamento y que las mismas se han tomado fielmente de los libros".
Así mismo, los balances estarán discriminados de la siguiente manera:
ACTIVOS: Corriente, no corriente y total
PASIVOS: Corriente, no corriente, total y
PATRIMONIO
Cuando la Entidad en desarrollo de la verificación financiera requiera confirmar

información adicional del aspirante, podrá solicitar los documentos que considere necesarios para el esclarecimiento de la información, tales como, estados financieros de años anteriores, anexos específicos o cualquier otro soporte. Así mismo, requerirá las aclaraciones que considere necesarias, siempre que con ello no se violen los principios de igualdad y transparencia de la contratación, sin que las aclaraciones o documentos que el aspirante allegue a la solicitud de la Superintendencia de Puertos y Transporte (o a quien esta delegue) puedan modificar, adicionar o complementar la propuesta.

Para efectos del dictamen de los estados financieros, se tendrá en cuenta lo dispuesto en el artículo 38 de la Ley 222 de 1995 que indica: "Son dictaminados aquellos estados financieros certificados que se acompañen de la opinión profesional del revisor fiscal o, a falta de éste, del contador público independiente que los hubiere examinado de conformidad con las normas de auditoría generalmente aceptadas. Estos estados deben ser suscritos por dicho profesional, anteponiendo la expresión "ver la opinión adjunta" u otra similar. El sentido y alcance de su firma será el que se indique en el dictamen correspondiente. Cuando los estados financieros se presenten conjuntamente con el informe de gestión de los administradores, el revisor fiscal o contador público independiente deberá incluir en su informe su opinión sobre si entre aquéllos y éstos existe la debida concordancia". En consecuencia entiéndase que quien certifica los estados financieros no puede dictaminar los mismos. Solo se aceptará "dictamen limpio", entendiéndose por éste, aquel en el que se declara que los estados financieros presentan razonablemente en todos los aspectos significativos, la situación financiera, los cambios en el patrimonio, los resultados de operaciones y los cambios en la situación financiera de la entidad, de conformidad con los principios de contabilidad generalmente aceptados.

b) Fotocopia de la tarjeta profesional del contador, revisor fiscal o contador independiente, según corresponda.
c) Certificación expedida por la Junta Central de Contadores, la cual no será anterior a tres (3) meses de la fecha de presentación de la oferta, del contador, revisor fiscal o contador independiente, según corresponda.

Los aspirantes a proveedor deberán presentar los estados financieros dictaminados a corte 31 de diciembre del año inmediatamente anterior. Para los años subsiguientes.

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

Se considerará habilitado financieramente el aspirante que cumpla con los siguientes indicadores:

INDICADORES	CONCEPTO	REQUISITO
CAPITAL REAL	CAPITAL SOCIAL, RESERVAS CONSTITUIDAS, UTILIDADES RETENIDAS, UTILIDADES DEL EJERCICIO	> $2.500.000.000
LIQUIDEZ	ACTIVO CORRIENTE / PASIVO CORRIENTE	>= 1,0
NIVEL DE ENDEUDAMIENTO	PASIVO TOTAL/ACTIVO TOTAL	<= al 60%

CAPITAL DE TRABAJO	ACTIVO CORRIENTE - PASIVO CORRIENTE	> $2.000.000.000
DE RIESGO	ACTIVO FIJO / PATRIMONIO NETO	< 0,8

En caso de participar en Unión Temporal o Consorcio, al menos uno de los miembros que lo conforman, deberá cumplir con los indicadores financieros.

2.6. LISTA DE REQUERIMIENTOS TÉCNICOS

Este documento establece los requerimientos técnicos mínimos que deben ser cumplidos por el aspirante a proveedor para garantizar la operación del Sistema de Control y Vigilancia para los CEA y CIA en sus diferentes componentes (Centro de Procesamiento de Datos, Centro de Operaciones de Seguridad, Mesa de Ayuda, Red de Comunicaciones, Software de Gestión y Sistema de Gestión de Calidad) y de la información de cada una de las transacciones en tiempo real en el momento que se realicen en cualquiera de los equipos de cómputo de los CEA Y CIA conectados al Sistema, así como la generación, procesamiento y transmisión de la información requerida.

La determinación de los Requerimientos y condiciones, por su condición fundamentalmente tecnológica, pueden estar sujetas a cambios como consecuencia del desarrollo de la tecnología. Para la elaboración de este documento, se ha tenido en cuenta la información en materia de normas, estándares y reglamentaciones técnicas Internacionales, en caso que alguna de estas normas técnicas internacionales quedara en desuso, se debe utilizar cualquier otra norma que la reemplace.

La plataforma tecnológica (hardware, software, comunicaciones, bases de datos, etc.) necesaria para el control, seguimiento y auditoría por parte de la Supertransporte de las formaciones y evaluaciones de aptitud para conducir por los CEA, y de asistencia a las horas de capacitación en las CEA que deberá ser provista, instalada y puesta en operación por el Operador, requiere cumplir como mínimo con lo siguiente:

- Centro de Procesamiento de Datos (CPD). Ubicación donde se concentran los recursos e infraestructura necesarios para el alojamiento y funcionamiento del Sistema.
- Centro de Operaciones de Seguridad (SOC). Se compone de personas, procesos, infraestructura y tecnología dedicados a gestionar, tanto de forma reactiva como proactiva, amenazas, vulnerabilidades y en general incidentes de seguridad de la información, con el objetivo de minimizar y controlar el impacto en la organización.
- Mesa de Ayuda (Help Desk). es un conjunto de recursos tecnológicos y humanos, 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 o recurso humano encargado de Mesa de Ayuda (MDA) debe proporcionar respuestas y soluciones a los usuarios finales, clientes o beneficiarios (destinatarios del servicio), y también puede otorgar asesoramiento en relación con una organización o institución, productos y servicios.
- Red de Comunicaciones. Infraestructura necesaria para interconectar todos los elementos del Sistema de Control y Vigilancia y los Centros de Enseñanza Automovilística y/o Centros Integral de Atención y con la Superintendencia de Puertos y Transporte (interface).
- Software de Gestión. Cada uno de los proveedores del sistema de seguridad, deberán proveer, A través de esta aplicación (SOFWARE), a

los Centros de Enseñanza Automovilística deberán realizar la formación, evaluación y certificación con los procesos de: registro o enrolamiento de centros, representantes legales, administradores, recepcionistas, instructores, capacitadores; validación del pago; asignación de citas; registro o enrolamiento del aspirante/solicitante; autenticación y validación biométrica dactilar de los aspirantes/solicitantes y de los instructores, capacitadores contra la base de datos de la RNEC; registro y control de la asistencia a los diferentes módulos de formación teórica y práctica, realización de la evaluación teórica en sus diferentes módulos; registro de los avances, y de los puntos a evaluar la aptitud por parte del instructor en campo; el registro y control de la asistencia a los curso de capacitación de infractores. Esta aplicación estará alojada en el CPD e integrada en el SOC, el Aliado de Recaudo y el Operador de Validación Biométrica de la RNEC. Este software de gestión deberá ser aprobado por la Superintendencia de Puertos y Transporte, que lo evaluará integralmente.

- Sistema de Gestión de Calidad. El Software de Gestión, deberá tener una herramienta como instrumento de registro, verificación y control de los actores y sus procesos que se regulan en este acto.

