

Por la cual se expide al anexo técnico para la implementación de los Sistemas de Control y Vigilancia de que trata la Resolución 13829 de 2014.

ANEXO TÉCNICO DE REQUISITOS Y REQUERIMIENTOS QUE DEBERAN CUMPLIR LOS PROVEEDORES DEL SISTEMA DE CONTROL Y VIGILANCIA PARA LOS CENTROS DE RECONOCIMIENTO DE CONDUCTORES, SEGÚN LA RESOLUCIÓN 13829 DE 2014

INTRODUCCIÓN

El presente documento define los requerimientos que deben cumplir aquellos aspirantes a proveedores del Sistema de Control y Vigilancia de que trata la Resolución 13829 de 2014. 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.

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 Reconocimiento de Conductores.

1.2 SISTEMA DE CONTROL Y VIGILANCIA DE LOS CENTROS DE RECONOCIMIENTO DE CONDUCTORES.

El Sistema de Control y Vigilancia es una infraestructura tecnológica operada por cualquier ente público o privado que el Centro de Reconocimiento de Conductores (en adelante CRC), 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 usuario aspirante y de los médicos o especialistas en el Centro de Reconocimiento de Conductores.
- La realización de cada una las pruebas.
- Que el certificado se expida desde la ubicación geográfica del Centro de Reconocimiento
- Que las pruebas se hagan desde los computadores de los Centros de Reconocimiento de Conductores, 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 CRC 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 física, mental y de coordinación motriz se expidió bajo el cumplimiento de los requisitos y condiciones fijados en las normas vigentes para el tema. Para ello, se hará uso de los medios tecnológicos sistematizados y digitalizados requeridos,

Por la cual se expide al anexo técnico para la implementación de los Sistemas de Control y Vigilancia de que trata la Resolución 13829 de 2014.

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 Centros de Reconocimiento de Conductores, buscan esencialmente garantizar la legitimidad a través de la realización del proceso de aptitud física, mental y de coordinación motriz, 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 y en virtud de las mismas, se expidió la Resolución 13829 del 2014, que reglamenta las características técnicas que deberá tener el Sistema de Control y Vigilancia para los Centros de Reconocimiento de Conductores, determinando las exigencias tecnológicas que deben implementar los Centros de Reconocimiento de Conductores, mediante el cual se reporta la información a la Superintendencia.

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 requisitos 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 Reconocimiento de Conductores.

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

Los Requisitos 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.

Por la cual se expide al anexo técnico para la implementación de los Sistemas de Control y Vigilancia de que trata la Resolución 13829 de 2014.

Los Requisitos Jurídicos, buscan principalmente garantizar la legalidad de las entidades a homologarse, de sus representantes

Los Requisitos 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 homologarse para conseguir esta meta, y presenta diferentes alternativas para el cumplimiento de los requisitos 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 - REQUISITOS DOCUMENTALES

A continuación se establecen los requisitos que deberán cumplir los aspirantes a homologación 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 Requisitos Documentales

La carta de interés y radicación de requisitos documentales, permitirá iniciar el proceso de validación de los requisitos para homologarse como proveedor del Sistema de Control y Vigilancia en los Centros de Reconocimiento de Conductores. Ver numeral 2.1.2: Modelo Carta de Interés y Radicación de Requisitos 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 requisitos 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.
- [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 2015**]”, donde NN debe ser reemplazada por el número de Resolución que expida la Superintendencia de Puertos y Transporte con el Anexo Técnico de Requisitos y Requerimientos para el Sistema de Control y Vigilancia de los Centros de RECONOCIMIENTO DE CONDUCTORES.
- “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.

Por la cual se expide al anexo técnico para la implementación de los Sistemas de Control y Vigilancia de que trata la Resolución 13829 de 2014.

2.1.2. Modelo Carta de Interés y Radicación de Requisitos 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 requisitos para homologarse como proveedor del Sistema de Control y Vigilancia para los CRCs.

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 Reconocimiento de Conductores (CRCs) como proveedor del Sistema de Control y Vigilancia.

Se anexa los requerimientos documentales exigidos en la Resolución NN de 2014 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. Requisitos del aspirante.

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

2.2.1 Instrucciones de la presentación del Documento con los Requisitos del aspirante.

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 requisitos documentales debe ser en español.
- Papel: Tamaño carta 8.1/2”x11”

Por la cual se expide al anexo técnico para la implementación de los Sistemas de Control y Vigilancia de que trata la Resolución 13829 de 2014.

2.2.2 Portada

La portada es la primera página y servirá para identificar claramente al aspirante que anexa los requisitos documentales, esta hoja debe contener el número 1 en área de foliación. Ver numeral 2.2.2.2: Modelo de la portada general.

2.2.3 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 del Sistema de Control y Vigilancia para los CRC, 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.
- [CIUDAD] Ciudad donde se origina la documentación.
- “201N”, donde “N” es el último dígito del año en el que se radican los documentos.

2.2.4 Modelo de la Portada General.

PRESENTACIÓN DE REQUISITOS 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]
201N

Índice General

El índice general permite organizar el documento en el orden en que se debe entregar, dependiendo de si el aspirante es una empresa, una Unión Temporal o un Consorcio, su contenido puede variar según los requisitos específicos para cada caso. Ver numeral 2.2.3.2 Modelo del índice general (Empresa, Unión Temporal o Consorcio).

2.3. 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.

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

INDICE GENERAL

	No. De Folio
1. REQUERIMIENTOS JURÍDICOS	
1.1. Requerimiento jurídico AAA.....	#
1.2. Requerimiento jurídico BBB.....	#

Por la cual se expide al anexo técnico para la implementación de los Sistemas de Control y Vigilancia de que trata la Resolución 13829 de 2014.

1.n.	Requerimiento jurídico nnn.....	#
2.	REQUERIMIENTOS ADMINISTRATIVOS	
2.1.	Requerimiento administrativo AAA.....	#
2.2.	Requerimiento administrativo BBB.....	#
2.n.	Requerimiento administrativo nnn.....	#
3.	REQUERIMIENTOS FINANCIEROS	
3.1.	Requerimiento financiero AAA.....	#
3.2.	Requerimiento financiero BBB.....	#
3.n.	Requerimiento financiero nnn.....	#
4.	REQUERIMIENTOS TÉCNICOS	
4.1.	Requerimiento técnico AAA.....	#
4.2.	Requerimiento técnico BBB.....	#
4.n.	Requerimiento técnico nnn.	#

Lista de Requisitos Jurídicos

Los Requisitos 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 incurso 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 con el Estado.

Por la cual se expide al anexo técnico para la implementación de los Sistemas de Control y Vigilancia de que trata la Resolución 13829 de 2014.

Las inhabilidades son una limitación a la capacidad de contratar con Entidades Estatales y están expresamente señaladas en la ley, que establece que no son hábiles para participar en Procesos de Contratación, además de quienes están en las siguientes situaciones:

- Las personas que se hallen inhabilitadas para contratar por la Constitución y las leyes.
- 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.
- 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.
- 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.
- 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.
- Los servidores públicos.

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.

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

Por la cual se expide al anexo técnico para la implementación de los Sistemas de Control y Vigilancia de que trata la Resolución 13829 de 2014.

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 proveedores 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 Reconocimiento de Conductores 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.

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 proveedores 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

Por la cual se expide al anexo técnico para la implementación de los Sistemas de Control y Vigilancia de que trata la Resolución 13829 de 2014.

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.

Por la cual se expide al anexo técnico para la implementación de los Sistemas de Control y Vigilancia de que trata la Resolución 13829 de 2014.

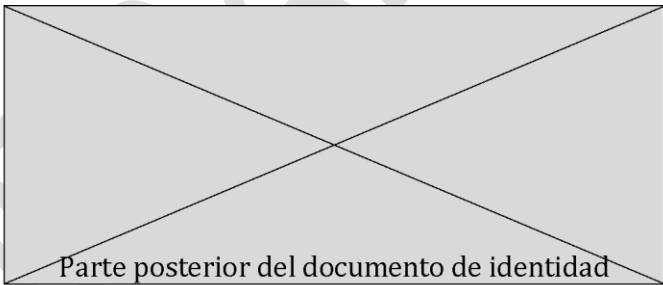
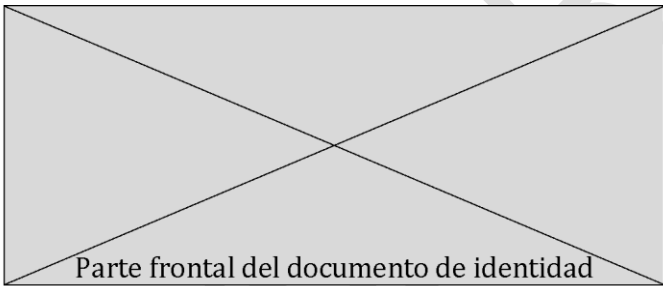
Esta clase excluye: La explotación de los sitios web. Se incluye en la clase 6312, «Portales web».

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. 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 requisitos documentales presentados por [RAZÓN SOCIAL EMPRESA, CONSORCIO O UNIÓN TEMPORAL], en su intención de participar en el proceso que adelanta la Superintendencia de Puertos y Transporte para prestar el servicio a los Centros de Reconocimiento de Conductores (CRCs) como proveedor del Sistema de Control y Vigilancia.



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)]

Por la cual se expide al anexo técnico para la implementación de los Sistemas de Control y Vigilancia de que trata la Resolución 13829 de 2014.

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, 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).

Especificaciones de la entrega del documento.

1. emitido por revisor fiscal o representante legal según corresponda, basado en el tipo Certificado de persona.
2. Su expedición debe ser igual o inferior a 30 días calendario al de la fecha de radicación.
3. 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.
4. 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 noventa 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 2.3.5.1: 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 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.

5. El certificado deberá ser autenticado con firma y huella.
6. [RAZÓN SOCIAL EMPRESA, CONSORCIO O UNIÓN TEMPORAL], deberá reemplazarse por el nombre del ente.

Por la cual se expide al anexo técnico para la implementación de los Sistemas de Control y Vigilancia de que trata la Resolución 13829 de 2014.

7. [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.
8. Deberá certificar el 100% de las acciones de la compañía.
9. [NN], debe reemplazarse por el día en número que se expide el certificado
10. [Mes en Letras], debe reemplazarse por el mes que se expide el certificado, descrito en letras.
11. [AAAA], debe reemplazarse por el año en que se expide el certificado, descrito en cuatro dígitos.
12. [Número de la Tarjeta Profesional], debe reemplazarse por el número de la Tarjeta Profesional del Revisor Fiscal Vigente.
13. Huella del Revisor Fiscal o Representante Legal dependiendo el tipo de empresa, debe colocarse la huella del Revisor Fiscal la cual debe ir autenticada.
14. 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 CRC.

Cordialmente,

[NOMBRES Y APELLIDOS DEL REVISOR FISCAL]

Revisor Fiscal

T.P. [Número de la Tarjeta Profesional]

Huella

del

Revisor

Fiscal

Por la cual se expide al anexo técnico para la implementación de los Sistemas de Control y Vigilancia de que trata la Resolución 13829 de 2014.

[RAZÓN SOCIAL O NOMBRE DE LA EMPRESA O CONSORCIO]

2.4 Lista de Requisitos Administrativos.

Los Requisitos Administrativos incluyen mecanismos que permitan la validación de aspectos tales como la trayectoria del aspirante, 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 derivado de su participación previa en actividades iguales o similares a las previstas en el objeto del contrato.

Los aspirantes 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.

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 plural.

Por otra parte, cuando un aspirante 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 Reconocimiento de Conductores.

Conforme a lo establecido en el Decreto 1510 del 2013: "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 requisitos habilitantes de experiencia, capacidad jurídica, capacidad financiera y capacidad organizacional". En este caso, la Entidad considera que los requisitos 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 d
- 4) Deberán desglosar el monto y objeto para el cual aplica dicha certificación.
- 5) Número de contratos a certificar: Los aspirantes deberán acreditar experiencia mediante certificación firmada por los contratantes o entes gubernamentales en máximo seis (6) certificaciones.

Por la cual se expide al anexo técnico para la implementación de los Sistemas de Control y Vigilancia de que trata la Resolución 13829 de 2014.

- 6) 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.
- 7) 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:
- 8) 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.
- 9) Software: Desarrollo y/o Implantación de Software.
- 10) 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 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.

Especificaciones de la entrega del documento.

Cada formato de certificaciones de experiencia del aspirante deberá estar firmado y con huella legible por el Representante Legal del aspirante 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 de cada una de las empresas que lo(a) conformen.

