REPÚBLICA DE COLOMBIA

MINISTERIO DE TRANSPORTE

SUPERINTENDENCIA DE PUERTOS Y TRANSPORTE

RESOLUCIÓN No. **DE**

28 MAY 2014 (009699)

"Por la cual se reglamentan las características técnicas del sistema de seguridad documental denominado "Sistema de Control y Vigilancia" para los Centros de Reconocimiento de Conductores para garantizar la legitimidad de los certificados y la protección al usuario de la falsificación y se realiza una derogatoria orgánica sobre la materia".

EL SUPERINTENDENTE DE PUERTOS Y TRANSPORTE

En ejercicio de las facultades constitucionales y legales, en especial las que le confiere el parágrafo del artículo 89° de la Ley 1450 de 2011, dentro del marco de los artículos 41, 42 y 44 del Decreto 101 de 2000, la Ley 105 de 1993, Ley 336 de 1996, entre otras, y

CONSIDERANDO

I. Sobre la obligación de la Superintendencia de Puertos y Transporte de reglamentar las características técnicas del sistema de seguridad documental denominado "Sistema de Control y Vigilancia" para los Centros de Reconocimiento de Conductores para garantizar la legitimidad de los certificados y la protección al usuario de la falsificación.

De conformidad con el artículo 41 del Decreto 101 de 2000, modificado por el Decreto 2741 de 2001 se delega en la Superintendencia de Puertos y Transporte "**Supertransporte",** la función de inspeccionar, vigilar y controlar la aplicación y el cumplimiento de las normas que rigen el sistema de tránsito y transporte.

Acorde con lo preceptuado en el parágrafo 3 del artículo 3 de la Ley 769 de 2002 la Superintendencia de Puertos y Transporte tiene la función de vigilar y controlar a *"Las autoridades, los organismos de tránsito, las entidades públicas o privadas que constituyan organismos de apoyo".*

La ley 769 de 2002 establece como principios rectores del Tránsito Terrestre a nivel nacional *"la seguridad de los usuarios, la calidad, la oportunidad, el cubrimiento, la*

"Por la cual se reglamentan las características técnicas del sistema de seguridad documental denominado "sistema de control y vigilancia" para los Centros de Reconocimiento de Conductores para garantizar la legitimidad de los certificados y la protección al usuario de la falsificación y se realiza una derogatoria orgánica sobre la materia".

libertad de acceso, la plena identificación, la libre circulación, la educación y la descentralización", preceptos conforme a los cuales se identifican las actividades que deben desarrollarse en los Centros de Reconocimiento de Conductores.

De acuerdo a los requisitos establecidos en el artículo 19 de la Ley 769 de 2002 (modificado por el artículo 5° de la Ley 1383 de 2010, modificado por el artículo 3 de la Ley 1397 de 2010 y por el artículo 196 del Decreto ley 019 de 2012) para la obtención de la licencia de conducción para vehículos automotores se requiere:

> *"e. Presentar certificado de aptitud física, mental y de coordinación motriz para conducir expedido por una Institución Prestadora de Salud o por un Centro de Reconocimiento de Conductores, de conformidad con la reglamentación que expida el Ministerio."*

En concordancia con el parágrafo de la norma en cita, se establece como uno de los requisitos para obtener la licencia de conducción por primera vez, la recategorización, o la renovación de la misma, el demostrar ante las autoridades de tránsito la aptitud física, mental y de coordinación motriz, valiéndose para su valoración de los medios tecnológicos sistematizados y digitalizados requeridos, que permitan medir y evaluar dentro de los rangos establecidos por el Ministerio de Transporte según los parámetros y límites internacionales, entre otros: la capacidad de visión y orientación auditiva, la agudeza visual y campimetría, los tiempos de reacción y recuperación al encandilamiento, la capacidad de coordinación entre la aceleración y el frenado, la coordinación integral motriz de la persona, la discriminación de colores y la phoria horizontal y vertical.

De conformidad con lo anterior, y de acuerdo a las facultades conferidas en el parágrafo del artículo 89 de la ley 1450 de 2011 mediante la cual se expide el Plan Nacional de Desarrollo 2010-2014, la Superintendencia de Puertos y Transporte está en la obligación de reglamentar las características técnicas de los sistemas de seguridad que deberán implementar cada uno de los vigilados, para que se garantice la legitimidad de esos certificados y se proteja al usuario de la falsificación.

Por lo enunciado, se hizo necesario expedir dicha reglamentación con base en sólidos estudios técnicos sobre el particular determinando qué condiciones técnicas mínimas deben implementar aquellos vigilados que emiten certificados, para que de esta manera se garantice la legitimidad y la autenticidad de los mismos.