2.6.1. Documentación Técnica

Para todos los casos se deberá aportar por parte del aspirante a proveedor la siguiente documentación técnica:

1. Adjuntar copia del certificado de registro de soporte lógico de la Dirección Nacional de Derechos de Autor. En el caso de que el aspirante utilice una licencia de software de una solución fabricada por otra compañía, el aspirante deberá adjuntar copia de la licencia de uso por parte de la compañía fabricante.
2. Adjuntar copia de la propiedad del aspirante a proveedor, o alguno de los miembros de la Unión Temporal o Consorcio, o autorización del uso, de la patente otorgada de invención o modelo de utilidad de un sistema o estructura, para validar y autenticar información biométrica de usuarios y funcionarios en entidades remotas, expedida por la Superintendencia de Industria y Comercio. Deberá contar en su alcance y/o reivindicaciones con los siguientes elementos estructurales:
   i. Lectores o captores de información biométrica tales como: Lector biométrico de huellas dactilares, con la funcionalidad de detectar dedos vivos y resolución de 500 DPI; cámara digital de alta definición, con profundidad de color a 24 bits, con enfoque automático; entre otros elementos de lectura de información biométrica.
   ii. Lectores o escáneres de información bidimensional que permitan de capturar, decodificar y leer información de las diferentes imágenes integradas en documentos de identificación con códigos de barra de una o dos dimensiones.
   iii. Dispositivos digitalizadores de firmas y lápiz óptico para realizar el registro de firmas manuscritas y que vincule firmas electrónicas.
   iv. Una infraestructura de computo central para el registro, gestión y control de la información con capacidades de almacenamiento escalable, multiprocesamiento de varios núcleos, diferentes tipos de memoria, componentes de entradas y salidas, comunicaciones seguras, identificación y monitoreo a través de la posición geográfica, control de tiempos mínimos y máximos que se deban cumplir en el proceso, un componente de generación de certificados, interoperabilidad con diferentes bases de datos a través de VPN o Redes Privadas virtuales.
   v. Un elemento de comunicaciones con módulos: Ethernet TCP/IP, GPRS, serial, USB, GPS con antena.
   vi. Comunicaciones a través de Redes de seguridad privada (VPN) y que permita

el acceso seguro a múltiples bases de datos.

3. Adjuntar copia de contrato del Centro de Procesamiento de Datos, en caso de que el CPD se encuentre subcontratado. Los contratos deberán tener una duración mínima de veinticuatro (24) meses.
4. Adjuntar relación de equipos identificando marca, modelo, el datasheet y soporte de Gartner o Forester Wave de las soluciones de servidores, IPS, Firewall, Herramienta DAM, Herramienta SIEM, SAN, Escáner de Vulnerabilidades, Application Delivery Controller, licencias de bases de datos, licencias de sistemas operativos. En el caso en el que el Centro de operaciones SOC se encuentre subcontratado, la relación presentada deberá ser del proveedor contratado.

2.6.2. Aspectos Técnicos Generales.

La Plataforma Tecnológica que soporta el proceso de inspección, vigilancia y control de la realización de la formación, evaluación y certificación de aptitud para conducir por parte de los CEA, y la asistencia a las capacitaciones del infractor por parte de los CIA estará a cargo de los operadores homologados. Sus instalaciones y las del sistema de respaldo (sistema espejo), deberán estar ubicadas en la República de Colombia, en un sitio seguro, con controles de acceso y vigilancia, que permita procesos de auditoría sobre la información. Lo compone además de los elementos de hardware requeridos, un conjunto de programas (software) que garantizan la adecuada operación. A su vez, el Sistema de Control y Vigilancia es el encargado del envío de la información solicitada por la Supertransporte en tiempo real.

Los servidores centrales del Sistema de Control y Vigilancia deben tener la capacidad necesaria para garantizar el procesamiento de las operaciones realizadas en los CEA y CIA, con la concurrencia que el mercado demande. Estos servidores deben tener la capacidad de ser expandidos a medida que aumenten y/o cambien las necesidades. El Sistema de Control y Vigilancia debe estar desplegado sobre una infraestructura en alta disponibilidad y contar con un CPD de respaldo para garantizar el Nivel de Servicio conforme el futuro contrato con los CEA y CIA.

El Sistema de Control y Vigilancia deberá tener una infraestructura tecnológica estable que garantice la disponibilidad de la información almacenada en una las bases de datos: información de control, resultados de los eventos, información de los registros o transacciones generadas. Debe tener como mínimo: un arreglo de servidores redundantes, comunicaciones redundantes, un sistema de red de comunicación de datos y una base de datos relacional.

- Registrar todas las transacciones y operaciones realizadas desde los computadores y equipos ubicados en los CEA y CIA y desde los vehículos de los CEA en campo, interconectados al Sistema de Control y Vigilancia: transacciones, eventos, datos de control, así como eventos de funcionamiento del Sistema de Control y Vigilancia;
- Toda transacción debe ser replicada al sistema redundante de respaldo. Se debe de garantizar que el 100 % de las transacciones se encuentran replicadas al momento de requerirse la entrada en operación del sistema de respaldo.
- Registro de todo el proceso de evaluación y certificación en el Software de Gestión;
- Garantizar el correcto funcionamiento de las actividades del Sistema de Control y Vigilancia en el CEA Y CIA;
- Generar los mecanismos de seguridad de la información en línea, a través de alarmas y alertas.
- Con la solicitud presentada ante la Superintendencia, se entiende que el operador conoce que está obligado a generar todos los reportes y cruces de información que sean solicitados por la Superintendencia.

2.6.3. Componentes del Sistema de Control y Vigilancia y sus Requerimientos Técnicos

El sistema técnico y en general el conjunto de sistemas e instrumentos técnicos o telemáticos, que posibiliten el registro, control e inspección; deberá disponer de los mecanismos de autenticación suficientes para garantizar, entre otros, la confidencialidad e integridad en las comunicaciones, validación, autenticidad y cómputo, el control de su correcto funcionamiento y el acceso a los componentes del sistema informático.

Los Operadores, deben disponer del material de software, equipos, sistemas, terminales e instrumentos en general, necesarios para el desarrollo de las actividades de inspección, vigilancia y control; debidamente homologados bajo los requerimientos técnicos y el establecimiento de las especificaciones necesarias para su funcionamiento.

El proceso deberá disponer de los componentes y características que se describen a continuación:

2.6.3.1. Centro de Operaciones de Seguridad SOC.

El cual estará conformado por un grupo de personas, procesos, infraestructura y tecnología dedicados a gestionar, tanto de forma reactiva como proactiva, amenazas, vulnerabilidades y en general incidentes de seguridad de la información, con el objetivo de minimizar y controlar el impacto en la organización.

Para este proceso se necesitará proveer de sistemas Hardware, software, comunicaciones, dispositivos de seguridad, servicios de integración y gestión de proyecto. A continuación se detallan los elementos Hardware y Software necesarios.

2.6.3.1.1. Seguridad Física y Ambiental

La Seguridad Física consiste en la aplicación de barreras físicas y procedimientos de control, como medidas de prevención y contramedidas ante amenazas a los recursos e información confidencial. Se refiere a los controles y mecanismos de seguridad dentro del SOC, así como los medios de acceso remoto al y desde el mismo; implementados para proteger el hardware y medios de almacenamiento de datos. Este tipo de seguridad está enfocado a cubrir las amenazas ocasionadas tanto por el hombre como por la naturaleza del medio físico en que se encuentra ubicado el centro. Las principales amenazas que se prevén en la seguridad física son:

1. Desastres naturales, incendios accidentales.
2. Amenazas ocasionadas por el hombre.
3. Sabotajes internos y externos deliberados.

Se analizarán y evaluarán los peligros más importantes que se corren en un centro de operaciones y monitoreo; con el objetivo de mantener una serie de acciones a seguir en forma eficaz y oportuna para la prevención, reducción, recuperación y corrección de los diferentes tipos de riesgos.

2.6.3.1.2. Control de Accesos:

2.6.3.1.2.1. Sistemas Biométricos.

El centro de operaciones de seguridad deberá contar con un control de acceso biométrico a través de huella dactilar, o de reconocimiento facial, o de verificación de patrones oculares. Se validará que cumplan con los estándares actuales para el acceso biométrico

seleccionado.

2.6.3.1.2.2. Protección electrónica

2.6.3.1.2.2.1.CCTV (Circuito Cerrado de Televisión)

El SOC deberá contar con un sistema de circuito cerrado de televisión, que permita monitorear y registrar las actividades de ingreso y las que se realizan al interior del SOC y el control sobre los elementos activos y pasivos dentro del mismo.

2.6.3.1.2.3. Condiciones Ambientales

2.6.3.1.2.3.1Sistema contra Incendios

Los diversos factores a contemplar y verificar para reducir los riesgos de incendio a los que se encuentra sometido son:

- El SOC debe contar con elementos de detección y extinción de fuego, en relación al grado de riesgo y la clase de fuego que sea posible en ese ámbito.
- No debe estar permitido fumar en el área.
- El SOC debe contar con un esquema de evacuación, y su personal debidamente capacitado ante desastres.
- Seguridad del Equipamiento. Es necesario proteger los equipos de cómputo instalándolos en áreas en las cuales el acceso a los mismos sólo sea para personal autorizado. Además, es necesario que estas áreas cuenten con los mecanismos de ventilación y detección de incendios adecuados. Para protegerlos se debe tener en cuenta que:
- La temperatura no debe sobrepasar los 23°C.
- Deben instalarse extintores manuales (portátiles) y/o automáticos (rociadores).