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 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.

Por la cual se expide al anexo técnico para la implementación de los Sistemas de Control y Vigilancia de que trata la Resolución 13829 de 2014.

	• 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, 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 redundará en resultados de calidad en sus negocios, contribuyendo al mejoramiento de la competitividad de la empresa, un factor que lo hace diferenciador entre sus competidores.

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

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.

Por la cual se expide al anexo técnico para la implementación de los Sistemas de Control y Vigilancia de que trata la Resolución 13829 de 2014.

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

- **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,

Por la cual se expide al anexo técnico para la implementación de los Sistemas de Control y Vigilancia de que trata la Resolución 13829 de 2014.

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, ISO 20000 ó ISO 15504). La certificación deberá estar vigente a la fecha de evaluación.

El aspirante 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.

Especificaciones de la entrega del documento.

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

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	
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	Certificación ISO 27001 Certificado No. _____ Fecha de Expedición: DDMMAAAA Fecha de Vencimiento: DDMMAAAA

Por la cual se expide al anexo técnico para la implementación de los Sistemas de Control y Vigilancia de que trata la Resolución 13829 de 2014.

Entidad Certificadora: Teléfono Contacto Ent. Certificadora:_____ Web Consulta Ent. Certificadora:_____ e-mail contacto Ent. Certificadora:_____	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.

Por la cual se expide al anexo técnico para la implementación de los Sistemas de Control y Vigilancia de que trata la Resolución 13829 de 2014.

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.

Por la cual se expide al anexo técnico para la implementación de los Sistemas de Control y Vigilancia de que trata la Resolución 13829 de 2014.

Se requerirá 1 (un) profesional en Ingeniería de Sistemas, Industrial, Electrónica o carreras afines, certificado como CEH, o contrato con una compañía para la prestación de Servicios de Ethical Hacking. 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 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, 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 una (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 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. 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 CRC, 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.

Por la cual se expide al anexo técnico para la implementación de los Sistemas de Control y Vigilancia de que trata la Resolución 13829 de 2014.

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 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 CRC'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 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 CRC's contratados.

El aspirante 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.

2.4.3.6 Especificaciones de la entrega del documento.

Por la cual se expide al anexo técnico para la implementación de los Sistemas de Control y Vigilancia de que trata la Resolución 13829 de 2014.

- 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 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 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: <u>(especifique el título de grado)</u> • ingeniería de sistemas, • industrial, • electrónica • carreras afines Posgrado ó certificación : <u>(especifique el título de posgrado)</u> • En gerencia de proyectos • Maestría en ingeniería de sistemas • Certificación de PMP Experiencia: • Dirección de proyectos en los últimos 3 años. Tipo de Contrato: <u>(especifique el tipo de contrato)</u> Pago de Aportes Parafiscales: <u>(Especifique el o los números de folio donde aporta la planilla con dicho pago)</u>
Equipo de trabajo de seguridad Gerente de SOC.(1)	Título profesional en: <u>(especifique el título de grado)</u> • ingeniería de sistemas, • industrial, • electrónica • carreras afines Posgrado ó certificación : <u>(especifique el título de posgrado)</u> • En seguridad informática • Certificación Auditor Interno ISO-27001 Tipo de Contrato: <u>(especifique el tipo de contrato)</u> Pago de Aportes Parafiscales: <u>(Especifique el o los números de folio donde aporta la planilla con dicho pago)</u>
Equipo de trabajo de seguridad Oficial de Seguridad. (1)	Título profesional en: <u>(especifique el título de grado)</u> • ingeniería de sistemas, • industrial, • electrónica • carreras afines Posgrado ó certificación : <u>(especifique el título de posgrado)</u> • En seguridad informática • certificado como CISSP

Por la cual se expide al anexo técnico para la implementación de los Sistemas de Control y Vigilancia de que trata la Resolución 13829 de 2014.

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

Por la cual se expide al anexo técnico para la implementación de los Sistemas de Control y Vigilancia de que trata la Resolución 13829 de 2014.

Ingenieros tecnológicos de desarrollo. (2 mínimo)	• <u>Tecnólogo de Sistemas - (Especifique Cantidad)</u> • <u>Posgrado y certificación en: (especifique el título de posgrado)</u> • Construcción de Software • Arquitectura Empresarial de Software • ITIL Foundation versión 3 o superior • <u>Certificación técnica o laboral: (especifique el lenguaje de desarrollo en que se encuentra construida la aplicación)</u> • Aplica (deberá adjuntar las respectivas certificaciones) • No aplica • <u>Contrato con una fábrica de software: (especifique el contrato con dicha fábrica, licencias de uso)</u> • Aplica (deberá adjuntar el contrato, licencias de uso y certificaciones del personal de la fábrica de software) • No aplica • <u>Tipo de Contrato: (especifique el tipo de contrato)</u> • <u>Pago de Aportes Parafiscales: (Especifique el o los números de folio donde aporta la planilla con dicho pago)</u>
Equipo de trabajo de soporte Coordinador de Soporte. (1)	<u>Título profesional en: (especifique el título de grado)</u> • <u>ingeniería de sistemas,</u> • <u>industrial,</u> • <u>electrónica</u> • <u>carreras afines</u> <u>Experiencia como Líder de Soporte: (especifique el o los números de folio donde aporta la experiencia)</u> <u>Tipo de Contrato: (especifique el tipo de contrato)</u> <u>Pago de Aportes Parafiscales: (especifique el o los números de folio donde aporta la planilla con dicho pago)</u>
Equipo de trabajo de soporte Coordinador de Soporte.	<u>Título profesional en: (especifique el título de grado)</u> • <u>ingeniería de sistemas,</u> • <u>industrial,</u> • <u>electrónica</u> • <u>carreras afines</u> <u>Experiencia como Líder de Soporte: (especifique el o los números de folio donde aporta la experiencia)</u> <u>Tipo de Contrato: (especifique el tipo de contrato)</u> <u>Pago de Aportes Parafiscales: (especifique el o los números de folio donde aporta la planilla con dicho pago)</u>
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: <u>(especifique el o los números de folio donde aporta la experiencia)</u>
Firma y Huella Representante Legal del Aspirante	

2.4.4 Aliado u Operador de Recaudo.

El aspirante a proveedor deberá contar con un aliado para el servicio de recaudo previamente homologado como operador de recaudo por parte de la Superintendencia de Puertos y Transporte. El operador de recaudo podrá ser una persona jurídica o Unión Temporal, en el caso de la Unión Temporal al menos uno de los socios deberá cumplir con los requisitos para homologarse como operador de del servicio de recaudo exigidos por la Superintendencia de Puertos y Transporte.

Primero se evalúan y homologan a los operadores independientemente y después se habilitan como prestadores del servicio (Se habilitan uno con el otro en alianza) que deberá cumplir con los siguientes requisitos y requerimientos:

Por la cual se expide al anexo técnico para la implementación de los Sistemas de Control y Vigilancia de que trata la Resolución 13829 de 2014.

El aliado u operador de recaudo que acredite 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.

El aliado de recaudo deberá ser un miembro del Sistema Financiero Colombiano o un 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.

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 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 data center principal y un datacenter alternativo, 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.Rs).
- 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 Número único de pago, valor de recaudo, número de identificación del candidato y fecha y hora del pago 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), CRC donde fue utilizado o consumido el PIN, fecha del uso del servicio, hora del uso del servicio, número único de uso, entre otros.
- Deberá presentar procedimiento que evite que tratan de falsificar comprobantes de recaudo.

El aliado de recaudo deberá tener puntos de atención propios o convenio con otras entidades que cumplan los requisitos aquí, en todos los municipios del país donde se encuentren los Centros de Reconocimiento de Conductores y deberá estar en la disposición de habilitar nuevos puntos de atención cuando queden puntos muy distantes de los CRCs.

El aliado de Recaudo deberá generar una póliza de cumplimiento a favor de cada Centro de Reconocimiento de Conductores y del homologado por el buen manejo del dinero recaudado.

El aliado de recaudo deberá brindar diferentes medios de pago como pueden ser: pagos a través de Internet, datafonos, dispositivos satélites ubicados en los CRCs, entre otros).

El aliado de recaudo deberá entregar un documento a la Superintendencia de Puertos y Transporte comprometiéndose con acuerdos de niveles de servicios del 99% en los periodos de atención de los CRC.

El aliado de recaudo deberá contar con certificación de calidad y con alguna de las siguientes certificaciones: ISO 27001, PCI DSS 2.0.

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 y que deberá ser evaluado y seleccionado como el

Por la cual se expide al anexo técnico para la implementación de los Sistemas de Control y Vigilancia de que trata la Resolución 13829 de 2014.

operador tecnológico de la Superintendencia de Puertos y Transporte ante la RNEC y haber cumplido con todos los requerimientos y evaluaciones exigidos por la Registraduría Nacional del Estado Civil RNEC. El operador Biométrico debe cumplir con los siguientes requerimientos:

1. Acreditar cumplimiento de requisitos con la RNEC,
2. Deberá tener Infraestructura Tecnológica aprobada, desplegada, auditada por la RNEC y con contratos en ejecución con otras entidades públicas del servicio de Validación de Identidad contra las bases de datos de identificación ciudadana (Biometría), que actualmente posee la RNEC, manejando el estándar ISO 19794, conforme a lo dispuesto en la Resolución 3341 del 2013 de la RNEC, su anexo y la normatividad vigente.
3. La validación de identidad biométrica deberá tener características de firma electrónica con validez jurídica y probatoria según el Decreto 2364 de 2012.
4. 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.
5. El aliado deberá contar con certificación de seguridad de la información ISO 27001.

El operador biométrico deberá hacer parte de la unión temporal o consorcio que se presente como aspirante a proveedor.

2.5 Lista de Requisitos Financieros.

Los requisitos 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 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 requisitos de capacidad financiera con base en su conocimiento del sector relativo al objeto del 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 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 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

Por la cual se expide al anexo técnico para la implementación de los Sistemas de Control y Vigilancia de que trata la Resolución 13829 de 2014.

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 convirtiéndolos 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	$\frac{\text{Efectivo}}{\text{Pasivo Corriente}}$	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	$\frac{(\text{Activo Corriente} - \text{Inventarios})}{\text{Pasivo Corriente}}$	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	$\frac{\text{Pasivo Corriente}}{\text{Pasivo Total}}$	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 existe 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	$\frac{\text{Pasivo no Corriente}}{\text{Pasivo Total}}$	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) existe 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 a 31 de Diciembre de 2014 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

Por la cual se expide al anexo técnico para la implementación de los Sistemas de Control y Vigilancia de que trata la Resolución 13829 de 2014.

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 de 2014. Para los años subsiguientes, se deberán presentar los estados financieros de los dos últimos años.

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	> \$2.000.000.000
LIQUIDEZ	ACTIVO CORRIENTE / PASIVO CORRIENTE	> 1,0
NIVEL DE	PASIVO TOTAL/ACTIVO TOTAL	<= al 55%

Por la cual se expide al anexo técnico para la implementación de los Sistemas de Control y Vigilancia de que trata la Resolución 13829 de 2014.

ENDEUDAMIENTO		
CAPITAL DE TRABAJO	ACTIVO CORRIENTE - PASIVO CORRIENTE	> \$2.500.000.000
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 REQUISITOS TÉCNICOS

Este documento establece los requisitos técnicos mínimos que deben ser cumplidos por el aspirante a proveedor para garantizar la operación del Sistema de Control y Vigilancia para los CRC´s 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 CRC conectados al Sistema, así como la generación, procesamiento y transmisión de la información requerida.

La determinación de los requisitos 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 evaluaciones de aptitud física, mental y de coordinación motriz realizadas por los CRC, 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 Reconocimiento de Conductores y con la Superintendencia de Puertos y Transporte (interfase).
- Software de Gestión. Cada uno de los proveedores del sistema de seguridad, deberán proveer, A través de esta aplicación (SOFTWARE), a los Centros de Reconocimiento de Conductores deberán realizar la evaluación y certificación con los procesos de: registro o enrolamiento de centros, representantes legales, administradores, recepcionistas, médicos y especialistas; validación del pago; asignacion de citas; registro o enrolamiento del solicitante; autenticación y validación biométrica dactilar de los solicitantes y de los médicos o especialistas contra la base de datos de la RNEC y grabar en el mecanismo redundante; registro de la evaluación médica y sus cuatro etapas (psicomotriz, optometría, auditiva y

Por la cual se expide al anexo técnico para la implementación de los Sistemas de Control y Vigilancia de que trata la Resolución 13829 de 2014.

médica); registro de la historia clínica. Esta aplicación estará alojada en el CPD e integrada con 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.