De suerte que, en ejercicio de las facultades conferidas por el parágrafo del artículo 89° de la Ley 1450 de 2011 la Superintendencia de Puertos y Transporte expidió las siguientes resoluciones:

1. **Resolución N° 7034 de 2012** *"Por la cual se reglamentan las características técnicas de los sistemas de seguridad de los Centros de Reconocimiento de Conductores, garantizando la legitimidad de los certificados y la protección al usuario de la falsificación."*

   Esta resolución tenía por objeto determinar en todo el territorio nacional la reglamentación de las características técnicas del sistema de seguridad que deben aplicar a los Centros de Reconocimiento de Conductores.

   Así mismo, está Resolución implementa el sistema de control y vigilancia, implementa un sistema de captura de video, y establece el término para la

"Por la cual se reglamentan las características técnicas del sistema de seguridad documental denominado "sistema de control y vigilancia" para los Centros de Reconocimiento de Conductores para garantizar la legitimidad de los certificados y la protección al usuario de la falsificación y se realiza una derogatoria orgánica sobre la materia".

implementación y aplicación de los Sistemas de Control y Vigilancia por parte de todos los Centros de Reconocimiento de Conductores y para la implementación y aplicación del Sistema de Captura de Video.

Adicionalmente, la Resolución en mención ordena expedir un anexo técnico para la homologación de los sistemas de Control y Vigilancia, entre otros aspectos.

2. **Resolución N° 191 de 2013** *"Por la cual se expide al anexo técnico para la homologación de los sistemas de Control y Vigilancia ordenado a través de la Resolución 7034 del 17 de octubre de 2012 y se modifica el término para su exigibilidad."*

Por medio de esta Resolución se expide el anexo técnico para la homologación de los sistemas de Control y Vigilancia ordenado a través de la Resolución 7034 del 17 de octubre de 2012 proferida por la Superintendencia de Puertos y Transporte, entre otros aspectos.

3. **Resolución N° 917 de 2014** *"Por la cual se suspenden parcial y temporalmente algunos artículos contenidos en la Resolución 7034 expedida por este despacho el 17 de octubre de 2012 y se dictan otras disposiciones".*

Como consecuencia de las notorias dificultades que se evidenciaron en el desarrollo de las actividades propias de los Centros de Reconocimiento de Conductores (CRC) asociadas con la implementación del sistema adoptado por la Resolución N° 7034 de 2012, fue necesario evaluar y verificar su funcionamiento, ello sin afectar los intereses de los usuarios que a todas luces son los destinatarios finales de toda esta reglamentación.

Con lo recopilado por esta entidad en su momento, llámese quejas, reclamos o peticiones así como hechos notorios, los y las cuales fueron corroboradas y que son de público conocimiento, se logró evidenciar que un sin número de quejas provenientes de solicitudes ciudadanas referentes a la prestación del servicio de los organismos de apoyo (el 47% de las quejas recepcionadas) y otras tantas provenientes de los propios centros de reconocimiento y que versan sobre presuntas dificultades en la puesta en funcionamiento del procedimiento establecido en la Resolución N° 7034 de 2012 que instituyó el sistema de control y vigilancia (el 53% restantes de las quejas).

Todo lo anterior ratificó la obligación de la Superintendencia de Puertos y Transporte de tomar las medidas contingentes y cautelares necesarias tendientes a garantizar la eficiente prestación del servicio público ofrecido por los Centros de Reconocimiento de Conductores (CRC), así como la correspondiente vigilancia de esta Superintendencia.

De suerte que, mediante la Resolución N° 917 de 2014 se resolvió lo siguiente:

> ***"Artículo 1.*** *Suspéndase hasta por dos meses contados a partir de la vigencia de la presente resolución, los efectos de los numerales 2, 3, 4, 5, 6, 7, 8 y 9, el parágrafo 1 y el segundo párrafo del parágrafo 2 del artículo 3, los artículos 4, 5 y 6 y el anexo técnico de la resolución 7034 de 2012 emanada de esta Superintendencia.*

"Por la cual se reglamentan las características técnicas del sistema de seguridad documental denominado "sistema de control y vigilancia" para los Centros de Reconocimiento de Conductores para garantizar la legitimidad de los certificados y la protección al usuario de la falsificación y se realiza una derogatoria orgánica sobre la materia".