2.6.3.1.2.3.2 Sistema de Aire Acondicionado.

Se debe proveer un sistema de ventilación y aire acondicionado. Teniendo en cuenta que los aparatos de aire acondicionado son causa potencial de inundaciones, en caso de utilizar sistemas de enfriamiento por agua se verificará que estén instaladas redes de protección en todo el sistema de cañería al interior y al exterior.

2.6.3.1.2.3.3Terremotos.

El SOC deberá contar con un esquema seguridad contra desastres naturales como sismos, terremotos e inundaciones, deberá contar con un esquema de evacuación ante terremoto.

2.6.3.1.2.3.4

Sistema de Alimentación Ininterrumpida (SAI). EL SOC deberá contar con un sistema de corriente regulada en línea y de contingencia que garantice la operatividad en ausencia del sistema de suministro de energía principal por un tiempo mínimo de 4 horas continuas. Se verificará en la visita:

2.6.3.1.3 Seguridad Lógica

2.6.3.1.3.1 Controles de Acceso

2.6.3.1.3.1.1 Identificación y Autenticación

Todos y cada uno de los equipos que se encuentren en el SOC deberán contar con sistemas que permitan definir políticas de protección de acceso a la información, como lo son usuarios y contraseñas.

2.6.3.1.3.2 Roles

Los sistemas instalados deben tener configurados y habilitados los roles de administración y operadores.

2.6.3.1.3.3 Modalidad de Acceso.

Los sistemas instalados deberán contar con medios seguros de acceso remoto para soporte y actualización a los mismos, por medio de VPN y sistemas de encriptación seguros.

2.6.3.1.3.4 Ubicación y horario.
El SOC podrá estar ubicado en el territorio nacional, los costos de traslado y viáticos diferentes a la ciudad de Bogotá serán asumidos por el aspirante a proveedor para su verificación en la visita de evaluación, y con un horario de prestación de servicio igual al horario de atención de los CEA Y CIA's monitoreados.

2.6.3.1.3.5 Administración.
La administración de los sistemas del SOC deberá estar a cargo de personal idóneo, con la experiencia solicitada demostrable. Utilizando herramientas de gestión y monitoreo,
compatibles con los sistemas instalados.

2.6.3.1.3.6 Actualizaciones de sistemas y aplicaciones.
Los sistemas del SOC deberán contar con medios de actualización manual y en línea por internet con la web del fabricante que permita la actualización permanente del mismo y/o aplicación de hotfixes para los mismos en pro de un correcto funcionamiento.

Deberá contar con los siguientes dispositivos:

SOLUCIÓN	REQUISITO MÍNIMO
FIREWALL PERIMETRAL UTM	Solución basada en hardware o software que deberá tener los servicios activos de Firewall, IPS (Intrusion Prevention System), Escáner de Vulnerabilidades de Red y Antivirus de Red. Debe tener como mínimo 1 Gbps de throughput y fuente redundante o alta disponibilidad. La solución utilizada deberá encontrarse en el cuadrante de Leaders, Visionaries o Challengers del Magic Quadrant for Unified Threat Management (UTM).
SIEM	Solución basada en hardware o software para la correlación de eventos de seguridad generados por el equipamiento y aplicaciones de la red de la plataforma tecnológica del Sistema de Control y
	Vigilancia. La solución utilizada deberá encontrarse en el cuadrante de Leaders o Visionaries del Magic Quadrant Security Information and Event
Protección de ENDPOINT	Solución basada en software para protección antimalware de los servidores utilizados del Sistema de Control y Vigilancia. La solución utilizada deberá encontrarse en el cuadrante de Leaders
Web Application Firewall	Solución basada en hardware, debe tener como mínimo funcionalidad de Firewall de Aplicaciones Web, que debe tener fuente redundante o alta disponibilidad. La solución utilizada deberá encontrarse en el Magic Quadrant for Web Application Firewalls de Gartner.

2.6.3.2 Centro de Procesamiento de Datos (CPD)

El Centro de Procesamiento de Datos es aquella ubicación donde se concentran todos los recursos necesarios para el procesamiento de la información del Sistema de Control y Vigilancia. También se conoce como centro de datos o su equivalente en inglés Datacenter. Un CPD, por tanto, es un edificio o sala de gran tamaño usada para mantener en él una gran cantidad de equipamiento electrónico.

Entre los factores más importantes que motivan la creación de un CPD se puede destacar el **garantizar la continuidad y disponibilidad** del servicio a clientes, empleados, ciudadanos, proveedores y empresas colaboradoras, pues en estos ámbitos es muy importante la protección física de los equipos informáticos o de comunicaciones implicados, así como servidores de bases de datos que puedan contener información crítica.

Requerimientos

Generales:

- Disponibilidad y monitorización"24x7x365" un centro de datos diseñado apropiadamente proporcionará disponibilidad, accesibilidad y confianza 24 horas al día, 7 días a la semana, 365 días al año.
- Fiabilidad: Los centros de datos deben tener redes y equipos altamente robustos y comprobados.
- Seguridad, redundancia y diversificación: Almacenaje exterior de datos, tomas de alimentación eléctrica totalmente independientes y de servicios de telecomunicaciones para la misma configuración, equilibrio de cargas, sistemas de alimentación ininterrumpida o SAI, control de acceso, etc.
- Control ambiental / prevención de incendios: El control de ambiente trata de la calidad de aire, temperatura, humedad, inundación, electricidad, control de fuego, y por supuesto, acceso físico.
- Acceso a internet y conectividad a redes de área extensa WAN para conectividad a Internet: Los centros de datos deben ser capaces de hacer frente a las mejoras y avances en los equipos, estándares y anchos de banda requeridos, pero sin dejar de ser manejables y fiables.
- El centro de procesamiento de datos principal deberá estar ubicado en el territorio nacional y el centro de procesamiento de datos redundante podrá estar ubicado en el territorio nacional o extranjero, los costos de traslado y viáticos diferentes a la ciudad de Bogotá serán asumidos por el aspirante a proveedor para su verificación en la visita de evaluación del centro de procesamiento de datos principal.

2.6.3.2.1. Seguridad Física y Ambiental.

La Seguridad Física consiste en la aplicación de barreras físicas y procedimientos de control, como medidas de prevención y contramedidas ante amenazas a los recursos e información confidencial. Se refiere a los controles y mecanismos de seguridad dentro y alrededor del CPD, así como los medios de acceso remoto al y desde el mismo; implementados para proteger el hardware y medios de almacenamiento de datos. Este tipo de seguridad está enfocado a cubrir las amenazas ocasionadas tanto por el hombre como por la naturaleza del medio físico en que se encuentra ubicado el centro. Las principales amenazas que se prevén en la seguridad física son:

1. Desastres naturales, incendios accidentales, tormentas e inundaciones.
2. Amenazas ocasionadas por el hombre.
3. Disturbios, sabotajes internos y externos deliberados.

Se analizarán y evaluarán los peligros más importantes que se corren en un centro de procesamiento; con el objetivo de mantener una serie de acciones a seguir en forma eficaz y oportuna para la prevención, reducción, recuperación y corrección de los diferentes tipos de riesgos.

2.6.3.2.2 Control de Acceso.

Las áreas restringidas como los CPD necesitan una buena gestión de los accesos a la sala. Los sistemas de control de accesos son sistemas creados para la gestión e integración informática de las necesidades de una empresa relacionadas con el control de accesos de sus empleados o de personas ajenas en sus edificios y delegaciones, existen varias

opciones de terminales según el nivel de seguridad necesario (banda magnética, proximidad, teclado/pin y biométrico). Sistemas Biométricos. El centro de operaciones de seguridad deberá contar con un control de acceso biométrico a través de huella dactilar, o de reconocimiento facial, o de verificación de patrones oculares. Se validará que cumplan con los estándares actuales para el acceso biométrico utilizado seleccionado.

2.6.3.2.3 Protección electrónica.

Está basada en el uso de sensores conectados a centrales de alarma que reaccionan ante la emisión de distintas señales. Cuando un sensor detecta un riesgo, informa a la central que procesa la información y responde según proceda.