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, emitida por la Superintendencia de Industria y Comercio.
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 evaluación y certificación de aptitud física, mental y de coordinación motriz por parte de los CRC, 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 CRCs, 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 CRCs.

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

Por la cual se expide al anexo técnico para la implementación de los Sistemas de Control y Vigilancia de que trata la Resolución 13829 de 2014.

datos relacional. El servidor o servidores deberán cumplir con los requerimientos de conectividad y seguridad (se utilizan como guía los estándares IEEE 802 y 27001).

- Registrar todas las transacciones y operaciones realizadas desde los computadores y equipos ubicados en los CRCs 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 CRC;
- 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 conforme a lo dispuesto en la resolución 13829 del 2014, 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.

Por la cual se expide al anexo técnico para la implementación de los Sistemas de Control y Vigilancia de que trata la Resolución 13829 de 2014.

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

2.6.3.1.2.3.1 Sistema 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.

2.6.3.1.2.3.3 Terremotos. 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.

2.6.3.1.2.4 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

Por la cual se expide al anexo técnico para la implementación de los Sistemas de Control y Vigilancia de que trata la Resolución 13829 de 2014.

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 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, y con un horario de prestación de servicio igual al horario de atención de los CRC'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 PERIMETR AL 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 Management de Gartner.
Protección de ENDPOINT	Solución basada en software para protección antimalware de los servidores utilizados del Sistema de Control y Vigilancia. La solución utilizada deberá encontrarse en el cuadrante de Leaders o Visionaries del Magic Quadrant for Endpoint Protection Platforms de Gartner.
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

Por la cual se expide al anexo técnico para la implementación de los Sistemas de Control y Vigilancia de que trata la Resolución 13829 de 2014.

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.

Requisitos 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 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.

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 CDP, 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.

Por la cual se expide al anexo técnico para la implementación de los Sistemas de Control y Vigilancia de que trata la Resolución 13829 de 2014.

2.6.3.2.2 Control de Acceso.

Las áreas restringidas como los CPDs 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 monitores 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 CDP 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).

Por la cual se expide al anexo técnico para la implementación de los Sistemas de Control y Vigilancia de que trata la Resolución 13829 de 2014.

- 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 deberá estar ubicado en territorio nacional, de la misma forma el sistema redundante (espejo), deberá estar ubicado en un lugar diferente al CDP.

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."

Por la cual se expide al anexo técnico para la implementación de los Sistemas de Control y Vigilancia de que trata la Resolución 13829 de 2014.

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 utilizados 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 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, 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:

Por la cual se expide al anexo técnico para la implementación de los Sistemas de Control y Vigilancia de que trata la Resolución 13829 de 2014.

- 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 (Seguridad 27001).

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 Arreglo 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 Homologado 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 requisitos 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 requisitos como homologado. Los costos de esta auditoría estarán a cargo del Homologado.

Por la cual se expide al anexo técnico para la implementación de los Sistemas de Control y Vigilancia de que trata la Resolución 13829 de 2014.

2.6.3.2.17 Otros Requisitos.

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

- El aspirante 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 requisitos 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 requisitos 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.

2.6.3.3 Sistema de Gestión de Calidad.

El Sistema de Gestión de Calidad tiene como objetivo estandarizar y unificar los sistemas de gestión que los Centros de Reconocimiento de Conductores establecen para realizar sus actividades de certificación de personas.

Asegurar que los organismos de certificación de personas que operan los esquemas de certificación de la aptitud física, mental y de coordinación motriz para conducir, trabajen de forma coherente, comparable y confiable.

Cumplir la reglamentación y legislación legal vigente aplicable a los CRC, unificar los criterios de evaluación definido por este sistema de gestión, con lo cual se busca proporcionar y mantener la confianza para todas las partes interesadas. Así mismo, se establecen las características del esquema de certificación que deberán implementar todos los Centros de Reconocimiento de Conductores.

2.6.3.3.1 Referencias Normativas o Marco Legal

- El Sistema de Gestión de Calidad, deberá garantizar el cumplimiento de la normatividad legal vigente que regula la certificación de la aptitud física, mental y de coordinación motriz para conducir tales como:
- Código Nacional de Tránsito (Ley 769 – Modificaciones Ley 1383 del 2010 y Ley 1397 de 2010), la Resolución 0217 del 2014 del Ministerio de Transporte.
- Código Nacional de Transito, Ley 769 de 2002 (Modificada por las Ley 1383 del 2010 y Ley 1397 del 2010).
- La Ley 1539 de 2012.
- Resolución 217 de 2014 del Ministerio de Transporte.
- Resolución 9699 de 2014. de la Superintendencia de Puertos y Transporte
- Resolución 13829:2014 de la Superintendencia de Puertos y Transporte

Por la cual se expide al anexo técnico para la implementación de los Sistemas de Control y Vigilancia de que trata la Resolución 13829 de 2014.

- Resolución 2003 de 2014 del Ministerio de la Protección Social.
- Las demás que las coemplentes o se expidan con posterioridad

2.6.3.3.2 Definiciones:

- **Sistema de Gestión de Calidad:** Es el sistema de gestión de calidad que cumple con los requisitos de la Norma NTC ISO/IEC 17024:2013, o la norma vigente, y que asegura que los organismos de certificación de personas que operan los esquemas de certificación de la aptitud física, mental y de coordinación motriz para conducir, trabajen de forma coherente, comparable y confiable bajo un solo criterio unificado y/o modelo técnico. Este estandariza los criterios, tablas de equivalencia, técnicas de evaluación y calificación, entre otras.
- **Certificado de Aptitud Física Mental y de Coordinación Motriz:** Es el documento expedido por el Centro de Reconocimiento de Conductores, mediante el cual se certifica ante las autoridades de tránsito, que el aspirante a obtener por primera vez, recategorizar y/o refrendar la licencia de conducción posee la aptitud física, mental y de coordinación motriz que se requieren para conducir un vehículo automotor.
- **Esquema de Certificación:** Requisitos específicos de certificación relacionados con categorías especificadas de personas a las que se aplican las mismas normas y reglas particulares, y los mismos procedimientos.
- **Proceso de Certificación:** Todas las actividades reguladas en el presente anexo que deben cumplir los Centros de Reconocimiento de Conductores para evaluar y expedir la certificación de aptitud física, mental y de coordinación motriz.
- **Evaluación:** Proceso regulado en el presente anexo mediante el cual se evalúa en los aspirante/pacientes el cumplimiento de los requisitos del esquema de certificación, que conduce a una decisión de certificación.
- **Examen:** Mecanismo regulado en el presente anexo que hace parte de la evaluación, que mide la competencia de un aspirante/paciente por uno o varios medios, tales como, medios científicos, orales, prácticos y por observación.
- **Competencia:** Capacidad demostrada de aptitudes y/o habilidades y atributos personales, como se define en el esquema de certificación.
- **Solicitante/Aspirante:** Persona que requiere al Organismo de Certificación de Personas su participación en el proceso de certificación de un esquema de certificación en particular conductores.
- **Examinador:** Persona con las calificaciones técnicas y personales pertinentes, que es competente para llevar a cabo y/o calificar un examen.
- **Calificación:** Demostración de atributos personales, educación, formación y/o experiencia laboral.
- **Apelación:** Solicitud presentada por un aspirante, candidato o persona que requiere la certificación, para reconsiderar cualquier decisión adversa tomada por el CRC relacionada con el estado de certificación deseada.
- **Queja:** Solicitud, en el ámbito de la evaluación de la conformidad, distinta de una apelación, presentada por una organización o persona a un OC de Certificación de Personas, de acción correctiva relacionada con las actividades de dicho CRC.

Por la cual se expide al anexo técnico para la implementación de los Sistemas de Control y Vigilancia de que trata la Resolución 13829 de 2014.

- **Agudeza Auditiva:** Capacidad de discriminación de estímulos auditivos.
- **Agudeza Visual:** Capacidad de discriminar detalles de los objetos a una distancia determinada, teniendo en cuenta factores como condiciones de luminosidad, contraste y tamaño. Se evalúa la visión cercana y la visión lejana.
- **Agudeza Visual Cinética:** Capacidad de discriminar detalles de los objetos cuando existe movimiento relativo al sujeto.
- **Anamnesis:** Información general del candidato obtenida a partir de una entrevista inicial y que se consigna en la primera parte de la Historia clínica.
- **Auditoría:** Proceso sistemático, independiente y documentado para la obtención de evidencias de cumplimiento del Sistema de Gestión de Calidad, confrontándolo con las normas vigentes de los entes reguladores, orientadas al mejoramiento de su calidad y rendimiento.
- **Auditoría Externa:** Las auditorías externas incluyen las que se denominan generalmente auditorías de segunda y tercera parte. Las auditorías de segunda parte las realizan las partes que tienen interés en la organización, por ejemplo, los clientes. Las auditorías de tercera parte las realizan organizaciones auditoras externas e independientes, con autoridad para certificar o acreditar una compañía bajo una norma de gestión establecida.
- **Auditoría Interna:** Auditoría que realiza la organización al Sistema de Gestión de Calidad implementado. La puede realizar personal interno.
- **Sistema Obligatorio de Garantía de Calidad de Atención en Salud del Sistema General de Seguridad Social en Salud (SOGCS):** Es el conjunto de instituciones, normas, requisitos, mecanismos y procesos deliberados y sistemáticos que desarrolla el sector salud para generar, mantener y mejorar la calidad de los servicios de salud en el país.
- **Calidad de la Atención de Salud:** Se entiende como la provisión de servicios de salud a los usuarios individuales y colectivos de manera accesible y equitativa, a través de un nivel profesional óptimo, teniendo en cuenta el balance entre beneficios, riesgos y costos, con el propósito de lograr la adhesión y satisfacción de dichos usuarios.
- **Sistema Único de Habilitación:** Es el conjunto de normas, requisitos y procedimientos mediante los cuales se establece, registra, verifica y controla el cumplimiento de las condiciones básicas de capacidad tecnológica y científica, de suficiencia patrimonial y financiera y de capacidad técnico-administrativa, indispensables para la entrada y permanencia en el Sistema, los cuales buscan dar seguridad a los usuarios frente a los potenciales riesgos asociados a la prestación de servicios y son de obligatorio cumplimiento por parte de los Prestadores de Servicios de Salud y las EAPB.
- **Condiciones de Capacidad Tecnológica, Científica y de Infraestructura:** Son los requisitos básicos de estructura y de procesos que deben cumplir los Prestadores de Servicios de Salud por cada uno de los servicios que prestan y que se consideran suficientes y necesarios para reducir los principales riesgos que amenazan la vida o la salud de los usuarios en el marco de la prestación del servicio de salud.
- **Auditoría para el mejoramiento de la calidad de la atención de salud:** Es el mecanismo sistemático y continuo de evaluación y mejoramiento de la calidad observada respecto de la calidad esperada de la atención de salud que reciben los usuarios.

Por la cual se expide al anexo técnico para la implementación de los Sistemas de Control y Vigilancia de que trata la Resolución 13829 de 2014.