> ***Artículo 2.*** *Suspéndase en los mismos términos del artículo anterior, de manera parcial lo previsto en el numeral primero del artículo 3 de la resolución 7034 de 2012, en lo que tiene que ver con la trazabilidad y correlación del pago que se efectúa mediante la entidad financiera. Entiéndase que los pagos deberán seguir siendo efectuados por medio del sistema financiero, sin que esto implique entonces que se deba entrelazar el mismo por medio del sistema de seguridad y vigilancia."*

4. **Resolución N° 2193 de 2014** *"Por medio de la cual se modifica parcialmente la Resolución No. 191 del 25 de enero de 2013, relacionada con la expedición del anexo técnico para la homologación de los sistemas de control y vigilancia ordenada a través de la Resolución 7034 del 17 de octubre de 2012; se da aplicación a las Resoluciones 917 del 27 de enero de 2014 expedida por la Superintendencia de Puertos y Transporte y, la Resolución 217 del 31 de enero de 2014 expedida por el Ministerio de Transporte; y se dictan otras disposiciones".*

Teniendo en cuenta que se debía articular la reglamentación proferida por esta Superintendencia en lo que hace a **la expedición del anexo técnico para la homologación de los sistemas de control y vigilancia ordenada a través de la Resolución N° 7034 del 17 de octubre de 2012, desarrollada mediante la Resolución N° 191 del 25 de enero de 2013** al amparo de lo señalado por el Ministerio de Transporte a través de la Resolución N° 217 del 31 de enero de 2014 y con fundamento en los documentos técnicos y jurídicos recogidos por la Superintendencia y, acudiendo al estudio integral que realizó el despacho del Superintendente Delegado de Tránsito y Transporte Terrestre Automotor en relación con el funcionamiento de los Centros de Reconocimiento de Conductores (CRC) y en especial el anexo técnico contenido en la Resolución N° 191 del 25 de enero de 2013 expedido por esta entidad, este despacho procedió a expedir la Resolución N° 2193 de 2014.

De conformidad con lo anterior, la Resolución N° 2193 de 2014: (i) Modifica el anexo técnico determinado en el artículo 1° de la Resolución N° 191 de 2013, (iii) En particular, modifica el anexo técnico de la Resolución N° 191 de 2013 en los requisitos financieros y en los requisitos documentales, (iii) Incluye dentro del Texto de la Resolución N° 7034 de 2012 algunos artículos, y (iv) Restablece los efectos jurídicos de algunos de los artículos suspendidos mediante Resolución N° 917 de 2014, entre otros aspectos.

5. **Resolución N° 4980 de 2014** *"Por medio de la cual se modifica la Resolución No. 2193 del 12 de febrero de 2014, y la Resolución 7034 de 2012".*

En razón al proceso de diagnóstico operativo del Sistema de Control y Vigilancia efectuado por la Superintendencia de Puertos y Transporte y debido a las fallas que se han presentado en la ejecución de dicho sistema, se realizaron unas mesas de trabajo con los diversos actores públicos y/o privados interesados, en las cuales se concluyó que era necesario modificar la Resolución N° 7034 de 2012 y la Resolución N° 2193 de 2014.

Como consecuencia de lo anterior, la Resolución N° 4980 de 2014 modifica los Requisitos del Sistema de Control y Vigilancia establecidos en la Resolución N° 7034 de 2012 (Artículo 3°) y se modifica el Artículo Cuarto de la Resolución 2193 de 2014 el cual quedó así:

"Por la cual se reglamentan las características técnicas del sistema de seguridad documental denominado "sistema de control y vigilancia" para los Centros de Reconocimiento de Conductores para garantizar la legitimidad de los certificados y la protección al usuario de la falsificación y se realiza una derogatoria orgánica sobre la materia".

> *"ARTICULO CUARTO: Restablézcase los efectos jurídicos de los artículos 4 y 5 y elimínese el artículo 6 con el respectivo anexo técnico de la Resolución 7034 de 2012."*

Conclusión Parcial.

En ejercicio de las facultades conferidas en el parágrafo del artículo 89° de la Ley 1450 de 2011 y atendiendo la obligación de la Superintendencia de Puertos y Transporte de reglamentar las características técnicas del sistema de seguridad documental para los Centros de Reconocimiento de Conductores buscando garantizar la legitimidad de los certificados y la protección al usuario de la falsificación, esta Superintendencia expidió las siguientes resoluciones: (i) Resolución N° 7034 de 2012, (ii) Resolución N° 191 de 2013, (iii) Resolución N° 917 de 2014, (iv) Resolución N° 2193 de 2014 y (v) Resolución N° 4980 de 2014, las cuales se actualizan, armonizan y se dejan en un solo texto normativo mediante el presente acto administrativo conforme lo ordenado por este mismo despacho.

Ahora bien, para proceder a la mencionada actualización, armonización y con el objetivo de dejar todas las Resoluciones mencionadas en un sólo cuerpo normativo se hace necesario efectuar una derogatoria orgánica.