2.6.3.2.3.1 CCTV (Circuito Cerrado de Televisión).

El centro de operaciones de seguridad deberá contar con un sistema de circuito cerrado de televisión, que permita monitorear y registrar las actividades de ingreso y las que se realizan al interior del CDP y el control sobre los elementos activos y pasivos dentro del mismo. También deberá contar con la posibilidad de interconectarse con el centro de monitorios de actividades de transporte de la Superintendencia.

2.6.3.2.4 Condiciones Ambientales.

En un CPD el mantenimiento de unas condiciones ambientales adecuadas es indispensable para un funcionamiento coherente de los sistemas informáticos, por el cual se deben controlar y mantener factores como la temperatura, humedad, entre otros.

2.6.3.2.4.1 Sistema contra Incendios.

Los diversos factores a contemplar y verificar para reducir los riesgos de incendio a los que se encuentra sometido un centro de cómputos son:

El área en la que se encuentran las computadoras El CPD debe estar en un sitio cuyos elementos local que no sean combustibles o inflamables.

- El local CPD no debe situarse encima, debajo o adyacente a áreas donde se procesen, fabriquen o almacenen materiales inflamables, explosivos, gases tóxicos o sustancias radioactivas.
- Las paredes deben hacerse de materiales incombustibles y extenderse desde el suelo al techo.

Debe construirse un "falso piso" instalado sobre el piso real, con materiales incombustibles y resistentes al fuego.

- No debe estar permitido fumar en el área de proceso.
- Deben emplearse muebles incombustibles, y cestos metálicos para papeles. Deben evitarse los materiales plásticos e inflamables.
- El piso y el techo en el recinto del centro de cómputo y de almacenamiento de los medios magnéticos deben ser impermeables.
- Seguridad del Equipamiento. Es necesario proteger los equipos de cómputo instalándolos en áreas en las cuales el acceso a los mismos sólo sea para personal autorizado. Además, es necesario que estas áreas cuenten con los mecanismos de ventilación y detección de incendios adecuados.
- Para protegerlos se debe tener en cuenta que:
- La temperatura no debe sobrepasar los 18° C y el límite de humedad no debe superar el 65% para evitar el deterioro.
- Los centros de cómputos deben estar provistos de equipo para la extinción de incendios en relación al grado de riesgo y la clase de fuego que sea posible en ese ámbito.
- Deben instalarse extintores manuales (portátiles) y/o automáticos (rociadores).
- Recomendaciones. El personal designado para usar extinguidores de fuego debe ser entrenado en su uso.
- Si hay sistemas de detección de fuego que activan el sistema de extinción, todo

el personal de esa área debe estar entrenado para no interferir con este proceso automático.

- Implementar paredes protectoras de fuego alrededor de las áreas que se desea proteger del incendio que podría originarse en las áreas adyacentes.
- Proteger el sistema contra daños causados por el humo. Este, en particular la clase que es principalmente espeso, negro y de materiales especiales, puede ser muy dañino y requiere una lenta y costosa operación de limpieza.
- Mantener procedimientos planeados para recibir y almacenar abastecimientos de papel

2.6.3.2.4.2 Sistema de Aire Acondicionado.

Se debe proveer un sistema de calefacción, ventilación y aire acondicionado separado, que se dedique al cuarto de computadoras CPD y equipos de proceso de datos en forma exclusiva.

Teniendo en cuenta que los aparatos de aire acondicionado son causa potencial de incendios e inundaciones, en caso de utilizar sistemas de enfriamiento por agua se verificará que estén instaladas redes de protección en todo el sistema de cañería al interior y al exterior, detectores y extinguidores de incendio, monitores y alarmas efectivas.

2.6.3.2.4.3 Inundaciones.

Para evitar este inconveniente se verificará que tengan un plan para tomar las siguientes medidas:

- ✓ Techo impermeable para evitar el paso de agua desde un nivel superior.
- ✓ Puertas acondicionadas para contener el agua que bajase por las escaleras.

2.6.3.2.4.4 Terremotos.

El Centro de Procesamiento de Datos (CPD) y el Centro de Operaciones de Seguridad deberán estar en una edificación antisísmico conforme al estándar actual requerido.

2.6.3.2.5 Sistema de Alimentación Ininterrumpida (SAI).

EL CPD deberá contar con un sistema de corriente regulada en línea y de contingencia que garantice la operatividad en ausencia del sistema de suministro de energía principal del edificio por un tiempo mínimo de 4 horas continuas. Los equipos de sistema de alimentación ininterrumpida deberán ser protección nivel 9 (ON- LINE de DOBLE CONVERSIÓN).

2.6.3.2.6 Red Eléctrica.

Para el desempeño eficiente y seguro de un CPD, se hace necesario contar con una red de distribución eléctrica adecuada. Para los CPD certificados TIER II o superior, se verificará en sitio el cumplimiento de los estándares establecidos.

2.6.3.2.7 Ubicación.

El CPD principal deberá estar ubicado en territorio nacional, el sistema redundante (espejo) podrá estar ubicado en territorio nacional o extranjero, el sistema redundante deberá estar ubicado en un lugar diferente al CPD Principal.

2.6.3.2.8 Consideraciones Generales.

El CPD debe contar con componentes redundantes, menos susceptibles a interrupciones, tanto planeadas como las no planeadas. El CPD debe contar con piso falso, UPS y generadores eléctricos, conectados como mínimo a una sola línea de distribución eléctrica. El diseño del CPD debe ser mínimo (N+1), lo que significa que existe al menos un duplicado de cada componente de la infraestructura.

2.6.3.2.9 Seguridad Lógica.
La Seguridad Lógica consiste en la "aplicación de barreras y procedimientos que resguarden el acceso a los datos y sólo se permita acceder a ellos a las personas autorizadas para hacerlo."

Es importante recalcar que la mayoría de los daños que puede sufrir un centro de cómputos no será sobre los medios físicos sino contra información por él almacenada y procesada.

Así, la Seguridad Física, sólo es una parte del amplio espectro que se debe cubrir para no vivir con una sensación ficticia de seguridad. El activo más importante que se posee es la información, y por lo tanto deben existir técnicas, más allá de la seguridad física, que la aseguren. Estas técnicas las brinda la Seguridad Lógica.
Existe un viejo dicho en la seguridad informática que dicta que "todo lo que no está permitido debe estar prohibido" y esto es lo que debe asegurar la Seguridad Lógica.
Los objetivos que se plantean son:

- ✓ Restringir el acceso a los programas y archivos.
- ✓ Asegurar que los operadores puedan trabajar sin una supervisión minuciosa y no puedan modificar los programas ni los archivos que no correspondan.
- ✓ Asegurar que se estén utilizando los datos, archivos y programas correctos en y por el procedimiento correcto.
- ✓ Que la información transmitida sea recibida sólo por el destinatario al cual ha sido enviada y no a otro.
- ✓ Que la información recibida sea la misma que ha sido transmitida.
- ✓ Que existan sistemas alternativos secundarios de transmisión entre diferentes puntos.
- ✓ Que se disponga de pasos alternativos de emergencia para la transmisión de información.

2.6.3.2.9.1 Controles de Acceso.
Los sistemas de control de acceso son sistemas creados para la gestión e integración informática de las necesidades de una empresa relacionadas con el control de accesos de sus empleados o de personas ajenas en sus edificios y delegaciones, existen varias opciones de terminales según el nivel de seguridad necesario (banda magnética, proximidad, teclado/pin, biométrico).

2.6.3.2.9.2 Identificación y Autenticación.
Todos y cada uno de los equipos que se encuentren en el CPD deberán contar con sistemas que permitan definir políticas de protección de acceso a la información, como lo son usuarios y contraseñas, con periodos de caducidad de contraseña, con combinaciones de complejidad, y de reusó de mínimo las 5 últimas contraseñas utilizadas

2.6.3.2.9.3 Roles.
Los sistemas instalados deben tener configurados y habilitados los roles de administración, operación y operador de backups.

2.6.3.2.9.4 Limitaciones a los servicios.
Estos controles se refieren a las restricciones que dependen de parámetros propios de la utilización de la aplicación o preestablecidos por el administrador del sistema.

2.6.3.2.10 Modalidad de Acceso.
Los sistemas instalados deberán contar con medios seguros de acceso remoto para soporte y actualización a los mismos, por medio de VPN y sistemas de encriptación seguros.