- **Software de Gestión de Calidad:** Es una herramienta tecnológica cuyo fin es centralizar, unificar y controlar todas las actividades propias del Sistema de Gestión de Calidad de los CRC a nivel nacional.
- **Comité Técnico:** Es la Instancia asesora del Ministerio de transporte y/o de la Súper Intendencia de Puertos y Transporte, encargada de proponer modificaciones, revisar, actualizar y avalar el esquema de certificación, las metodologías y los documentos que lo respaldan. Esta facultad podrá ser delegada en el proveedor del Sistema.
- **Miembros del Comité Técnico.** Los miembros del comité del esquema de certificación son funcionarios del Ministerio de transporte y/o de la Súper Intendencia de Puertos y Transporte que demuestran competencia para desarrollar, revisar y validar el Esquema de Certificación. Esta facultad podrá ser delegada en el proveedor del Sistema.
- **Método de Evaluación:** El método de evaluación será el regulado en el marco legal vigente. La validación de cada uno de los métodos deberá ser suministrado por el proveedor de los equipos utilizados por el Centro de Reconocimiento de Conductores.
- **Esquema de Certificación:** Requisitos específicos para evaluación y certificación, regulados en la ley 769 de 2002 o el marco legal vigente y desarrollado en el presente anexo, que deben cumplir los aspirantes/pacientes que deseen obtener por primera vez, recategorizar o refrendar su licencia de conducción de vehículos automotores.
- **Condiciones de capacidad tecnológica y científica:** Son los Equipos y Medios Tecnológicos idóneos y requeridos para que cada uno de los CRC pueda desempeñar sus actividades de evaluación conforme a la normatividad vigente.
- **CENTRO DE RECONOCIMIENTO DE CONDUCTORES:** "ARTÍCULO 2o. CENTRO DE RECONOCIMIENTO DE CONDUCTORES. Los Centros de Reconocimiento de Conductores son las instituciones que cuentan con la facultad para realizar la evaluación y certificación de la aptitud psicofísica para conducir.
- **Sistema Integrado de Seguridad:** Es una infraestructura tecnológica operada por cualquier ente público o privado previamente homologado por la Súper Intendencia de Puertos y Transporte, para asegurar el cumplimiento de los parámetros técnicos mínimos que le permita prestar con calidad el servicio para garantizar la expedición segura del certificado de aptitud física mental y de coordinación motriz
- **Validez:** Los proveedores de los equipos e instrumentos utilizados en la evaluación suministrarán la información suficiente donde se garantiza que las pruebas miden lo requerido por el esquema de certificación.
- **Equidad:** El esquema de certificación al ser garantizará por sí mismo la igualdad de oportunidades de éxito a todos los pacientes/aspirantes.
- **Fiabilidad:** La fiabilidad de las evaluaciones, sin perjuicio del evaluador o momento en que se realicen las pruebas, será garantizada por el esquema de certificación toda vez que se aplicarán las mismas formas de evaluación en todos los Centros de Reconocimiento de Conductores a todos pacientes/aspirantes.
- **Desempeño:** Cada Organismo garantizará la forma como el personal cumple con lo establecido en el Esquema de Certificación, a través de la evaluación del desempeño.

Por la cual se expide al anexo técnico para la implementación de los Sistemas de Control y Vigilancia de que trata la Resolución 13829 de 2014.

- **Baremación:** Los baremos iniciales serán suministrados por los proveedores de los diferentes equipos de evaluación y posteriormente El software de gestión ajustará los baremos de aprobación de conformidad con la población específica colombiana.

2.6.3.3.3 Requisitos Generales

2.6.3.3.3.1 Temas Generales

Los centros de reconocimiento de conductores, deberán cumplir con los siguientes documentos que los acreditan como una entidad legal.

- Certificado de existencia y de representación legal de la sociedad.
- Certificado de matrícula mercantil del establecimiento de comercio.
- Formulario de inscripción en el registro especial de prestadores de servicios de salud.
- Certificado de suficiencia patrimonial.
- Balance general suscrito por un contador con tarjeta profesional y fotocopia de la cedula de ciudadanía.
- Concepto de uso de suelos.
- Licencia de construcción.
- Permiso de vertimientos líquidos y de emisiones atmosféricas.
- Sistema de prevención y control de incendios.
- Plan de emergencias y desastres.
- Planes de mantenimiento de la planta física, instalaciones físicas e instalaciones fijas.
- Planes de mantenimiento de los equipos.
- Certificación INVIMA de persona idónea para el mantenimiento de equipos biomédicos.
- Certificación de instalaciones eléctricas, expedida por un ingeniero eléctrico, un técnico SENA en electricidad, donde indique que se la instalación se encuentra actualizada con el Reglamento Técnico Internacional de Instalaciones Eléctricas.

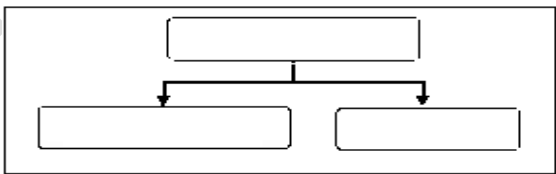
2.6.3.3.3.2 Responsabilidad en Materia de Decisión de la Certificación.

Los Centros de Reconocimiento de Conductores son responsables por las certificaciones que emiten para lo cual deberán contratar bajo su responsabilidad, mediante contrato laboral al personal certificador.

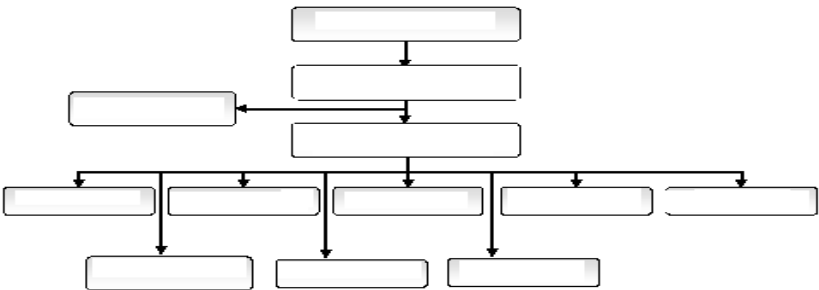
2.6.3.3.3.3 Gestión de la Imparcialidad

2.6.3.3.3.3.1 El organigrama de Los Centros de Reconocimiento de Conductores, deberá respetar como mínimo el siguiente esquema:

ORGANIGRAMA DE LA ALTA DIRECCIÓN DEL OC



Organigrama del Organismo de Certificación de Personas



Por la cual se expide al anexo técnico para la implementación de los Sistemas de Control y Vigilancia de que trata la Resolución 13829 de 2014.

Este será susceptible de ampliaciones de conformidad a las necesidades de la empresa, el mercado, etc.

Los Centros de Reconocimiento de Conductores, implementaran el procedimiento para gestionar la imparcialidad, suministrado por el sistema de gestión de calidad.

Cada Centro de Reconocimiento de Conductores, deberá publicar la declaración por la cual establece la importancia que se da a la imparcialidad en al proceso de evaluación y certificación.

2.6.3.3.3.2 Todo el personal del Centro de Reconocimiento de Conductores, deberán estar sensibilizados en la imparcialidad del proceso, frente a sus solicitantes, candidatos y personas certificadas, por lo que en el área de inducción se deberá capacitar a los evaluadores y certificadores del procedimiento de imparcialidad.

2.6.3.3.3.3 El sistema de gestión de calidad, al contar con procedimientos estandarizados obligatorios para todas las evaluaciones, permite por si solo que el proceso de evaluación y certificación sea equitativo para todos los solicitantes, candidatos y personas certificadas, así mismo no permite establecer algún tipo de restricción para acceder a la certificación y obliga a dar cumplimiento a lo establecido en las normas técnicas y legales vigentes.

2.6.3.3.3.4 Cada Centro de Reconocimiento de Conductores podrá realizar convenios, alianzas o acuerdos comerciales, pero deberá registrar en la matriz de riesgos suministrada por el sistema de gestión de calidad los controles que adelanta para garantizar que los acuerdos comerciales no generan presiones indebidas que afecten la imparcialidad de las certificaciones.

2.6.3.3.3.5 Los centros de reconocimiento de conductores deberán diligenciar la matriz de riesgo, donde se identifican y gestionan las amenazas a la imparcialidad de manera continua y sistemática.

2.6.3.3.3.6 Al ser mandato legal el proceso de certificación se estructuro y gestiono de manera que garantiza y salvaguarda la imparcialidad del proceso de evaluación y certificación.

2.6.3.3.4 Responsabilidad Legal y Financiamiento. *Solamente podrán operar como organismos de certificación de personas quien demuestre tener los recursos financieros suficientes para la operación. Los centros de reconocimiento de conductores deberán realizar un estudio de factibilidad del negocio y del costo de la implementación del mismo para, de acuerdo con los resultados, determinar si cuenta con los recursos financieros suficientes para cubrir la compra o alquiler de equipos biomédicos e informáticos, adecuación de instalaciones, contratación del personal durante por lo menos doce meses, pago de servicios de auditoría y acreditación y demás elementos requeridos para la operación.*

Los centros de reconocimiento de conductores que operan al momento de ser promulgada este documento deberán demostrar la suficiencia patrimonial y financiera requerida por las normas legales vigentes para continuar operando, por lo que el representante legal deberá reportar a la Superintendencia de Puertos y Transporte de la información financiera del costo de su operación en el mes inmediatamente anterior, el precio de venta de cada examen y el valor de otros ingresos, para demostrar que el centro de reconocimiento de conductores es viable económicamente. Esta información será reportada a la DIAN para lo de su competencia.

El incumplimiento durante tres meses continuos de este numeral será causal de suspensión de la acreditación y desconexión del software de gestión hasta tanto demuestre que se encuentra en condiciones económicas y financieras para operar.

Por la cual se expide al anexo técnico para la implementación de los Sistemas de Control y Vigilancia de que trata la Resolución 13829 de 2014.

2.6.3.3.4 REQUISITOS RELATIVOS A LA ESTRUCTURA

2.6.3.3.4.1 Dirección y Estructura de la Organización

2.6.3.3.4.1.1 El Centro de Reconocimiento de Conductores, da cumplimiento a este requisito con el organigrama establecido en el numeral El Centro de Reconocimiento de Conductores, da cumplimiento a este requisito con el organigrama establecido en el numeral 2.6.3.3.3.1.

2.6.3.3.4.1.2 Los individuos responsables de las siguientes actividades son:

- a) Junta de socios o propietario, definen las políticas relativas a la operación del centro de reconocimiento de conductores, aporta el capital inicial o de trabajo
- b) El gerente o representante legal establece los procedimientos requeridos para la operación, contrata personal, realiza seguimientos al cumplimiento de las políticas establecidas por la junta de socios o dueño, gestiona recursos, firma acuerdos, contratos. El responsable del área de calidad que puede ser el mismo gerente/representante legal, implementa el sistema de gestión de calidad única nacional, protocolos, programa de capacitación, programas de mantenimiento de equipos e instalaciones.
- c) El contador es el responsable de las finanzas del organismo de certificación, quien informará al gerente / representante legal de la viabilidad financiera de la operación
- d) El desarrollo y mantenimiento del esquema de certificación está a cargo de la norma legal vigente
- e) Los profesionales en área de la salud como psicología, optometría, fonoaudiología y medicina general serán los responsables de la evaluación
- f) Las decisiones relativas a la certificación estará a cargo de cualquier profesional de la salud.

2.6.3.3.4.2 Estructura del Organismo de Certificación en relación con las actividades de Formación

Este requisito no aplica ya que los Centros de Reconocimiento de Conductores no realizan actividades de formación.

2.6.3.3.5 REQUISITOS RELATIVOS AL PERSONAL

2.6.3.3.5.1 Requisitos Generales al Personal

2.6.3.3.5.1.1 Mínimo una vez al año el Centro de Reconocimiento de Conductores realizara evaluación y seguimiento al desempeño del personal (Recepcionista, psicología, Optometría, Fonoaudiología, medicina general y certificación) que interviene en el proceso de certificación.

Esta evaluación de desempeño debe ser registrada en el software único de gestión en cuanto fecha de realización, resultado de la misma y método empleado.

2.6.3.3.5.1.2 Cada Centro de Reconocimiento de Conductores deberá contar al menos con el siguiente personal para realizar sus actividades de certificación.

Un Psicólogo;
Un Optómetra;
Un Fonoaudiólogo;
Un Médico general
Un profesional de la salud (con función de certificador)
Personal Técnico, administrativo y subalterno que resulte necesario

El Centro de Reconocimiento de Conductores, debe asegurar que el personal evaluador y certificador cuenta con la competencia necesaria, para lo cual el Sistema de Gestión de calidad, cuenta con el procedimiento "Gestión Humana" en el que se establece la metodología para asegurar la competencia del personal.

El Centro de Reconocimiento de Conductores debe asegurar y demostrar que el personal con el que cuenta es suficiente para el volumen de atención que realiza.

Por la cual se expide al anexo técnico para la implementación de los Sistemas de Control y Vigilancia de que trata la Resolución 13829 de 2014.

2.6.3.3.5.1.3 En el software de gestión, se publican los perfiles de cargo en el que se establecen los deberes y responsabilidades de los evaluadores y certificadores.

2.6.3.3.5.1.4 Los Centros de Reconocimiento de Conductores, deben mantener actualizado en su archivo físico los registros que demuestren, calificaciones, formación, experiencia, competencias para el personal evaluador y certificador.

2.6.3.3.5.1.5 El sistema de gestión de calidad cuenta con mecanismos de control que permiten garantizar la confidencialidad de la información que se genera en el proceso de evaluación y certificación de la aptitud psicofísica para conducir.