II. **Sobre la obligación de la Superintendencia de Puertos y Transporte de efectuar una derogatoria orgánica.**

El Artículo Sexto de la Resolución N° 2193 de 2014 *"Por medio de la cual se modifica parcialmente la Resolución No. 191 del 25 de enero de 2013, relacionada con la expedición del anexo técnico para la homologación de los sistemas de control y vigilancia ordenada a través de la Resolución 7034 del 17 de octubre de 2012; se da aplicación a las Resoluciones 917 del 27 de enero de 2014 expedida por la Superintendencia de Puertos y Transporte y, la Resolución 217 del 31 de enero de 2014 expedida por el Ministerio de Transporte; y se dictan otras disposiciones"* establece:

> *"**Ordénese** al Despacho de la Delegada de Tránsito y Transporte Terrestre Automotor de esta Superintendencia para que en un término máximo de 2 meses contados a partir de la ejecutoria de la presente resolución, actualice, armonice y deje en un solo texto normativo la Resolución No. 7034 de 2012 expedida por esta entidad y de que trata este acto administrativo, para que conste de manera articulada y en un único cuerpo normativo las modificaciones contenidas en el presente acto administrativo".*

De conformidad con lo ordenado en el artículo en cita, el Despacho de la Delegada de Tránsito y Transporte Terrestre Automotor efectuó un estudio de racionalización normativa que buscó superar las dificultades de inflación reglamentaria, dispersión normativa, des legitimización del ordenamiento, incertidumbre institucional y baja duración de la vigencia de las Resoluciones.

En el estudio efectuado por el Despacho de la Delegada de Tránsito y Transporte Terrestre Automotor se efectuó una revisión de las Resoluciones 7034, 191, 917, 2193 y 4980 en cita y expedidas por la Superintendencia de Puertos y Transporte para contribuir al propósito de racionalizar e integrar en un único cuerpo normativo las características técnicas del sistema de seguridad documental denominado

"Por la cual se reglamentan las características técnicas del sistema de seguridad documental denominado "sistema de control y vigilancia" para los Centros de Reconocimiento de Conductores para garantizar la legitimidad de los certificados y la protección al usuario de la falsificación y se realiza una derogatoria orgánica sobre la materia".

"Sistema de Control y Vigilancia" para los Centros de Reconocimiento de Conductores.

El estudio en mención pretendió, de una parte, realizar un análisis para determinar qué artículos están vigentes y cuáles, por derogación, expresa o tácita, subrogación o modificación, deben ser retirados del ordenamiento jurídico; y por otra, crear herramientas jurídicas y técnicas que permitan crear y mantener en esta Superintendencia una reglamentación de conformidad con lo ordenado en el parágrafo del artículo 89° de la Ley 1450 de 2011.

Con todo, el resultado del estudio efectuado es la expedición de la presente Resolución que busca ser coherente, simple y sobretodo, acercar al ciudadano y a quienes tienen la obligación y responsabilidad de aplicar el conjunto de reglas que rigen las características técnicas del sistema de seguridad documental denominado "Sistema de Control y Vigilancia" para los Centros de Reconocimiento de Conductores.

Ahora bien, como quiera que la orden del Artículo Sexto de la Resolución N° 2193 de 2014 es actualizar, armonizar y dejar en un sólo texto normativo todas las disposiciones relacionadas con las características técnicas del sistema de seguridad documental denominado "Sistema de Control y Vigilancia" para los Centros de Reconocimiento de Conductores, es necesario efectuar una **derogatoria orgánica.**

Sobre la derogatoria de las normas y su función, la Corte Constitucional se ha pronunciado un sin número de veces. Ejemplo de ello es la **Sentencia C-901/11** con ponencia del Dr. Jorge Iván Palacio Palacio, en la que se estableció sobre este particular mecanismo, lo siguiente:

> *"La derogación tiene como función "dejar sin efecto el deber ser de otra norma, expulsándola del ordenamiento. Por ello se ha entendido que la derogación es la cesación de la vigencia de una disposición como efecto de una norma posterior", que no se fundamenta en un cuestionamiento sobre la validez de la normas, por ejemplo, cuando es declarada inexequible, "sino en criterios de oportunidad libremente evaluados por las autoridades competentes (…).*
>
> *(..) En la sentencia C-159 de 2004 examinó la constitucionalidad de los artículos 71 y 72 del Código Civil, que contemplan la figura de la derogación clasificándola en expresa y tácita, como también se refirió al artículo 3º de la Ley 153 de 1887 que establece la derogación orgánica. Señaló que en* ***la derogación expresa*** *el legislador determina de manera precisa el o los artículos que retira del ordenamiento, por lo que no se hace necesaria ninguna interpretación, ya que simplemente se cumple una función de exclusión desde el momento que así se establezca. La* ***derogación orgánica*** *refiere a cuando la nueva ley regula integralmente la materia, que en términos de la Corte Suprema de Justicia supone "que la nueva ley realiza una mejora en relación con la ley antigua; que aquella es más adecuada a la vida social de la época y que, por tanto, responde mejor al ideal de justicia, que torna urgente la aplicación de la nueva ley; […] que por lo mismo debe ser lo más amplia posible para que desaparezcan las situaciones que el propio legislador ha querido condenar y evidentemente arrasó con la ley nueva".*
>
> *Por su parte, la* ***derogación tácita*** *obedece a un cambio de legislación, a la existencia de una incompatibilidad entre la ley anterior y la nueva ley, lo cual hace indispensable la interpretación de ambas leyes para establecer la vigente en la materia o si la* ***derogación es parcial o total.*** *Tiene como efecto limitar en el tiempo la vigencia de una norma, es decir, suspender su*