2.6.3.2.11 Ubicación y Horario.
El acceso a determinados recursos del sistema puede estar basado en la ubicación física y/o lógica de los datos o personas. En cuanto a los horarios, este tipo de controles permite limitar el acceso de los usuarios a determinadas horas de día o a determinados días de la semana. De esta forma se mantiene un control más restringido de los usuarios y zonas de ingreso.

2.6.3.2.12 Administración.
La administración de los sistemas del CPD deberá estar a cargo de personal idóneo, con la experiencia solicitada demostrable. Utilizando herramientas de gestión y monitoreo, compatibles con los sistemas instalados.

2.6.3.2.13 Administración del Personal y Usuarios – Organización del personal.
Este proceso debe llevar los siguientes cuatro pasos:

1) Definición de puestos. Debe contemplarse la máxima separación de funciones posibles y el otorgamiento del mínimo permiso de acceso requerido por cada puesto para la ejecución de las tareas asignadas.
2) Determinación de la sensibilidad del puesto.
3) Elección de la persona para cada puesto.
4) Entrenamiento inicial y continuo del empleado.

2.6.3.2.13.1 Actualizaciones de sistemas y aplicaciones.
Los sistemas del CPD deberán contar con medios de actualización manual y en línea por internet con la web del fabricante que permita la actualización permanente del mismo y/o aplicación de hotfixes para los mismos en pro de un correcto funcionamiento.

2.6.3.2.14 Gestión de Almacenamiento de la Información
El Sistema de almacenamiento debe contemplar las siguientes consideraciones:

- Sistema de fuentes de poder n+1.
- El sistema de almacenamiento debe contemplar arreglos de discos en raid 5 con Spare disks, mínimo 1 disco en Spare.
- Doble sistema de conexión con servidor, en iScsi o F.O.
- Se debe considerar un sistema de respaldo de información, con procesos de restauración de la información y sus protecciones correspondientes. Se debe garantizar un respaldo de la información, donde deberá tener una redundancia de la base de datos. Se realizarán pruebas de restauración de datos.
- Debe contemplar interfaz de administración Web, vía Ethernet.
- Debe configurarse alertas sobre eventos de control de espacio en disco, así como monitoreo de los eventos generados por posibles fallas o alarmas del hardware o configuraciones.

Se deben mostrar el procedimiento establecido para el manejo y almacenamiento de la información, donde se pueda constatar:

- Que la documentación del sistema estará protegida contra el acceso no autorizado.
- Que se tienen políticas, procedimientos y controles formales de intercambio de información.
- Se debe mostrar que se cuenta con registro de usuarios, contraseñas y privilegios por cada usuario.
- Se debe demostrar que los equipos cuentan con las respectivas licencias del software utilizado, incluyendo sistema operativo.

- Se debe mostrar que se cuentan con procedimientos para el manejo y almacenamiento de la información con el fin de proteger la integridad de dicha información.
- Se debe demostrar que se cuenta con políticas y procedimiento de análisis del riesgo, disponibilidad e integridad de la información.

2.6.3.2.15 Normatividad en Seguridad LOPD y LSSICE.

El aspirante a proveedor debe garantizar que respeta la confidencialidad y el derecho de habeas data de sus clientes para acceder, conocer, modificar, actualizar, suministrar, rectificar o suprimir la información suministrada, así como para revocar la autorización otorgada para el tratamiento de la misma. Por lo tanto, el ejercicio de sus derechos se deberá realizar de acuerdo con los Requerimientos establecidos en las disposiciones legales

2.6.3.2.16 Auditorías de Seguridad Informática.

El homologado deberá someterse como mínimo a una auditoría en Seguridad Informática al año, por un auditor definido por la Superintendencia que escogerá por convocatoria pública. En la auditoria se validará el sostenimiento del cumplimiento de los Requerimientos técnicos, jurídicos y administrativos, como homologado. Los costos de esta auditoría estarán a cargo del Homologado.

2.6.3.2.17 Otros Requerimientos.

El aspirante a proveedor deberá presentar un documento técnico que permita garantizar la idoneidad del mismo. El documento técnico deberá contar con los siguientes capítulos:

- El aspirante a proveedor debe anexar el esquema de soporte para atención de los ANS (ACUERDO DE NIVELES DE SERVICIO) de la solución completa.
- El aspirante a homologación podrá tener subcontratado el servicio de Centro de Operaciones de Seguridad SOC. En este caso deberá presentar el contrato firmado con el proveedor que le preste el servicio de SOC mínimo por veinticuatro (24) meses y, las hojas de vida del equipo de seguridad podrán ser funcionarios del proveedor de SOC y cumpliendo con la totalidad de Requerimientos administrativos exigidos para el equipo de trabajo. Se aclara que el único responsable ante la Superintendencia por los ANS (ACUERDO DE NIVELES DE SERVICIO) es el homologado y no el SOC contratado.
- En caso de presentar desarrollos propios, se debe adjuntar copia del certificado de registro de soporte lógico de la Dirección Nacional de Derechos de Autor. En el caso de que el aspirante utilice una licencia de software de una solución fabricada por otra compañía, el aspirante deberá adjuntar copia de la respectiva licencia.
- El aspirante a homologación podrá tener subcontratado el servicio de Centro de Procesamiento de Datos (CPD). En este caso deberá presentar el contrato firmado con el proveedor que le preste el servicio de CPD mínimo por veinticuatro (24) meses y cumpliendo con la totalidad de Requerimientos exigidos. Se aclara que el único responsable ante la Superintendencia por los ANS (ACUERDO DE NIVELES DE SERVICIO) es el homologado y no el CPD contratado.
- El proveedor deberá suministrar Hardware, Software, Comunicaciones y Servicios de Integración y Gestión de Proyecto.

2.6.4. SOFTWARE DE GESTIÓN DEL SISTEMA DE CONTROL Y VIGILANCIA

El Software de Gestión del Sistema de Control y Vigilancia, implementado para los Centros Enseñanza Automovilística y para los Centros Integrales de Atención, deberá contar con los siguientes módulos integrados con las funcionalidades que se describen a continuación:

2.6.4.1. Módulo de Agendamiento de Clases, Capacitaciones y Evaluaciones.

El proveedor del Sistema de Control y Vigilancia, deberá disponer de una plataforma web y aplicaciones para celulares inteligentes (Android, IOS), para el agendamiento de clases que deberá permitir al aspirante/solicitante, la búsqueda geográfica de los CEA autorizados a través de un mapa georreferenciado donde pueda indicar la ubicación donde realizar la dicha búsqueda.

El aspirante/solicitante para poder agendar su cita, deberá estar registrado en una CEA autorizada a través del Software de Gestión del Sistema de Control y Vigilancia, y deberá haber comprado un (1) PIN del servicio de enseñanza teórica y práctica para obtener la Certificación de Aptitud para Conducir del CEA donde se encuentre registrado, a través de los aliados de recaudo de los proveedores del Sistema de Control y Vigilancia.

Las plataformas de agendamiento de citas deberán validar antes de asignar una cita la veracidad del PIN y que no haya sido utilizado.

Las plataformas de agendamiento deberán permitir verificar, reprogramar o cambiar las citas de los aspirantes/solicitantes según la política de cada CEA autorizada y la normatividad vigente.

Cuando un aspirante/solicitante se inscriba simultáneamente a dos programas de capacitación en el mismo CEA en un periodo no superior a tres meses desde el momento de la primera inscripción, la plataforma homologará y registrará la asistencia a las clases teóricas y de taller similares para ambos programas, sin necesidad que el aspirante/solicitante repita la capacitación a excepción de las clases específicas de cada programa en los módulos de mecánica básica y técnicas de conducción, sin reducir la intensidad horaria exigida conforme a la normatividad vigente.

2.6.4.2. Módulo de Software del Sistema de Gestión de Conformidad.

Se definirán y validarán las siguientes funcionalidades y requerimientos:

1. Registro del Centro (Nit, Nombre, Matrícula Mercantil, Resolución de Habilitación del Ministerio de Transporte, Certificado de Conformidad vigente y de los vehículos por categoría con su respectivo número de placa marca, clase, línea, servicio, color, modelo, referencia, No. VIN, serial del motor, serial del chasis y SOAT.
2. Registro de todos los Instructores y personal administrativo de los CEA y CIA donde se incluyan: El Tipo de Documento, No. De Documento, Nombres, Apellidos, No. Licencia de Conductor, Categoría de la licencia de conducción, Número de la licencia de Instructor, Categoría de la licencia del instructor, títulos académicos, en los documentos que fuera necesario con su respectiva vigencia.
3. Registro de las revisiones técnico mecánicas RTMyEC de los vehículos de cada CEA, de la fecha de expedición, vigencia, CDA que expide el certificado con su soporte.
4. Además de las funcionalidades incorporadas en los demás módulos.