2.6.3.3.5.1.6 El Centro de Reconocimiento de Conductores, debe contratar laboralmente al personal que interviene en el proceso de evaluación y certificación. Así mismo se deberán realizar las evaluaciones establecidas en la Resolución 2346 de 2007 del Ministerio de la Protección Social.

2.6.3.3.5.1.7 Cuando el Centro de Reconocimiento de Conductores certifique a alguno de sus funcionarios, la evaluación deberá realizarse bajo supervisión para prevenir cualquier conflicto de interés que afecte la imparcialidad de las actividades.

2.6.3.3.5.2 PERSONAL QUE INTERVIENE EN EL PROCESO DE CERTIFICACION

2.6.3.3.5.2.1 Generalidades

El personal que labora en el Centro de Reconocimiento de Conductores debe registrar en el Software de Gestión, las personas hasta tercer grado de consanguinidad y afinidad, para que en el momento que estos soliciten certificación, se realice supervisión de las actividades de evaluación.

2.6.3.3.5.2.2 Requisitos para examinadores.

2.6.3.3.5.2.2.1 El personal evaluador debe cumplir con los siguientes requisitos:

Hoja de vida

- Certificados laborales
- Certificados de estudio
- Diploma universitario
- Acta de grado.
- Carné y/o resolución de inscripción en la seccional de salud que realizara sus funciones.
- Tarjeta profesional para quienes aplique de acuerdo a su fecha de grado.

Posterior al proceso de contratación, se debe realizar una etapa de inducción en la que se asegure que cada evaluador conoce y es capaz de realizar las pruebas requeridas en la normatividad legal vigente para la certificación de la aptitud física mental y de coordinación motriz para conducir.

Esta inducción debe cumplir con el siguiente esquema:

Fase	Inducción	Temas	Responsable	Método
Primera	Información de la empresa	Funciones del cargo, Historia de la empresa, organigrama.	Administrador del centro.	

Por la cual se expide al anexo técnico para la implementación de los Sistemas de Control y Vigilancia de que trata la Resolución 13829 de 2014.

Segunda	Sensibilización en norma ISO/IEC 17024	Se dan a conocer los lineamientos de la norma.	Director de calidad	Presentaciones powerpoint
Tercera	Sensibilización en normatividad vigente para expedir certificados de aptitud psicofísica para conducir e instructivos de evaluación y manejo de equipos.	Fase teórica. Se da conocer la normatividad, pruebas a realizar y criterios de aprobación. Fase práctica. Una vez explicada la parte teórica, se procede a realizar etapa práctica.	Para evaluador y certificador solo puede ser un profesional par que se encargue de esta actividad	Documental y presencial.
Cuarta	Evaluación de la inducción	Se evalúa la adherencia a los temas impartidos.	El responsable de la evaluación debe ser una persona diferente al que dicto la capacitación.	La evaluación de la inducción deber ser realiza en el Software de gestión.

2.6.3.3.5.2.2 Cuando se evidencie que alguno de los funcionarios involucrados en el proceso de evaluación (Recepción, evaluadores, certificador) tiene algún conflicto de interés, el Centro de Reconocimiento de Conductores deberá realizar supervisión de las actividades para evitar que la confidencialidad e imparcialidad de las evaluaciones no se vea afectada. Esta supervisión deberá dejarse registrada.

2.6.3.3.5.2.3 Requisitos relativos a otro personal que interviene en la evaluacion.

El personal administrativo que interviene en el proceso de evaluación y certificación, (calidad, recursos humanos, gerencia) no puede realizar presiones indebidas en los evaluadores y certificadores. De presentarse alguna presión indebida, el profesional deberá registrar el hecho en el espacio de observaciones del Software de gestión único de calidad.

2.6.3.3.5.2.3.1 Contratación externa.

El Centro de Reconocimiento de Conductores debe tener acuerdos documentados con todos los proveedores de productos y servicios relacionados directamente en el proceso de evaluación y certificación en los que se salvaguarde la confidencialidad y se eviten conflictos de interés.

La evaluación no puede ser subcontratada, esta debe ser realizada únicamente por el organismo habilitado y acreditado.

Cuando el organismo de certificación contrata externamente trabajos relacionados con la certificación debe:

- a). Asumir la responsabilidad total por el trabajo contratado externamente.
- b) Asegurarse de que el organismo que realiza los trabajos contratados externamente es competente y cumple las disposiciones aplicables de esta Norma internacional, para lo cual se debe utilizar el formato evaluación de proveedores suministrado por el sistema de gestión de calidad.

Por la cual se expide al anexo técnico para la implementación de los Sistemas de Control y Vigilancia de que trata la Resolución 13829 de 2014.

- c) Evaluar y hacer el seguimiento del desempeño de los organismos que realizan los trabajos contratados externamente de acuerdo con sus procedimientos documentados, para lo cual se debe utilizar el formato reevaluación de proveedores suministrado por el sistema de gestión de calidad.
- d) Tener registros que demuestren que los organismos que realizan los trabajos contratados externamente cumplen todos los requisitos pertinentes del trabajo contratado externamente; y
- e) Mantener una lista de los organismos que realizan trabajos contratados externamente, para lo cual se debe utilizar el formato listado maestro de proveedores suministrado por el sistema de gestión de calidad.

2.6.3.3.5.2.3.2 Otros recursos.

Los Centros de Reconocimiento de Conductores deben realizar las actividades de evaluación y certificación de la aptitud psicofísica para conducir utilizando instalaciones adecuadas, equipos y recursos requeridos en la normatividad legal vigente.

2.6.3.3.5.2.4 Requisitos relativos a los registros y la información.

2.6.3.3.5.2.4.1 Registros de solicitantes, candidatos y personas certificadas.

- Los registros del proceso de evaluación y certificación como informe y certificado se almacenan magnéticamente en el Software único de gestión, y en archivo físico para los Centro de Reconocimiento que deseen imprimir los registros del proceso.
- Los registros de certificación llevaran un consecutivo para cada Centro de Reconocimiento de Conductores, solo podrán acceder a ellos personal autorizado como evaluadores y certificadores con lo cual se salvaguarda la confidencialidad de la información.
- Este numeral no aplica, ya que si una persona certificada pierde alguna de sus facultades no es posible retirar la certificación emitida.

2.6.3.3.5.2.5 Información Pública.

Cada Centro de Reconocimiento de Conductores podrá consultar en cualquier momento si una persona posee una certificación vigente, valida, y su respectivo alcance ingresando al Software de gestión.

2.6.3.3.5.2.5.1 El alcance de las certificaciones de la Aptitud psicofísica para conducir que pueden ser expedidas por los Centros de reconocimiento de conductores son las siguientes:

Categorías del grupo 1 (Particulares)	CATEGORIAS DEL GRUPO 2 (Públicas)
• A1 o 01: Para conducir motocicletas hasta 100 c.c. • A2 o 02: Para conducir motocicletas, motociclos, mototriciclos mayores a 100 c.c. • B1 o 03: Para conducir motocarros, automóviles, camperos, Camionetas y microbuses de servicio particular.	• C1 o 04: Para conducir motocarros, automóviles, camperos, camionetas y microbuses de Servicio público. • B2 o C2 o 05: Para conducir camiones rígidos, busetas y buses de servicios públicos y particular • B3 o C3 o 06: Conducir vehículos articulados de servicio público

El proceso de certificación se realiza teniendo en cuenta el enfoque funcional y deberá ser publicado en las carteleras del Centro de Reconocimiento de Conductores.

SELECCIÓN (Recepción)	Esta etapa comprende el proceso de recepción en el cual se selecciona a los aspirantes que ingresaran a la evaluación para certificar la aptitud psicofísica para conducir.
-----------------------	---

Por la cual se expide al anexo técnico para la implementación de los Sistemas de Control y Vigilancia de que trata la Resolución 13829 de 2014.

	Aquí se deben tener en cuenta los requisitos que se han establecido para ser admitido en el proceso de evaluación y certificación.
DETERMINACIÓN (Evaluación)	Una vez que se ha cumplido con los requisitos definidos en la etapa de selección, se pasa al proceso de determinación que comprende 4 evaluaciones a saber: Psicomotriz Audiometría Visiometría Por último y sin excepción alguna, se realiza la evaluación de medicina general
ATESTACIÓN (Certificación)	Una vez han sido realizadas las 4 evaluaciones citadas en la etapa anterior, un profesional de la salud basado en los criterios de aprobación definidos en la normatividad legal vigente, tomara la decisión de otorgar la certificación de aptitud física mental y de coordinación motriz para conducir. Realizada la atestación, el certificado es publicado a la plataforma del RUNT.

2.6.3.3.5.2.5.2 Los requisitos para acceder al proceso de evaluación y certificación son los siguientes:

Esto deberá estar disponible en las carteleras informativas de cada Centro de Reconocimiento de Conductores.

CATEGORIAS DEL GRUPO 1 (Particulares)	CATEGORIAS DEL GRUPO 2 (Publicas)
• Saber leer y escribir. • Ser mayor de 16 años. • Estar inscrito en el RUNT. • Estar a paz y salvo o contar con acuerdo de pago por concepto de comparendos o multas de tránsito. • Obtener cita previa. • Aportar un PIN como evidencia del pago del costo del examen • Presentar su documento de identificación (original). • Diligenciar el formulario de solicitud • Autorizar el tratamiento de datos sensibles (biométricos y de la salud). • Permitir el registro, autenticación y validación de la huella dactilar de los dedos índice derecho e izquierdo, en todo el proceso de evaluación. • Presentarse con gafas, lentes, audífonos, prótesis o cualquier ayuda que requiera para conducir con seguridad. • Permitir tomar una fotografía. • Estar dispuesto a realizar las pruebas en el orden que se le indique	• Saber leer y escribir. • Ser mayor de 18 años • Estar inscrito en el RUNT. • Estar a paz y salvo o contar con acuerdo de pago por concepto de comparendos o multas de tránsito. • Obtener cita previa. • Aportar un PIN como evidencia del pago del costo del examen • Presentar su documento de identificación (original). • Diligenciar el formulario de solicitud. • Autorizar el tratamiento de datos sensibles (biométricos y de la salud). • Permitir el registro, autenticación y validación de la huella dactilar de los dedos índice derecho e izquierdo, en todo el proceso de evaluación. • Presentarse con gafas, lentes, audífonos, prótesis o cualquier ayuda que requiera para conducir con seguridad. • Permitir tomar una fotografía. • Estar dispuesto a realizar las pruebas en el orden que se le indique

El Centro de Reconocimiento de Conductores debe tener publicidad exacta y no inducir el error a los solicitantes y/o candidatos.

Por la cual se expide al anexo técnico para la implementación de los Sistemas de Control y Vigilancia de que trata la Resolución 13829 de 2014.

2.6.3.3.5.2.6 Confidencialidad

- La divulgación de la información solo podrá realizarse por intermedio del Software de gestión y podrá acceder solo el personal autorizado con usuario y contraseña que son únicas e intransferibles.
- Todo el personal que labora en el Centro de Reconocimiento de Conductores, debe firmar las actas de conflicto de interés, confidencialidad e imparcialidad.
- Las únicas fuentes autorizadas para recibir información sensible de los solicitantes / candidatos es el personal de Recepción, y evaluación (Psicólogo, Optometría, Fonoaudiología, Medicina General). Esta información solo puede ser divulgada por solicitud escrita cuando la ley así lo requiera.
- El Centro de Reconocimiento de Conductores debe registrar en la matriz de riesgos la manera en que asegura que los organismos relacionados no comprometen la confidencialidad.