"Por la cual se reglamentan las características técnicas del sistema de seguridad documental denominado "sistema de control y vigilancia" para los Centros de Reconocimiento de Conductores para garantizar la legitimidad de los certificados y la protección al usuario de la falsificación y se realiza una derogatoria orgánica sobre la materia".

> *aplicación y capacidad regulatoria, aunque en todo caso el precepto sigue amparado por una presunción de validez respecto de las situaciones ocurridas durante su vigencia. Cuando se deroga tácitamente una disposición no se está frente a una omisión del legislador sino que al crear una nueva norma ha decidido que la anterior deje de aplicarse siempre que no pueda conciliarse con la recientemente aprobada. Así lo ha sostenido la Corte al indicar que "la derogación no siempre puede ser expresa, pues ello implicaría confrontar cada nueva ley con el resto del ordenamiento. Es decir, se le exigiría al Congreso una dispendiosa labor que no tiene razón de ser, pues la tarea legislativa se concentra en asuntos específicos definidos por el propio Congreso, con el objeto de brindar a los destinatarios de las leyes seguridad jurídica y un adecuado marco para la interpretación y aplicación de las mismas (v. gr. sentencia C-025 de 1993)".*
>
> *Además, para que sea posible la derogación debe darse por otra de igual o superior jerarquía.* ***Entonces, la derogación tácita es aquella que surge de la incompatibilidad entre la nueva ley y las disposiciones de la antigua****, que suele originarse en una declaración genérica en la cual se dispone la supresión de todas las normas que resulten contrarias a la expedida con ulterioridad.". (Resaltado fuera de texto)*

De modo que, existen tres tipos de derogación:

1. **Derogación Expresa:** Cuando de manera precisa se establece él o los artículos que se retiran del ordenamiento. En este tipo de derogación no hace falta ninguna interpretación, ya que simplemente se cumple una función de exclusión desde el momento que así se establezca.
2. **Derogación Tácita:** Cuando se presenta una incompatibilidad entre la norma anterior y la nueva norma, lo cual hace indispensable la interpretación de ambas normas para establecer la vigente en la materia o si la derogación es parcial o total.
3. **Derogación Orgánica:** Cuando la nueva norma regula integralmente la materia excluyendo del ordenamiento jurídico todas las anteriores sobre susodichos asuntos.

Tal y como se mencionó, la presente Resolución pretende dejar en único cuerpo normativo la reglamentación sobre las características técnicas del sistema de seguridad documental denominado "Sistema de Control y Vigilancia" para los Centros de Reconocimiento de Conductores en cumplimiento de las facultades conferidas en el parágrafo del artículo 89° de la Ley 1450 de 2011. De modo que, en últimas, lo que se lleva a cabo mediante el presente acto administrativo es una derogatoria orgánica.

El ejercicio que de la derogatoria orgánica se efectúa mediante la presente Resolución pretende evitar futuras quejas, reclamos, dificultades, inconformidades y disgustos, tanto de los ciudadanos y usuarios, como de los propios Centros de Reconocimiento.

Así mismo, la presente Resolución materializa el principio de buena fe administrativa que se deriva del principio de racionalidad y objetividad el cual debe conducir a la Administración en sus relaciones internas y en sus relaciones con los ciudadanos[1].

[1] RODRÍGUEZ – ARANA MUÑOZ. Aproximación al Derecho Administrativo Constitucional.

"Por la cual se reglamentan las características técnicas del sistema de seguridad documental denominado "sistema de control y vigilancia" para los Centros de Reconocimiento de Conductores para garantizar la legitimidad de los certificados y la protección al usuario de la falsificación y se realiza una derogatoria orgánica sobre la materia".

III. Contenido de la presente Resolución.

La presente Resolución contiene toda la reglamentación del parágrafo del artículo 89° de la Ley 1450 de 2011 y determina las condiciones técnicas mínimas que deben implementar aquellos vigilados que emiten certificados, para que de esta manera se garantice la legitimidad y la autenticidad de los mismos.

Con el fin de garantizar una mayor calidad y transparencia en el proceso de expedición de los certificados por parte de los Centros de Reconocimiento de Conductores, es necesario que los mismos adopten las disposiciones técnicas mínimas requeridas por esta Superintendencia.