2.6.4.3. Módulo de Administración.

En este módulo se definirán los Centros de Enseñanza Automovilística y los Centros Integrales de Atención con datos tales como: NIT, Nombre o Razón de la Empresa, sedes habilitadas, ID RUNT, Departamento, Municipio, Zona a la que pertenece, Dirección, Teléfono, correo electrónico, datos del Representante Legal (Tipo ID, No. de ID, Nombres, Apellidos, Registro y Validación de Identidad), Horarios y Cupos de cada Sede y Aula, Vehículos, Resolución de Habilitación del Ministerio de Transporte y de todos los documentos que soportaron la habilitación así como la vigencia de los mismos, documentación con soporte de los Estados Financieros necesarios, al igual que el registro de las diferentes tarifas.

El Software de Gestión además debe permitir: el registro de las certificaciones de conformidad con su vigencia, el ente certificador y el resultado de cada visitas de auditoria, de seguimiento y/o recertificación y la digitalización de los certificados expedidos; el registro de las dimensiones de cada aula y su capacidad, al igual del registro digitalizado de la planimetría de las diferentes aulas de la escuela, capacidad de las aulas, deberán ir en tamaño carta u oficio en resolución de 100dpi, legible.

Registro del área de práctica, detallando su espacio, dirección física y geográfica; georreferenciación de la(s) sede(s) habilitada(s) de formación teórica, donde imparten la capacitación; identificación de los vehículos registrados al CEA; identificación de los equipos de cómputo y sus componentes principales (Board, Disco Duro, Tarjeta de Red).

El representante legal o administrador que delegue el representante legal realizará el registro de todos los usuarios (administradores, recepcionistas, instructores, capacitadores).

El Software de Gestión del Sistema de Control y Vigilancia generará las respectivas alertas de vencimiento de los requisitos de habilitación.

2.6.4.4. Módulo de Enrolamiento o Registro.

Se realizará el registro de todos los actores que intervienen en el proceso y de los aspirantes/solicitantes. Para el registro se escaneará toda la información del documento de identificación que se encuentra impresa y en el código de barras bidimensional para la verificación de la legitimidad del documento, luego se procederá al registro de la información biométrica tales como huellas dactilares, fotografía del rostro, huella de voz, firma manuscrita, etc; en los dispositivos electrónicos captadores dispuestos por el proveedor del Sistema de Control y Vigilancia, la información biométrica servirá como mecanismo de identificación durante todas las formaciones, evaluaciones y capacitaciones. Al finalizar todo el proceso y antes de expedir el Certificado de Aptitud para Conducir, se validará con el operador tecnológico de la RNEC, la información biométrica dactilar del aspirante/solicitante, el cual responderá con el hit de validación positivo o negativo, con su certificación digital y estampado cronológico.

Deberá permitir además el registro digitalizado de la solicitud aceptada y firmada por el aspirante.

Se deberán registrar y enrolar cada uno de los formadores, instructores de los CEA y los capacitadores para el caso de los CIA. En todo caso se deberán enrolar con las 10 huellas dactilares y el resto de información biométrica.

2.1.2.1. Módulo Registro de exámenes.

Cada CEA deberá realizar el registro de un banco o base de datos de preguntas en el Software de Gestión del Sistema de Control y Vigilancia, de al menos diez (10) por cada apartado, módulo y/o tema como son: Mecánica Básica; Marco Legal; Técnicas de Conducción; Adaptación al Medio; Ética, Prevención de Conflictos y Comunicación, entre otros según la normatividad vigente.

2.1.2.2. Módulo de Examinaciones Teóricas.

El Software de Gestión del Sistema de Control y Vigilancia deberá generar evaluaciones de forma aleatoria de al menos dos (2) preguntas por cada apartado, módulo y/o tema tomadas del Banco o Base de Datos de Preguntas. El Software de Gestión deberá registrar los resultados de todas las evaluaciones, generando un ranking de preguntas por grado de dificultad. Las evaluaciones generadas deben ser diferentes para cada aspirante evaluado que se encuentre programado en la misma fecha, hora y lugar.

La herramienta del Software de Gestión del Sistema de Control y Vigilancia permitirá definir por el CEA, los rangos de aprobación determinados por la normatividad legal vigente. El sistema controlará que el aspirante podrá iniciar las clases prácticas, cuando culmine satisfactoriamente la capacitación teórica.

2.1.2.3. Módulo de Examinaciones Prácticas.

El Software de Gestión del Sistema de Control y Vigilancia a través de la aplicación para celulares inteligentes, debe permitir el registro de los resultados de la Formación-Examinación Práctica, donde instructor pueda ir registrando y verificando el cumplimiento cada uno de los treinta y dos (32) puntos a evaluar, donde incorpora si el aspirante ha realizado correctamente (SI/NO), es APTO o NO APTO los puntos a evaluar o verificar, así como el recorrido realizado a través del GPS integrado en el celular inteligente del instructor.

2.1.2.4. Módulo de Registro de los resultados.

El Software de Gestión del Sistema de Control y Vigilancia para los CEA, deberá llevar un registro de toda la información de los resultados obtenidos de cada evaluación y el resultado final que defina la aptitud según los parámetros de evaluación definidos por cada Escuela y sujetos a verificación y modificación por parte de la Agencia Nacional de Seguridad Vial.

2.1.2.5. Módulo de Evaluación de Aptitud.

En este módulo solo deberán tener permisos de acceso, particulares a su perfil, los capacitadores y/o los instructores designados para cada labor y creados previamente por el Representante Legal quien este autorice de las CIAS ó CEAS. Se realizará la validación de identidad biométrica a través de la huella dactilar, huella de voz, o reconocimiento facial del aspirante/solicitante al principio y al final de cada evaluación, según los diferentes apartados de formación definidos en la resolución 3245 del 2009 y la normatividad que la adicione, modifique o reemplace; además del control de los tiempos mínimos de cada evaluación y el registro y calificación de los criterios de evaluación.

En caso de que el aspirante/aspirante repruebe algún examen, el CEA a través del Software de Gestión del Sistema de Control y Vigilancia podrá parametrizar el procedimiento para volver a presentar los respectivos exámenes.

2.1.2.6. Módulo de Control de Asistencia

2.1.2.6.1. Centros Integrales de Atención. El Software de Gestión del Sistema de Control y Vigilancia debe realizar el registro y control de la asistencia de los infractores e instructores a las capacitaciones validando biométricamente su huella dactilar al principio y al final de la capacitación.

2.1.2.6.2. Centros de Enseñanza Automovilística. El Software de Gestión del Sistema de Control y Vigilancia debe realizar el registro y control de la asistencia de los aspirantes e instructores en las capacitaciones o clases teóricas y prácticas validando biométricamente a través de la huella dactilar, huella de voz, o reconocimiento facial del aspirante/solicitante al principio y al final de cada al principio y al final de la capacitación.

2.1.2.7. Módulo de Certificación.

El representante legal del CEA o del CIA o su(s) delegado(s), serán los responsables de certificar la aptitud en conducción o la reeducación en conducción a través de su usuario, contraseña y validación de su huella. Ambos serán igualmente responsables y solidarios civil, penal y administrativamente, de la veracidad información registrada en el Sistema de Control y Vigilancia. El Representante Legal deberá crear en este módulo a su(s) delegado(s).

Dentro de las funciones del representante legal y/o su delegado, está el verificar el cumplimiento de la normatividad vigente en cada una de las capacitaciones y evaluaciones realizadas, donde la decisión de aprobar o no estos procesos estará bajo su responsabilidad.

2.1.2.8. Expedición del Certificado.

En la expedición del certificado de aptitud para conducir por el Representante Legal o su delegado de cada CEA o CIA, serán emitidos a través del Software de Gestión del Sistema de Control y Vigilancia una vez validado todo el proceso.