2.6.3.3.5.2.7 Seguridad.

2.6.3.3.5.2.7.1 Las medidas de seguridad que se deben implementar para evitar las tentativas de fraude durante el proceso de certificación son las siguientes:

- a) Una vez el CRC ha entregado toda su documentación que soporta que es un establecimiento legal, se procederá a crear el CRC y sus usuarios en el software de gestión.
- b) Todos los usuarios del software de gestión, deberán contar de un usuario y contraseña.
- c) El sistema validará que un usuario con el rol de "Médico general/Psicólogo/Fonoaudiólogo/Optómetra/Profesional certificador" se encuentren totalmente enrolados, es decir que hayan cargado su documento de identidad, capturado su información biométrica (Foto, Firma, Huellas) y registrado su información personal. Si no se encuentran enrolados el software de gestión, no se permitirá su ingreso y por lo tanto no podrán participar en el proceso de expedición de un examen médico.
- d) Todos los solicitantes deberán tener una cita previa en un CRC para proceder a realizar un examen médico, el software de gestión valida con el recaudador que el solicitante tenga un PIN valido de lo contrario no se permite la creación de la cita.
- e) Antes de iniciar el proceso de expedición del examen médico el/la recepcionista carga el documento de identidad, captura la información biométrica (Foto, Firma, Huellas) y registra la información personal del solicitante, el software de gestión valida la identidad del solicitante apoyado en RNEC y Centrales de riesgo. Si todas las validaciones son exitosas el software de gestión graba la información del solicitante en una SmartCard que deberá presentar durante todo el proceso.
- f) Durante el proceso de expedición del examen médico cada profesional de la salud y el paciente deberán registrar su huella al inicio y al final de cada prueba y presentar su SmartCard, el software de nacional valida la identidad del paciente y del médico.
- g) Al finalizar el proceso el médico certificador procede a registrar la información del examen ante el RUNT, el software de gestión expone un servicio para que se verifique que la información cargada en la plataforma del RUNT es la misma que se encuentra en la base de datos del software de gestión.
- h) Durante todo el proceso el sistema registra logs de auditoría que posteriormente se analizan con la ayuda de un correlador de eventos para generar alertas que indiquen procedimientos fuera del proceso establecido.

Por la cual se expide al anexo técnico para la implementación de los Sistemas de Control y Vigilancia de que trata la Resolución 13829 de 2014.

2.6.3.3.5.2.7.2 Los exámenes que se aplican para evaluar la aptitud psicofísica para conducir y los rangos de aprobación, están publicados en la normatividad legal vigente, por lo cual todos los aspirantes / candidatos pueden conocer el material de los mismos. Sin embargo se han establecido los siguientes controles:

- a) Para acceder al material de los exámenes cada evaluador debe ingresar al Software de gestión con su respectivo usuario y contraseña.
- b) La naturaleza de los exámenes son electrónicos.
- c) La seguridad se mantiene durante todo el proceso de examen, ya que solo acceden a ellos personal autorizado y que ha firmado acuerdos de confidencialidad e imparcialidad.
- d) No se considera ninguna amenaza por el uso repetido de los exámenes.

2.6.3.3.5.2.7.3 Los Centros de Reconocimiento de Conductores deben evitar las tentativas de fraude en el examen.

- a) Los candidatos al firmar el formulario de solicitud se comprometen a no divulgar los exámenes que se practican ni tomar parte en prácticas fraudulentas.
- b) Los candidatos nunca pueden estar solos en los lugares de evaluación, se requiere de la permanente vigilancia de los evaluadores.
- c) El Software de gestión requiere la confirmación de identidad del aspirante / candidato en todo el proceso de evaluación y certificación. Si la verificación no es satisfactoria, no se puede iniciar el procedimiento.
- d) En la entrada de cada lugar de evaluación se debe colocar un aviso en el que se informe la prohibición de utilizar durante la ejecución de los exámenes aparatos electrónicos como celulares, Tablet, etc.
- e) Los resultados de los exámenes quedan inmodificables una vez han sido guardados en las plantillas del Software de gestión.

2.6.3.3.5.2.8 Esquemas de certificación.

2.6.3.3.5.2.8.1 Los Centros de Reconocimiento de Conductores, deben aplicar el esquema de certificación definido en este documento, el cual está desarrollado con las evaluaciones y lo criterios de aprobación establecidos en la normatividad legal vigente para la expedición del certificado de aptitud psicofísica para conducir.

2.6.3.3.5.2.8.2 El esquema de certificación desarrollado en el Sistema de Gestión de Calidad, contiene:

- a) Alcance de la certificación
El alcance de las certificaciones de la Aptitud psicofísica para conducir que pueden ser expedidas por los Centros de reconocimiento de conductores son las siguientes:

CATEGORIAS DEL GRUPO 1 (Particulares)	CATEGORIAS DEL GRUPO 2 (Públicas)
• A1 o 01: Para conducir motocicletas hasta 100 c.c. • A2 o 02: Para conducir motocicletas, motociclos, mototriciclos mayores a 100 c.c. • B1 o 03: Para conducir motocarros, automóviles, camperos, Camionetas y microbuses de servicio particular.	• C1 o 04: Para conducir motocarros, automóviles, camperos, camionetas y microbuses de Servicio público. • B2 o C2 o 05: Para conducir camiones rígidos, busetas y buses de servicios públicos y particular • B3 o C3 o 06: Conducir vehículos articulados de servicio público

Estos deberán estar publicados en un lugar de fácil visualización.

Por la cual se expide al anexo técnico para la implementación de los Sistemas de Control y Vigilancia de que trata la Resolución 13829 de 2014.

b) Una persona certificada en este esquema ha cumplido con uno de los requisitos para solicitar, renovar o recategorizar la licencia de conducción.

c) Para acceder al proceso de evaluación y certificación, no se requiere de competencia específica, ya que se certifican aptitudes físicas, mentales y de coordinación motriz que posee un individuo.

d) Las Aptitudes que se requieren para obtener la certificación son las establecidas por la normatividad legal vigente como son físicas, mentales y de coordinación motriz para conducir vehículos automotores.

e) Los prerrequisitos son los establecidos en el numeral 7.3.2 de este numeral.

f) El código de conducta que un aspirante y candidato es el siguiente:

1. Es obligación del aspirante o persona certificada mantener un trato cordial y respetuoso no utilizar lenguaje vulgar o soez con las personas que se encuentren dentro de las instalaciones del centro de certificación de personas, en especial hacia el personal administrativo, médicos y profesionales de la salud del centro.

2. Todo aspirante está obligado a no fumar, consumir bebidas alcohólicas o sustancia psicoactivas durante su permanencia en las instalaciones del centro de certificación de personas.

3. Es obligación de todo aspirante NO ofrecer dinero, dadas o sobornos a los profesionales de la salud o cualquier otro funcionario del centro de certificación de personas para cambiar o mejorar los resultados de las evaluaciones psicosenométricas practicadas, so pena de incurrir en prisión.

4. En caso que se requiera alguna información adicional para poder tomar la decisión de certificación, el aspirante está en la obligación de proveerla en un plazo menor a 60 días y de esta manera poder culminar el proceso de certificación.

5. Durante todas las declaraciones, interrogatorios y evaluaciones dadas durante el proceso de certificación el aspirante mantendrá un total apego a la verdad y es consciente de las implicaciones legales que le acarrearán cualquier falta en este aspecto.

6. Está terminantemente prohibido el porte de armas durante la permanencia del aspirante en las instalaciones del centro de certificación de personas.

2.6.3.3.5.2.8.3 Los requisitos del proceso de certificación de la aptitud psicofísica para conducir son los siguientes:

a) Criterios para la certificación inicial y la renovación.

Certificación inicial, Para otorgar un certificado de aptitud psicofísica para conducir, se evalúa al candidato frente a los requisitos establecidos en la normatividad legal vigente los cuales han sido contemplado en este documento.

Renovación de la certificación: No es posible realizar renovación de las certificaciones aptitud psicofísica para conducir, ya que la normatividad que las reglamenta exige realizar la certificación sin tener en cuenta datos históricos, de tal manera que toda certificación se realiza como una solicitud inicial.

b) Métodos de evaluación, debido a que la normatividad legal vigente que reglamenta la expedición de la certificación de la aptitud psicofísica para conducir establece evaluaciones

Por la cual se expide al anexo técnico para la implementación de los Sistemas de Control y Vigilancia de que trata la Resolución 13829 de 2014.

en áreas de la salud como audiometría, visiometría, psicología y medicina general, los métodos de evaluación están definidos propiamente en ellas mismas.

Estos métodos están detallados en los instructivos de evaluación visual, auditiva, psicomotriz y medicina general, los cuales hacen parte integral del sistema de gestión de calidad.

c) Métodos y criterios de vigilancia, suspender y retirar la certificación,

Los criterios de vigilancia, suspensión y retiro de la certificación no aplican, ya que la normatividad legal vigente que reglamenta la expedición de la certificación de la aptitud psicofísica para conducir no los establece.

d) Criterios para efectuar cambios en el alcance o en el nivel de la certificación.

La normatividad legal vigente que reglamenta la expedición de la certificación de la aptitud psicofísica para conducir establece toda certificación como una solicitud inicial, por lo cual una vez emitida la misma no es posible realizar modificaciones en su alcance o nivel ya certificado.

El esquema de certificación al ser propiedad del Estado colombiano, el desarrollo, revisión y validación le corresponde a este .

Los Centros de Reconocimiento de Conductores no son dueños del esquema de certificación de la aptitud psicofísica para conducir, pero deben asegurar que aplica lo establecido en este numeral 8 así como los demás requisitos contemplados en este documento.

2.6.3.3.5.3 REQUISITOS RELATIVOS AL PROCESO DE CERTIFICACION

2.6.3.3.5.3.1 PROCESO DE SOLICITUD

El sistema de gestión de calidad, suministrara a todos los Centros de Reconocimiento de Conductores del país, el formato SOLICITUD, el cual contendrá como mínimo los siguientes elementos:

- Número de PIN
- Nombres y apellidos completos del solicitante
- Fecha de nacimiento AAAA/MM/DD
- Estado civil
- Grupo sanguíneo y RH
- Afiliación a EPS
- Dirección de residencia
- Domicilio
- Teléfono
- Escolaridad
- Categoría
- Tramite
- Autorizaciones y consentimientos:

(1).Acepto cumplir con las disposiciones, obligaciones y deberes pertinentes al esquema de certificación.

(2).Autorizo que la información de mi historia clínica y mis datos personales, biométricos, confidenciales y sensibles, sean tratados, procesados, examinados, verificados y custodiados por el Centro de Reconocimiento de Conductores.

(3) Autorizo el reporte ante el Registro Único Nacional de Tránsito - RUNT del Ministerio de Transporte, solamente el contenido de la información de mi historia clínica que sea requerida para la expedición del mi licencia de conducción.

Por la cual se expide al anexo técnico para la implementación de los Sistemas de Control y Vigilancia de que trata la Resolución 13829 de 2014.

(4) Declaro que haré buen uso del certificado de aptitud expedido por el Centro de Reconocimiento de Conductores y que no presentaré declaraciones relativas a la certificación
(5) Acepto el tratamiento de mis datos sensibles o revisión de la información y registros asociados contenidos en mi historia clínica por: Organismo Nacional de Acreditación de Colombia, Superintendencia de Puertos y Transporte o alguna otra entidad diferente a las autorizadas por Ley? SI _____ NO _____

NOTA: Los datos sensibles son aquellos que afectan la intimidad del titular o cuyo uso indebido pueda generar su discriminación, tales como aquellos que revelen el origen racial o étnico, la orientación política, las condiciones religiosas o filosóficas, la pertenencia a sindicatos, organizaciones sociales, de derechos humanos o que promuevan intereses de cualquier partido político o que garanticen los derechos y garantías de partidos políticos de oposición como los datos relativos a la salud, a la vida sexual y los datos biométricos.

(6) Si al final del proceso de certificación se expide el certificado, me comprometo a informar sin demora sobre cuestiones que puedan afectar mi capacidad para la certificación ofrecida, si este evento ocurre antes de realizar el trámite ante el organismo de tránsito.

(7) Me comprometo a no divulgar ningún material de los exámenes confidenciales realizados, ni tomar parte en prácticas fraudulentas de examen en el CRC.

(8) Me comprometo a no adulterar, falsificar, ni utilizar este certificado y emitir declaraciones de manera engañosa o no autorizada, so pena de responder civil, penalmente ante las autoridades de la Republica de Colombia..

(9) Conozco el procedimiento y evaluaciones medicas de certificación psico-sensométrica que se me van a practicar en el CRC y doy mi CONSENTIMIENTO INFORMADO al CRC para realizar dichas evaluaciones definidas en el esquema de certificación, el cual me ha sido explicado por el personal de recepción del CRC. Asimismo he leído comprendo el esquema de certificación descrito en la cartelera del CRC. Expreso voluntariamente mi intención de participar en las evaluaciones médicas, después de haber comprendido la información que se me ha dado acerca de los objetivos de las evaluaciones, mis derechos y responsabilidades.

(10). Firmo este documento al frente LEGITIMANDO mi capacidad legal para consentir.

En esta etapa del proceso de certificación, el software de gestión validar la identidad de la persona que realiza la solicitud confrontándola contra la réplica de la base de datos del operador de validación biométrica de la Registraduría Nacional del Estado Civil. Registrará en la base de datos la información obtenida de la validación para efectuar las comprobaciones de identidad en cada punto del proceso de evaluación y certificación.