De acuerdo a lo dicho y en aplicación a los principios contenidos en el artículo 209 de la Constitución Política, el artículo 3 de la ley 1437 de 2011 (Código de Procedimiento Administrativo y de lo Contencioso Administrativo) y los contenidos en el artículo 3 de la ley 489 de 1998, especialmente los de coordinación, celeridad, economía, eficacia y eficiencia, la reglamentación técnica que deben adoptar los vigilados que emitan certificados conforme se solicita en el parágrafo del artículo 89 de la ley 1450 de 2011, debe tener en cuenta lineamientos que les faciliten adaptarse a sus nuevas obligaciones legales, las cuales se orientan a dar efectividad y seguridad al proceso del registro y expedición del Certificado de Aptitud física, mental y de coordinación motriz.

De igual forma, es necesario indicar que para garantizar dicha seguridad se requiere de la adecuación, implementación y uso de elementos técnicos que generen un esquema de seguridad, mediante el desarrollo de procedimientos que permitan dar credibilidad y certeza que los certificados expedidos fueron emitidos conforme lo ha establecido en la normatividad colombiana, protegiendo a los usuarios y tutelando los principios cardinales en materia de tránsito y transporte terrestre, particularmente los de seguridad y calidad en la prestación del servicio.

Todo el precedente análisis, más la infinidad de reuniones con los CRC; más la verificación de las quejas, reclamos, noticias y hechos notorios; más los estudios técnicos del caso y por sobre todo el análisis de derogatoria orgánica que hace parte del presente expediente y que reposa en los archivos de la entidad, sirvieron al Superintendente Delegado de Tránsito y Transporte Terrestre Automotor para proyectar el presente acto administrativo que hoy se expide mediante la presente Resolución.

En mérito de lo anteriormente expuesto el Superintendente de Puertos y Transporte.

RESUELVE:

Capítulo I

Objeto y ámbito de aplicación

Artículo 1º. Objeto y ámbito de aplicación. El objeto de la presente Resolución es reglamentar las características técnicas del sistema de seguridad documental denominado "Sistema de Control y Vigilancia" para los Centros de Reconocimiento de

"Por la cual se reglamentan las características técnicas del sistema de seguridad documental denominado "sistema de control y vigilancia" para los Centros de Reconocimiento de Conductores para garantizar la legitimidad de los certificados y la protección al usuario de la falsificación y se realiza una derogatoria orgánica sobre la materia".

Conductores en todo el territorio nacional para garantizar la legitimidad de los certificados y la protección al usuario de la falsificación y realizar una derogatoria orgánica sobre la materia.

Capítulo II

Implementación del Sistema de Control y Vigilancia

Articulo 2º. Sistema de Control y Vigilancia. El Sistema de Control y Vigilancia es una infraestructura tecnológica operada por cualquier ente público o privado previamente validado por la Superintendencia de Puertos y Transporte, o por quien esta delegue, para asegurar el cumplimiento de los parámetros técnicos mínimos y de otra índole dictados en la presente Resolución y de los que se fijen posteriormente, que le permita prestar con calidad el servicio para garantizar la expedición segura del certificado de aptitud física mental y de coordinación motriz; la presencia del candidato en el Centro de Reconocimiento de Conductores; la realización de las pruebas y evaluaciones por los médicos o especialistas; que el certificado se expida desde la ubicación geográfica del Centro de Reconocimiento de Conductores; 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 de pago; la correlación o trazabilidad para el cruce de información y que estén conectados con el centro de monitoreo de la Superintendencia de Puertos y Transporte, el actor del Sistema Financiero y el RUNT.

Articulo 3º. Requisitos del Sistema de Control y Vigilancia. Para la realización de los exámenes de aptitud física, mental y de coordinación motriz, todos los Centros de Reconocimiento de Conductores en virtud del parágrafo del artículo 89 de la ley 1450 del 2011, deberán dar cumplimiento a los siguientes protocolos de seguridad:

1. Los Centros de Reconocimiento de Conductores garantizarán el registro del pago mediante un actor del sector financiero debidamente vigilado por la Superintendencia Financiera de Colombia, con cobertura nacional quien llevará una base de datos de todos los pagos y su utilización por el servicio de los certificados médicos expedidos por los Centros de Reconocimiento, la cual debe tener correlación o trazabilidad para el cruce de información con el centro de monitoreo de la Superintendencia de Puertos y Transporte. Así mismo, la entidad financiera y el Centro de Reconocimiento deberán permitir a la Superintendencia de Puertos y Transporte la consulta en línea de los registros de pagos realizados a través del respectivo actor del sector financiero. Se permitirán diferentes canales de pago, siempre y cuando sea a través del sector financiero, con compra del PIN asociado a la cédula de Ciudadanía.