El sistema controlará que el CEA desarrolle el proceso de capacitación, de forma proporcional a los pagos recibidos, de forma tal que se imparta capacitación en proporción al pago realizado, y que sólo se expida el certificado, una vez se culmine satisfactoriamente la capacitación y se haya pagado en su totalidad.

2.1.2.9. Módulo de Informes.

El Software de Gestión del Sistema de Control y Vigilancia deberá contar con un generador de informes estadísticos y de cumplimiento conforme a los requerimientos de la Superintendencia de Puertos y Transporte y las autoridades que así lo requieran.

2.1.2.10. Módulo de Aplicaciones Móviles.

El Software de Gestión del Sistema de Control y Vigilancia contará con una aplicación para dispositivo celular Smartphone compatible con Android, IOS, donde el aspirante/solicitante y el instructor puedan ver a que clases ha asistido, cuales clases les hace falta, el diagrama de nivel cumplimiento, la agenda de aulas y clases teóricas del CEA autorizado donde estás inscrito, disponibilidad de vehículos, tarifas, Pines adquiridos por el aspirante/solicitante,

estado de cuenta, agenda programada de clases teóricas del instructor, notificaciones, recordatorios de clases agendadas, datos de contacto del aspirante/solicitante e instructores asignados, módulo de solicitud de re-agendamiento, sistema de seguimiento GPS para clases prácticas para aspirantes/solicitantes e instructores, entre otros.

El software del Sistema de Control y Vigilancia, deberá contar con una funcionalidad que permita parametrizar el número de cuotas (si el pago se realiza de forma diferida), con su correspondiente valor, pudiendo determinar el número máximo de cuotas.

2.1.3. VISITAS DE VERIFICACIÓN A LOS ASPIRANTES A PROVEEDORES DEL SISTEMA DE CONTROL Y VIGILANCIA.

Se realizará las siguientes visitas en máximo dos (2) días hábiles. En estas visitas el evaluador tomará evidencia, fotográfica y fílmica para verificar el cumplimiento de los requerimientos.

Se deberá tener a disposición los recursos necesarios para poder realizar las verificaciones.
En la visita se verificará los requerimientos y requisitos técnicos y tecnológicos descritos anteriormente y adicionalmente siguientes requerimientos:

a) El Sistema de Control y Vigilancia deberá disponer de un dispositivo de Identificación del Vehículo físico y electrónico que se adhiera a un elemento fijo del mismo de forma permanente (parabrisas, chasis entre otros), y debe tener un sistema o medida de protección que lo proteja ante intento de manipulación, deberá permitir el registro de la ubicación del vehículo, debe permitir la validación de la identificación biométrica del aspirante/solicitante e instructor al principio y al final de cada clase y examen, deberá monitorear la ubicación del vehículo en tiempo real durante las formación práctica del alumno, teniendo trazabilidad desde el inicio y hasta la finalización de la clase. Deberá realizar las validaciones generando una alerta en caso de presentar alguna inconsistencia al centro de monitoreo. El dispositivo de identificación de los vehículos tendrá que ser resistente a condiciones ambientales adversas, sujeto al parabrisas o al chasis del vehículo o en lugar visible y de fácil acceso. Se controlará la operación de los vehículos autorizados en las CEAs a través de un dispositivo que contenga un módulo de geo-posicionamiento GPS con la precisión suficiente y permanente, que permita rastrear y enviar las coordenadas geográficas de los recorridos de las clases y/o evaluaciones prácticas programadas.
b) El Sistema de Control y Vigilancia deberá controlar los cupos de las escuelas, conforme a la capacidad autorizada e instalada.
c) El Sistema de Control y Vigilancia deberá realizar la verificación de los equipos requeridos para el funcionamiento y operaciones autorizadas por la entidad competente y que se encuentren dentro de las instalaciones del CEA. El Sistema de Control y Vigilancia validara el ID de la tarjeta principal, disco duro y la tarjeta de red física de cada uno de los PC del CEA y CIA que hagan parte de la operación de los CEA y CIA. El homologado realizará el enrolamiento de cada equipo PC que se use en el proceso.
d) Verificación de mapa de ubicaciones de Centros, máquinas y vehículos. Se deberá mostrar la ubicación de por lo menos dos centros de enseñanza automovilística (o en su defecto un Centro Integral de Atención y un Centro de Enseñanza Automovilística) en la cual se muestre el estado de su conexión. Para el caso de los Centros de Enseñanza Automovilística deberá demostrar la ubicación geográfica y el recorrido mínimo de dos vehículos (un automóvil y una motocicleta).
e) En la Examinación Práctica, el instructor deberá ir registrando y verificando el cumplimiento cada uno de los puntos de la evaluación, registrando si los ha realizado correctamente (SI/NO).
f) Verificación de la extracción de la información del documento de identidad.

g) Verificación de tramitación del PIN contra la entidad de recaudo.

2.6.5.1 Visita al Centro de Operaciones de Seguridad.

a) El centro de operaciones de seguridad deberá contar con un control de acceso biométrico.
b) El centro de operaciones de seguridad deberá contar con un sistema de circuito cerrado de televisión.
c) El centro de operaciones de seguridad deberá estar ubicada en territorio nacional.
d) Se deberá tener a disposición de los recursos necesarios para poder realizar las verificaciones:
e) Prueba de ataque perimetral. El especialista de hacking presentado en el equipo de trabajo del SOC, deberá ejecutar un escaneo de puertos a una de las direcciones de red utilizadas por el sistema presentado a homologar. Posterior a esto el IPS deberá identificar, registrar y reaccionar ante este escaneo procediendo a interrumpir la comunicación entre el escáner atacante y el sistema. Posterior a esto el evento deberá quedar registrado en la herramienta de SIEM.
f) Verificación de Endpoint. Se deberá demostrar que se encuentran instaladas en los servidores la solución de antimalware.
g) Trazabilidad de la ubicación del vehículo durante la clase, y al final de la clase.
h) Dispositivo que controle la ubicación del CEA o del CIA
i) Dispositivo que controle biométricamente a la entrada de cada aula de capacitación.

2.6.5.2 Visita a un Centro de Enseñanza Automovilística.

Se deberá mostrar el funcionamiento del Sistema de Control y Vigilancia. Se procederá a realizar visita a un (1) CEA en el cual se encuentre instalada la solución y se permita verificar los siguientes escenarios:

1. Verificación del proceso de pago. Se deberá demostrar el pago del valor integral o parcial de la capacitación, examen de aptitud y el certificado directamente sobre la red de recaudo del actor del aliado de recaudo. Esto deberá cumplir con todos los requerimientos exigidos en la lista de chequeo del anexo técnico. En el caso de requerirse participación del aliado de recaudo para realizar esta verificación, el aspirante será el encargado de coordinar todos los Requerimientos para poder realizar la prueba. Se verificará además la consulta de validez y consumo de un (1) número PIN con un aspirante/solicitante y un convenio.

2. Verificación del proceso de enrolamiento y operación de los diferentes actores de los CEA. Se deberá demostrar que el Software de Gestión del Sistema de Control y Vigilancia, realice el registro de empresas, establecimientos comerciales y sus respectivos Representantes Legales, Personal Administrativo, con su correspondiente perfil y de los aspirantes /solicitantes; así como capturar la información biométrica, biográfica y datos complementarios definidos en este documento, a través de los siguientes dispositivos:

   i. Lector biométrico de huellas con funcionalidad activa de dedo vivo (LFD), con módulo SAM para el proceso de enrolamiento.
   ii. Sistema de control de asistencia con lector biométrico de huellas, se conectará a través de IP integrado con módulo SAM, para las aulas de formación.

iii. Cámara con sensor digital de alta definición, con componentes ópticos Carl Zeiss y que genera imágenes nítidas, deberá soportar el estándar de reconocimiento facial ISO/IEC 19794-5 a través de software.

iv. Captura y extracción de la información del Código Bidimensional contenido en la cédula de ciudadanía con los parámetros de la ficha técnica vigente a través de Pistola y/o Escáner de lectura de código bidimensional.

v. Captura y digitalización de firmas manuscritas a través de Pad-Tableta digitalizadora.

vi. Verificación de validación de equipos. Se deberá demostrar que un dispositivo de hardware incorporado en cada PC del CEA y CIA, permita la identificación y realice la validación geofísica de los PCS registrados, cada 60 minutos integrado con el SOC en el servidor de validación de geo-posicionamiento. Además deberá extraer la información de la dirección MAC y el número de serie de la tarjeta madre del PC.