Igualmente en esta etapa se dará a conocer el proceso de certificación, los derechos de los solicitantes y deberes de las personas certificadas y las tarifas

Cada Centro de Reconocimiento de Conductores, deberá verificar la solicitud para confirmar que el solicitante cumple con los requisitos para acceder al proceso de evaluación y certificación de la aptitud psicofísica para conducir.

2.6.3.3.5.3.2 PROCESO DE EVALUACIÓN

El proceso de evaluación establecido en el sistema de gestión de calidad, implementa el esquema de certificación establecido en la norma legal vigente, así:

- Cumplir con los requisitos establecidos en el presente documento para ser admitido en el proceso de certificación.
- El Centro de Reconocimiento de Conductores deberá aplicar los métodos de evaluación definidos en el sistema de gestión.
- Aplicar las evaluaciones valiéndose de personal calificado, medios tecnológicos y sistematizados requeridos para cada evaluación.
- Aplicar criterios de aprobación establecidas en la norma vigente para la certificación de la aptitud psicofísica para conducir.
- Validar la identidad del candidato al inicio y al final de cada prueba
- Validar la identidad del profesional de la salud al inicio y al final de cada prueba

Por la cual se expide al anexo técnico para la implementación de los Sistemas de Control y Vigilancia de que trata la Resolución 13829 de 2014.

- El proceso podrá iniciar por cualquiera de las áreas de optometría, audiometría y psicología.
- Para acceder a la evaluación de medicina general, el candidato deberá haber practicado previamente las evaluaciones de optometría, audiometría y psicología.
- Una vez registradas las primeras cien mil pruebas en el software de gestión, esta herramienta establecerá los tiempos mínimos para cada una de las evaluaciones. En caso de error por parte del evaluador en la utilización del Software de gestión, se deberá generar la evidencia necesaria.
- No se podrá iniciar simultáneamente dos pruebas para el mismo evaluado
- No se podrá iniciar simultáneamente dos pruebas por el mismo evaluador salvo en el área de psicología, en donde se permitirá máximo tres candidatos al mismo tiempo.
- El Centro de Reconocimiento de Conductores deberá garantizar la realización de todas las pruebas establecidas en la normatividad vigente para expedir la certificación de la aptitud psicofísica para conducir.

2.6.3.3.5.3 PROCESO DEL EXAMEN

El proceso del examen establecido en el sistema de gestión de calidad, aplica el esquema de certificación establecido en la norma legal vigente, así:

- El salón destinado para cada uno de los exámenes, deberá contar con un área mínima de 10m² y el menor de los lados deberá medir mínimo 2.5 metros.
- El examen de audiometría deberá realizarse en un medio sonoamortiguado, empleando una cabina insonora.
- El proceso de examen deberá ser realizado por profesionales en cada una de las áreas correspondientes a psicología, optometría, fonoaudiología y medicina general, de conformidad en la norma legal vigente.
- Cada centro de reconocimiento de conductores deberá garantizar la legalidad de los documentos que soporten los evaluadores dispuestos para el examen.
- El examen se debe realizar teniendo en cuenta lo establecido en la norma legal vigente que reglamenta la expedición de la certificación de la aptitud psicofísica para conducir.

2.6.3.3.5.3.4 DECISIÓN DE LA CERTIFICACIÓN

La decisión de certificación debe ser tomada por un profesional de la salud competente e idónea que conoce los rangos de aprobación definidos en el esquema de certificación y que no participe en la evaluación del candidato a certificar.

Esta actividad deberá ser realizada empleando el software de gestión.

Cada Centro de Reconocimiento de Conductores es responsable directo del otorgamiento de la certificación, y por ende conserva su autoridad al respecto sin delegar, o poder delegar, a terceros sus decisiones pertinentes a la certificación.

El Centro de Reconocimiento de Conductores, como organismo de certificación de personas, garantiza el cumplimiento de la normatividad legal vigente sobre las cuales realiza la certificación de personas.

Cada Centro de Reconocimiento de Conductores, deberá emitir un certificado el cual será generado por el Software de gestión y contendrá como mínimo la siguiente información:

Referencia a las normas por las cuales se expide el certificado.
Referencia al organismo de certificación.
NIT del organismo de certificación.
Dirección y teléfono del organismo.
Registro IPS del organismo.
Fecha de expedición y vencimiento.
Registro de habilitación ante el ministerio de transporte.
Número de registro de inscripción ante secretaria de salud.

Por la cual se expide al anexo técnico para la implementación de los Sistemas de Control y Vigilancia de que trata la Resolución 13829 de 2014.

Logo de acreditación del Onac con su respectivo código.

Fotografía del candidato.

Tipo de trámite y categoría certificada.

Servicio solicitado.

Información básica del candidato como nombres, apellidos, número de documento, teléfono, fecha de nacimiento, dirección y ocupación.

Concepto de cada una de las áreas evaluadas.

Firma del certificador.

Firma y huellas de la persona certificada.

2.6.3.3.5.3.5 SUSPENDER, RETIRAR O REDUCIR EL ALCANDE DE LA CERTIFICACIÓN.

Este numeral no es aplicable en el esquema de certificación de la aptitud psicofísica para conducir, ya que la norma legal vigente que lo reglamenta no establece los criterios para suspender, retirar o reducir el alcance de una certificación emitida.

2.6.3.3.5.3.6 PROCESO DE RENOVACION DE LA CERTIFICACIÓN.

La renovación de la certificación no aplica debido a que la norma legal vigente que reglamenta la expedición de la certificación de la aptitud psicofísica para conducir establece evaluaciones de aptitud física, mental y de coordinación motriz, las cuales pueden variar con el tiempo, por ello las condiciones de certificación no se pueden mantener y toda solicitud de certificación debe ser realizada como inicial

2.6.3.3.5.3.7 USO DE CERTIFICADOS LOGOS Y MARCAS.

Los Centros de Reconocimiento de Conductores que proporcionan una marca o logo de certificación, deberán documentar las condiciones de uso y gestionar adecuadamente los derechos de uso y representación.

2.6.3.3.5.3.8 APELACIONES CONTRA DECISIONES DE CERTIFICACION

El sistema de gestión de calidad proporcionará el procedimiento para la gestión de las apelaciones contra las decisiones de certificación en el cual se establece la metodología para recibir, evaluar y tomar decisiones relativas a las apelaciones.

El Centro de Reconocimiento de Conductores deberá entregar a cada apelante un recibido de su solicitud.

En el Software de gestión cada Centro de Reconocimiento de Conductores, deberá registrar las apelaciones que reciba así como su respectivo seguimiento y respuesta.

Este procedimiento debe estar publicado en las carteleras del Centro de Reconocimiento de Conductores.

QUEJAS.

El sistema de gestión de calidad proporcionará el procedimiento para la gestión de las Quejas en el cual se establece la metodología para recibir, evaluar y tomar decisiones relativas a las quejas.

El Centro de Reconocimiento de Conductores deberá entregar a cada persona un recibido de la queja que ha registrado

En el Software de gestión cada Centro de Reconocimiento de Conductores, deberá registrar las quejas que reciba así como su respectivo seguimiento y resolución de la misma.

Este procedimiento debe estar publicado en las carteleras del Centro de Reconocimiento de Conductores.

Por la cual se expide al anexo técnico para la implementación de los Sistemas de Control y Vigilancia de que trata la Resolución 13829 de 2014.

2.6.4 REQUISITOS RELATIVOS AL SISTEMA DE GESTIÓN.

El sistema de gestión se desarrolla siguiendo los lineamientos de la norma NTC ISO/IEC 17024:2013 o su versión vigente, la cual define los requisitos que debe cumplir una organización que se dedica a la certificación de personas.

El Sistema de Gestión de Calidad tendrá una sola estructura documental para todos los Centros de Reconocimiento de Conductores, capaz de apoyar y demostrar el cumplimiento coherente de los requisitos de la norma NTC ISO/IEC 17024:2013.

El Sistema de Gestión de Calidad documenta cada uno de los requisitos aplicables a la norma NTC ISO/IEC 17024:2013, y cuenta con procedimientos para el control de documentos, control de registros, acciones correctivas, acciones preventivas, auditorías internas, y revisión por la dirección.

La divulgación del Sistema de Gestión de Calidad será a través de un acto administrativo de carácter general, emitido por la Súper intendencia de Puertos y Transporte. En igual sentido se divulgarán las actualizaciones o modificaciones.

2.6.4.1 IMPLEMENTACION DEL SISTEMA DE GESTIÓN DE CALIDAD

El Sistema de Gestión de Calidad entrara en vigencia una vez sea promulgado el acto administrativo y tendrá un periodo de transición de máximo 90 días para ser implementado por todos y cada uno de los Centros de Reconocimiento de Conductores. Solamente una vez extinguido este plazo será exigible la implementación del sistema de gestión de calidad por los organismos de acreditación.

2.6.4.2 SEGUIMIENTO AL CUMPLIMIENTO DEL SISTEMA DE GESTION DE

El seguimiento al cumplimiento del sistema de gestión de calidad estará a cargo de la Súper Intendencia de Puertos y Transporte, para lo cual se apoyará en los medios tecnológicos y sistematizados del software de gestión.

Los Centro de Reconocimiento de Conductores serán auditados continuamente por el software de gestión y el CRC que no cumpla con las exigencias establecidas en el sistema de gestión de calidad, será reportado al organismo de control correspondiente para que se tomen las medidas pertinentes.

2.6.4.3. SEGURIDAD.

El Sistema de Gestión de Calidad contará con las siguientes actividades para evitar las tentativas de fraude durante el proceso de evaluación y certificación.

- Se deberá validar la presencia del solicitante/candidato y del personal evaluador durante todo el proceso de evaluación y certificación mediante los protocolos de seguridad definidos por el Ministerio de Transporte.
- El personal evaluador y certificador solo podrá ingresar al Software de Gestión del Sistema de Control y Vigilancia con usuario y contraseña.
- El Software de Gestión del Sistema de Control y Vigilancia deberá garantizar la integridad de los resultados de las evaluaciones realizadas.
- El Software de Gestión del Sistema de Control y Vigilancia no generará usuario al personal evaluador y certificador hasta que se cumplan con los requisitos definidos en el Sistema de Gestión.
- El Sistema de Gestión deberá garantizar la confidencialidad de toda la información que se genere en el proceso de evaluación y certificación.

Por la cual se expide al anexo técnico para la implementación de los Sistemas de Control y Vigilancia de que trata la Resolución 13829 de 2014.

2.6.4.4 SOFTWARE DE GESTIÓN DEL SISTEMA DE CONTROL Y VIGILANCIA

El Software de Gestión del Sistema de Control y Vigilancia, deberá ser un sistema integrado, amigable al usuario final, parametrizable, que permita realizar actualizaciones automáticas.

El Software de Gestión del Sistema de Control y Vigilancia deberá contener los siguientes módulos integrados con las funcionalidades que se describen a continuación:

2.6.4.4.1 Módulo de Agendamiento Único de Citas.

Deberá contener una plataforma web para el solicitante que requiera agendar una cita para el servicio de Examen de Aptitud Física, Mental y de Coordinación Motriz para conductores en los CRCs autorizados.

El solicitante para poder agendar su cita, deberá haber comprado un (1) PIN del servicio para el examen médico de aptitud para conducir 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 al solicitante la búsqueda geográfica de los CRCs autorizados a través de un mapa georreferenciado donde pueda indicar la ubicación donde realizar la dicha búsqueda.

Las plataformas de agendamiento deberán permitir generar el formulario de datos básicos para el diligenciamiento previo al examen al asignar la cita.

Las plataformas de agendamiento deberán permitir verificar, reprogramar o cambiar las citas de los solicitantes. Para reprogramar o cambiar una cita de un solicitante, este lo deberá hacer con una antelación mínima de veinticuatro (24) horas.