2. Los Centros de Reconocimiento de Conductores deberán implementar un sistema de agendamiento nacional que permita, ordenar y centralizar el proceso de atención a los usuarios en cada Centro de Reconocimiento de Conductores, así como permitir que la Superintendencia de Puertos y Transporte pueda verificar el cumplimiento de dicho ejercicio de agendamiento. La cita sólo podrá ser programada con el PIN de recaudo a través de un sistema electrónico de asignación de citas, que deberá cobijar aspectos tales como: Sitio web centralizado de agendamiento, configuración de datos, disponibilidad del Centro

"Por la cual se reglamentan las características técnicas del sistema de seguridad documental denominado "sistema de control y vigilancia" para los Centros de Reconocimiento de Conductores para garantizar la legitimidad de los certificados y la protección al usuario de la falsificación y se realiza una derogatoria orgánica sobre la materia".

de Reconocimiento de Conductores, registro de citas, opción de peticiones quejas y reclamos, reprogramación o cambio de cita y una línea nacional de información para los usuarios, según lo dispuesto por la Resolución N° 217 de 2104 expedida por el Ministerio de Transporte.

3. Integrar el sistema único de agendamiento con el sistema de pagos del sector financiero para validar que toda asignación de cita tenga un pago correspondiente al examen médico.

4. Registrar y validar al ciudadano a través del documento de identidad original o Contraseña, cuando fuera el caso, tomando su información al inicio de las pruebas con lectores de código de barras. Así mismo, el prestador del servicio realizará una validación del registro de pago, con captura de huella con funcionalidad activa de dedo vivo, así como retratar al aspirante o candidato mediante fotografía y tomará un registro digital de la firma manuscrita.

5. La foto del usuario será capturada a través de una cámara con sensor digital de alta definición, que produzca imágenes nítidas con un alto grado de detalle, con el fin de identificar a la persona aspirante. Dicha cámara debe cumplir con estándar ISO/IEC19794-5 (Information Tecnology – Biometric Data Interchange Formats – Face Image Data).

6. El Sistema de Control y Vigilancia deberá integrarse con el sistema de agendamiento con el fin de verificar el cumplimiento de todos los pasos previos a la realización de los exámenes médicos, a saber: compra del PIN y asignación de cita mediante el proceso de agendamiento, según lo dispuesto por la Resolución N° 217 de 2104 expedida por el Ministerio de Transporte.

7. Los especialistas y médicos de cada Centro de Reconocimiento de Conductores deberán ser registrados al inicio de su contrato como requisito previo para la realización de la actividad. De igual manera, la misma actividad descrita deberá surtirse al haber cambio de trabajo en un Centro de Reconocimiento diferente.

8. El Sistema de Control y Vigilancia podrá activar las validaciones del especialista o médico en una de las pruebas, al comienzo o al final de las mismas, y de manera aleatoria. Las validaciones se realizarán a través de la huella con la funcionalidad activa de dedo vivo.

9. El RUNT podrá activar el registro y envío de los resultados al final de cada una de las pruebas por parte de cada especialista de los Centros de Reconocimiento de Conductores.

10. El Centro de Reconocimiento de Conductores deberá registrar y enviar los resultados de los exámenes al terminar cada prueba directamente al Sistema de Control y Vigilancia.

    El Sistema de Control y Vigilancia validará todas y cada una de las pruebas realizadas con los criterios de evaluación establecidos en la Resolución N° 1555 de 2005 expedida por el Ministerio de Transporte o aquellas que la modifiquen, deroguen o adicionen. Este sistema controlará los tiempos mínimos en que se debe realizar cada prueba (psicomotriz, optometría, auditiva y médica).

"Por la cual se reglamentan las características técnicas del sistema de seguridad documental denominado "sistema de control y vigilancia" para los Centros de Reconocimiento de Conductores para garantizar la legitimidad de los certificados y la protección al usuario de la falsificación y se realiza una derogatoria orgánica sobre la materia".

11. El Sistema de Control y Vigilancia deberá realizar control sobre la validación geofísica del Centro de Reconocimiento de Conductores y de los equipos desde donde se transmite la información.

12. El Sistema de Control y Vigilancia se conectará por medio de una Red Privada Virtual (VPN – Virtual Private Network) la cual tendrá dispositivos de seguridad y comunicaciones que permitan controlar y validar geográficamente la ubicación de los sistemas antes mencionados los cuales estarán instalados en cada Centro de Reconocimiento de Conductores. La finalidad de lo anterior es poder tener certeza de que los certificados que se expidan realmente sean resultado de la realización de los exámenes de aptitud física, mental y de coordinación motriz desde la sede acreditada y en la dirección que se reporta, pudiendo controlar y autorizar los equipos en mención de cada Centro de Reconocimiento de Conductores.