Verificaciones a realizar:

vii. Verificación de la integración con la plataforma del Operador tecnológico QUE CUMPLA CON LOS REQUERIMIENTOS EXIGIDOS EN EL NUMERAL 2.4.5, a través de la validación de la témplate de la huella dactilar capturada en el CEA y en CIA, en el proceso de enrolamiento contra un ambiente de pruebas, verificando si pertenecen y NO pertenecen al instructor, capacitador y aspirante.

viii. Verificación de la presencia del instructor, capacitador y aspirante, en todo el proceso de formación, evaluación. Se deberá demostrar que el usuario se valide biométricamente, al principio y final de cada formación o evaluación.

ix. La aplicación deberá contar con mecanismo alterno de validación en el proceso de enrolamiento para tramitar las excepciones del aspirante/solicitante con discapacidades que no les permita registrar y validar la huella dactilar requerida.

x. El sistema deberá contar con un mecanismo alterno y redundante de validación biométrica de identidad.

1. Verifique que la aplicación continúa dentro del proceso de validación de identidad cuando no se pueda realizar la comparación de huellas dactilares contra la réplica de la base de datos de la Registradora Nacional del estado Civil, para determinar la identidad del aspirante/solicitante.
2. Verifique que la aplicación realice como mínimo cuatro (4) preguntas socio-demográficas del aspirante/solicitante.
3. Verifique que las preguntas contengan un grupo de posibles respuestas en donde solo una es la correcta.
4. Verifique que la aplicación inicie el proceso de enrolamiento con otra IDENTIFICACION BIOMETRICA diferente O EL NUMERO DE CEDULA, si el aspirante/solicitante respondió correctamente las preguntas.
5. Verifique que la aplicación continúe en el proceso de validación de identidad si no se puede confirmar la identidad con el grupo de preguntas y que la aplicación vuelva a presentar un segundo grupo de preguntas diferentes a las iniciales.
6. Verifique que la aplicación no realice más de dos intentos para validar la identidad del aspirante/solicitante.

i. Validación de identidad con el proceso alternativo para tarjetas de identidad "TI" y Cédulas de Extranjería "CE".

ii. Compruebe que la aplicación realiza el escaneo del anverso y reverso del documento.

iii. Compruebe que la aplicación almacena las imágenes como soporte del documento presentado por el candidato.
iv. Compruebe que se extrae la información legible del documento con tecnología de reconocimiento de caracteres "OCR".
v. Verifique que los datos han sido extraídos tanto del anverso como del reverso del documento "TI".

7. Verifique la geo-posición o posición geográfica del CEA y del CIA en un centro de monitoreo, y la ruta georreferenciada de los vehículos en tiempo real.

2.6.6 Infraestructura Tecnológica en los CEA y CIA.

El aspirante a proveedor deberá suministrar y soportar los siguientes dispositivos, suministros y periféricos en los Centros de Enseñanza Automovilística con las siguientes características y/o funcionalidades:

- Un lector Biométrico de huellas en la Recepción para el proceso de enrolamiento y en cada equipo de examinación o evaluación con las siguientes especificaciones:
  i. Tipo de Sensor Óptico, Resolución del Sensor: 500 dpi, Área de captura de la Imagen: 16 x 24 mm o superior, además deberá tener un módulo SAM.
  ii. Observaciones: El lector biométrico con lector de tarjetas inteligentes integrado y las tarjetas serán propiedad del proveedor homologado y cualquier daño o pérdida de estos en los Centros será asumido por los CEA y CIA donde se asignaron dichos elementos.
  iii. Los elementos que sean asignados a un CEA y/o CIA, no podrán ser trasladados de ubicación (a otro CEA, CIA u otro lugar).
  iv. En los casos de detectar con evidencias el intento de manipulación o traslado de los dispositivos y suministros, el proveedor homologado impedirá a que continúen las validaciones de identidad desde el CEA y/o CIA identificado y se le informará a la Superintendencia de Puertos y Transporte para lo pertinente.

- Pistola o Escáner Lector de Código de Barras Bidimensional.
- Cámara con sensor digital de alta definición, con componentes ópticos Carl Zeiss y que genera imágenes nítidas, deberá soportar el estándar de reconocimiento facial ISO/IEC 19794-5 a través de software.
- Pad de firmas.
- Dispositivo de Identificación de Geo-posición. Hardware que deberá tener la función de identificar la geo-posición del Centro y PC mediante el uso de tecnología GPS:

  i. Seguridad. El Representante Legal del CEA y CIA será el responsable de la buena utilización del sistema de acuerdo a las recomendaciones del proveedor homologado con quien contrate el servicio, con el fin de evitar manipulación y/o daños que se puedan causar deliberadamente o de manera accidental al sistema.
  ii. Actualización máxima de la Geo-referenciación, comunicación celular y/o satelital. Marcación del posicionamiento interno cada 60 minutos.
  iii. Envío de la información de la ubicación al centro de control y/o plataforma de monitoreo cada 60 minutos enviará una (1) posición con la identificación del PC, dirección MAC y número de serie de la tarjeta madre.
  iv. Compatibilidad. Con los prestadores de servicios móviles de comunicación en cuanto a tecnología, cobertura y disponibilidad requerida, existentes en el mercado.

- Los computadores de los CEA y CIA autorizados que interactúen con el Sistema de Control y Vigilancia deberán tener las siguientes características:
  i. Memoria RAM 4 GB como mínimo.
  ii. Disco Duro con almacenamiento mínimo disponible 50 GB.
  iii. Tarjeta de Red Ethernet Física 10/100/1000
  iv. Sistema Operativo Windows 7 o superior.
  v. Procesador de Tercera Generación o Superior.

Nota: Los CEA deberán tener además de computadores para el registro y enrolamiento, computadores para realizar las evaluaciones o examinaciones teóricas a los aspirantes.

2.6.7 Compromisos Posteriores

El aspirante a proveedor debe generar una carta de compromiso firmada por el representante legal, en la cual establezca que una vez reciba la homologación se comprometerá a realizar las siguientes actividades:

1) Los aspirantes a proveedores deberán presentar un documento de compromiso posterior, que la disponibilidad del servicio (ANS o SLA) con los CEA y CIA deberá ser al iniciar la operación como mínimo del 98,5% con base en el horario de atención de los CEA y CIA.
2) Antes de entrar en operación se deberán realizar las integraciones con la plataforma RUNT a través de webservices para que el RUNT valide si la solicitud de registro en HQ-RUNT cumple con registro completo en Sistema de Control y Vigilancia a través del Software de Gestión. Y a establecer un canal dedicado con el sistema RUNT a cuenta del proveedor homologado.
3) Antes de entrar en operación realizar todas las integraciones con un operador tecnológico avalado por la Registraduría Nacional del Estado Civil para cumplir con el proceso de validar la identidad de los usuarios contra la Base de Datos de la RNEC. El operador tecnológico avalado por la Registraduría Nacional del Estado Civil deberá garantizar la validación de identidad a través de una réplica, licenciamiento y personal certificado conforme a los requerimientos de la RNEC, además deberá entregar junto con el hit de validación de identidad una certificación digital y estampado cronológico, además de seguridad e integridad en el log.
4) Establecer un canal dedicado y VPN a cuenta del proveedor homologado con el centro de monitoreo de la Superintendencia de Puertos y Transporte.
5) Garantizar que se realice el control de las tarifas del curso, de conformidad a lo establecido por el Ministerio y Transporte.

2.6.8 Equipos (compra, suministro e instalación).

Con el objeto de garantizar la calidad, compatibilidad y buen funcionamiento del sistema de control y vigilancia, los dispositivos entregados e instalados a los CEA y CIA para su operación, tales como lector biométrico de huella dactilar con módulo SAM y el lector biométrico de huella con funcionalidad de Control de Asistencia, entre otros, serán suministrados y de propiedad de cada homologado. El valor generado por compra, suministro de los equipos, su mantenimiento e instalación en los CEA Y CIA será incluido en la tarifa final que el homologado defina para la prestación del SICOV a cada tipo de Centro no generando un costo adicional al vigilado.

El mantenimiento de los equipos y del software, debe realizarse por el homologado, quien podrá cobrarle al CEA las reparaciones que deban realizarse cuando los daños de los equipos se causen en indebida manipulación por parte del CEA.