2.6.4.4.2 Módulo de Software del Sistema de Gestión de Calidad. Se definirán y validarán las siguientes funcionalidades y requerimientos:

1. Registro del Centro (Nit, Nombre, Matrícula Mercantil, Registro de Prestador, Resolución de Habilitación del Ministerio de Transporte, Registro de Acreditación ante el ONAC y sus anexos) y de los equipos de evaluación (Audiómetros, Visiómetros, Baterías Psicomotrices, fonendoscopios, tensiómetros, entre otros) con su respectiva marca, modelo, referencia y seriales.
2. Registro de las calibraciones de los equipos de cada CRC, de la fecha de calibración y de su vigencia, entidad que expide el certificado o documento de calibración con su soporte. El software deberá llevar el histórico de todas las calibraciones de los equipos.
3. Registro de mantenimientos preventivos y correctivos de los equipos.
4. Registro y control de la verificación diaria de equipos diariamente conforme a lo dispuesto en el Sistema de Gestión de Calidad, generación de alarmas por no realizar el registro de la verificación de los equipos diariamente en los periodos establecidos.
5. Registro de los médicos autorizados por el Ministerio de Transporte con su registro de soporte expedido por dicha Entidad, se deberá incluir el respectivo registro médico de cada profesional o especialista con su respectivo registro ante la Secretaría de Salud en que se encuentra inscrito el profesional de la salud.
6. Además de las de las funcionalidades incorporadas en los demás módulos.

2.6.4.4.3 Módulo de Administración. En este módulo se definirán los Centros de Reconocimiento con datos tales como: NIT, Nombre o Razón de la Empresa, Sedes

Por la cual se expide al anexo técnico para la implementación de los Sistemas de Control y Vigilancia de que trata la Resolución 13829 de 2014.

acreditadas o establecimientos de comercio, ID RUNT, Departamento, Municipio, Zona a la que pertenece, Dirección, Teléfono, Datos del Representante Legal (Tipo ID, No. de ID, Nombres, Apellidos, Registro y Validación de Identidad), Horarios y Cupos de cada sede o establecimiento donde se guardará el soporte del Anexo de la acreditación en su última versión, Resolución de Habilitación del Ministerio de Transporte y su soporte.

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

2.6.4.4.4 Módulo de Enrolamiento o Registro. Se realizará el registro de todos los actores que intervienen en el proceso y de los solicitantes. El registro del solicitante se realizará previa verificación del PIN y de su utilización, se escaneará toda la información del documento de identificación la 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 las huellas de los índices derecho e izquierdo a través de los lectores dispuestos y se enviará al operador tecnológico de la RNEC, la cual responderá con el hit de validación positivo o negativo con su certificación digital y estampado cronológico al Software de Gestión del Sistema de Control y Vigilancia, este grabará la información en el mecanismo redundante que servirá como mecanismo de identificación durante todas las evaluaciones.

2.6.4.4.5 Módulo de Evaluación de Pruebas. En este módulo solo deberán tener permisos de acceso, particulares a su perfil, los médicos o especialistas designados para cada labor y creados previamente por el Representante Legal del CRC. Se realizará la validación de identidad del especialista o médico a través del mecanismo redundante al principio y al final de cada prueba (psicomotriz, auditiva, visión y médica), además del control de los tiempos mínimos de cada prueba y el registro y validación de los criterios de evaluación conforme a lo dispuesto en la resolución 0217 del 2014 del Ministerio de Transporte.

2.6.4.4.6 Módulo de Certificación. En este módulo solo deberán tener permisos de acceso, particulares a su perfil, los médicos designados para esta labor y creados previamente por el Representante Legal del CRC. Se realizará la validación de identidad del médico a través del mecanismo redundante al final de la decisión de certificación del examen. Dentro de las funcionalidades está el verificar el cumplimiento de los criterios de evaluación de cada una de las pruebas realizadas y aprobar o requerir aclaraciones a los especialistas que deberán quedar registrados en el Software de Gestión del Sistema de Control y Vigilancia.

2.6.4.4.7 Expedición del Certificado. En la expedición del certificado de aptitud física, mental y de coordinación motriz realizada por los médicos o especialistas de cada CRC autorizado, serán emitidos a través del Software de Gestión del Sistema de Control y Vigilancia una vez validado todo el proceso.

2.6.5 VISITAS DE VERIFICACIÓN

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.

En la visita se verificará los siguientes requerimientos:

- El centro de operaciones de seguridad deberá contar con un control de acceso biométrico.
- El centro de operaciones de seguridad deberá contar con un sistema de circuito cerrado de televisión.
- El centro de operaciones de seguridad deberá estar ubicada en territorio nacional.
- El centro de operaciones de seguridad deberá contar con un video Wall con mínimo cuatro pantallas.
- Se deberá tener a disposición de los recursos necesarios para poder realizar las verificaciones:

a) 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

Por la cual se expide al anexo técnico para la implementación de los Sistemas de Control y Vigilancia de que trata la Resolución 13829 de 2014.

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.

b) Verificación de información biométrica cifrada. El aspirante deberá mostrar la ubicación en la cual se almacene la información biométrica con el fin de verificar que esta se encuentre cifrada.

c) Verificación de Endpoint. Se deberá demostrar que se encuentran instaladas en los servidores la solución de antimalware.

d) Verificación de mapa de ubicaciones de Centros y máquinas. Se deberá mostrar la ubicación de por lo menos dos centros de reconocimiento en la cual se muestre el estado de su conexión.

e) Verificación de la extracción de la información del documento de identidad.

f) Verificación de tramitación del PIN contra la entidad de recaudo

2.6.5.1 Visita al Centro de Operaciones de Seguridad.

El centro de operaciones de seguridad deberá contar con un control de acceso biométrico.

El centro de operaciones de seguridad deberá contar con un sistema de circuito cerrado de televisión.

El centro de operaciones de seguridad deberá estar ubicada en territorio nacional.

Se deberá tener a disposición de los recursos necesarios para poder realizar las verificaciones:

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.

Verificación en la base de datos de información biométrica cifrada. El aspirante deberá mostrar la ubicación en la cual se almacene la información biométrica con el fin de verificar que esta se encuentre cifrada.

Verificación de Endpoint. Se deberá demostrar que se encuentran instaladas en los servidores la solución de antimalware.

2.6.5.2 Visita a un Centro de Reconocimiento de Conductores.

Se deberá mostrar el funcionamiento del Sistema de Control y Vigilancia. Se procederá a realizar visita a un (1) CRC 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 del examen de aptitud 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 requisitos para poder realizar la prueba. Se verificará además la consulta de validez y consumo de un (1) número PIN con un solicitante y un convenio.

2) Verificación del proceso de enrolamiento y operación de los diferentes actores de los CRCs. Se deberá demostrar que el Software de Gestión del Sistema de Control y Vigilancia, realice el registro de empresas, establecimientos comerciales u organismos certificadores de personas y sus respectivos Representantes Legales, Personal Administrativo, Médicos, Especialistas con su correspondiente perfil y de los solicitantes; así como capturar la información biométrica, biográfica y datos complementarios conforme al Sistema de Gestión de Calidad definido en este documento, a través de los siguientes dispositivos:

i. Lector biométrico de huellas con funcionalidad activa de dedo vivo (LFD), con lector de tarjetas smartcard integrado con módulo SAM para cifrar las comunicaciones entre el lector biométrico de huellas y el Software de Gestión del Sistema de Control y Vigilancia.

Por la cual se expide al anexo técnico para la implementación de los Sistemas de Control y Vigilancia de que trata la Resolución 13829 de 2014.

- ii. Tarjeta Inteligente: Deberá guardar la información biométrica dactilar cifrada y servirá como mecanismo de validación de identidad, a través de una aplicación Match on Card (MoC), de los Médicos y Especialistas del CRC y los solicitantes durante todo el proceso de evaluación y certificación.
- 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 de 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 interno incorporado en cada PC del CRC, 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:

- i. Verificación de la integración con la plataforma del Aliado Operador Biométrico a través de la validación de la template de la huella dactilar capturada en el CRC en el proceso de enrolamiento contra un ambiente de pruebas, verificando pertenecen y NO pertenecen al Médico, Especialista y solicitantes.
- ii. Verificación de la presencia del solicitante y de los médicos o especialistas en todo el proceso de evaluación. Se deberá demostrar que el usuario se valide a través de la huella, al principio y final de cada evaluación, a través del mecanismo redundante que será la tarjeta inteligente o smartcard.
- iii. La aplicación deberá contar con mecanismo alternativo de validación en el proceso de enrolamiento para tramitar las excepciones de solicitantes con discapacidades que no les permita registrar y validar la huella dactilar requerida.

- 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 RNEC para determinar la identidad del solicitante.
- 2. Verifique que la aplicación realice como mínimo cuatro (4) preguntas socio-demográficas del 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 huella dactilar diferente si el 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 solicitante.

- iv. Validación de identidad con el proceso alternativo temporal para tarjetas de identidad "TI" y Cédulas de Extranjería "CE".
 - 1. Compruebe que la aplicación realiza el escaneo del anverso y reverso del documento.
 - 2. Compruebe que la aplicación almacena las imágenes como soporte del documento presentado por el candidato.
 - 3. Compruebe que se extrae la información legible del documento con tecnología de reconocimiento de caracteres "OCR".
 - 4. Verifique que los datos han sido extraídos tanto del anverso como del reverso del documento "TI".
 - 5. Compruebe que existe una extracción de la imagen de la huella dactilar del documento de identidad escaneado.

Por la cual se expide al anexo técnico para la implementación de los Sistemas de Control y Vigilancia de que trata la Resolución 13829 de 2014.

6. Verifique que se obtiene una imagen de la huella dactilar indicada en el documento de identidad con un lector biométrico que posea función activa de captura de dedo vivo.
7. Compruebe que se realiza una comparación de las huellas dactilares (huella extraída de la TI contra la huella capturada por el lector biométrico).

2.6.6 Infraestructura Tecnológica en los CRCs.

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

- Un lector Biométrico de huellas dactilares con lector de tarjetas inteligentes (smartcard) integrado con las siguientes especificaciones:
 1. Tipo de Sensor Óptico, Resolución del Sensor: 500 dpi, Área de captura de la Imagen: 16 x 24 mm o superior, deberá permitir cifrado a través de hardware o software para el intercambio de información entre el lector biométrico de huellas y el lector de tarjetas inteligentes, certificado por el FBI, además deberá tener un módulo SAM. El intercambio de información se realizará bajo metodología match-on-card.
 2. Mínimo de diez (10) tarjetas inteligentes por Centro que se utilizarán como mecanismo redundante de identificación de los solicitantes y de los médicos o especialista para el registro, autenticación y validación biométrica. La información en la tarjeta estará cifrada y dichas tarjetas serán reutilizadas después de terminar cada proceso para el caso de los solicitantes.
 3. 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 CRC donde se asignaron dichos elementos.
 4. Los elementos que sean asignados a un CRC, no podrán ser trasladados de ubicación (a otro CRC u otro lugar).
 5. En los casos de detectar con evidencias el intento de manipulación de los dispositivos y suministros, el proveedor homologado dispondrá de la desconexión del CRC del Sistema e informará a la Superintendencia de Puertos y Transporte y a las autoridades competentes.
- 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 Geoposición. Hardware interno deberá la función de identificar la geo-posición del Centro y PC mediante el uso de tecnología GPS:
 - Sincronización. GPS Mínimo 30 canales, Cobertura Nacional. El sistema de posicionamiento debe garantizar la permanente georreferenciación de la máquina en todo el territorio Nacional.
 - Seguridad. El Representante Legal del CRC 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.
 - Precisión de ubicación. Radio máximo de veinte (20) metros de margen de error en la posición geográfica donde esté ubicada la antena en área urbana y (treinta) 30 metros en área rural en cobertura satelital. Protocolo de comunicación NMEA con sentencias output GSA, RMC y GSV.
 - Actualización máxima de la Geo-referenciación, comunicación celular y/o satelital. Marcación del posicionamiento interno cada 60 minutos.
 - 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.

Por la cual se expide al anexo técnico para la implementación de los Sistemas de Control y Vigilancia de que trata la Resolución 13829 de 2014.

- **Compatibilidad.** Con los prestadores de servicios móviles de comunicación en cuanto a tecnología, cobertura y disponibilidad requerida, existentes mercado.
- Los computadores de los Centros de Reconocimiento de Conductores 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. Una ranura PCI Express (X1) disponible.
 - v. Sistema Operativo Windows 7 o superior.

2.6.7 Compromisos Posteriores

El aspirante a homologarse 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 CRC deberá ser al iniciar la operación como mínimo del 98,5% con base en el horario de atención de los CRC.
2. Antes de entrar en operación 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.

2.6.8 Equipos. Con el objeto de garantizar la calidad d y compatibilidad y funcionamiento, los dispositivos entregados e instalados a los CRC en su operación, tales como lector biométrico de huella dactilar integrado con el lector de tarjetas inteligentes (Smart card), al igual que las tarjetas inteligentes entregadas y el dispositivo de hardware interno incorporado en cada PC, SON DE PROPIEDAD DE CADA PROVEEDOR HOMOLOGADO.