13. Habrá una conexión por parte de los Centros de Reconocimiento de Conductores al Sistema de Control y Vigilancia por medio de canales de Internet óptimos para la operación, con una dirección IP Pública Fija. Deberá existir un canal dedicado suficiente entre el Sistema de Control y Vigilancia y los Centros y entre este y el centro de monitoreo de la Superintendencia de Puertos y Transporte, de tal forma que permita la conexión óptima para que esta ejerza sus actividades de inspección, vigilancia y control.

Parágrafo Primero: A efectos de desarrollar el cumplimiento de las actividades antes descritas se deberá contar con la siguiente información:

Se deberá permitir por parte del RUNT el ingreso a la Red Privada Virtual (VPN) para acceder al descargue de los archivos que contendrán las FUPAS y los certificados médicos correspondientes, dicho acceso debe ser diario y continuo. Lo anterior implica que la contraseña de acceso debe ser permanente para esta entidad. También se le solicitará al RUNT los archivos y los datos concernientes a los tiempos transcurridos en el proceso completo de certificación.

El Sistema de Control y Vigilancia deberá entregar al Centro de Monitoreo de la Superintendencia de Puertos y Transporte un informe de conciliación diario de toda la información suministrada legítimamente por cada uno de los actores. La Superintendencia de Puertos y Transporte tendrá acceso en tiempo real a las fuentes de información para hacer sus propios procedimientos de inspección vigilancia y control.

El RUNT deberá aportar los cupos utilizados diariamente para que estos puedan ser corroborados frente a aquellos asignados por el Ministerio de Transporte. Dicha información deberá ser suministrada por estos dos actores cada quince (15) días o cuando lo requiera la Superintendencia de Puertos y Transporte para desarrollar la actividad de Control y Vigilancia. Adicionalmente, en caso de encontrarse hallazgos en un Centro de Reconocimiento de Conductores, se confrontará esta información por medio de visita administrativa en la que se efectuará un ejercicio comparativo entre el ingreso de usuarios diario del Centro de Reconocimiento de Conductores frente a los usuarios atendidos y esto a su vez, confrontado con los valores máximos diarios permitidos por el Ministerio de Transporte en la realización de la actividad. Lo anterior, acorde a la información suministrada por el RUNT y el Ministerio de Transporte.

"Por la cual se reglamentan las características técnicas del sistema de seguridad documental denominado "sistema de control y vigilancia" para los Centros de Reconocimiento de Conductores para garantizar la legitimidad de los certificados y la protección al usuario de la falsificación y se realiza una derogatoria orgánica sobre la materia".

La Superintendencia de Puertos y Transporte y el RUNT deberán propiciar la implementación de un canal dedicado, punta a punta, con el fin de proporcionarle mayor disponibilidad de información a esta Superintendencia.

El RUNT deberá permitir el ingreso a su plataforma a la Superintendencia de Puertos y Transporte con un usuario que proporcione privilegios de interrupción de la transmisión y/o cargue de certificados médicos. Esto, con el fin de poder aplicar las medidas preventivas operativas a que haya lugar en los Centros de Reconocimiento de Conductores.

Parágrafo Segundo: Una vez se encuentren integradas las plataformas del RUNT y los Sistemas de Control y Vigilancia, los Centros de Reconocimiento de Conductores sólo podrán cargar los certificados de aptitud física, mental y de coordinación motriz al RUNT si han cumplido los requisitos del Sistema de Control y Vigilancia estipulados en esta Resolución.

Parágrafo Tercero: Además de dar cumplimiento a lo requerido en la Resolución N° 1555 de 2005 expedida por el Ministerio de Transporte o por las normas que la modifiquen, sustituyan, deroguen o adicionen, el Sistema de Control y Vigilancia descrito en este capítulo deberá ser validado por la Superintendencia de Puertos y Transporte, o por quien esta delegue, tomando en cuenta las especificaciones técnicas mínimas que se expidan.

Artículo 4°. Conectividad y Acceso del Sistema de Control y Vigilancia. El Sistema de Control y Vigilancia deberá permitir a la Superintendencia de Puertos y Transporte para el ejercicio de sus funciones de inspección, vigilancia y control, realizar consulta en línea de los certificados médicos de aptitud física, mental y de coordinación motriz y bases de datos conforme a los criterios de auditoría y de búsqueda que esta requiera; así mismo, estarán obligados a conectarse al Centro de Monitoreo de la Superintendencia de Puertos y Transporte y al RUNT y entregarán alarmas automatizadas al Centro de Monitoreo, bajo los criterios, estructura y periodicidad definidos por la Superintendencia de Puertos y Transporte, la cual podrá solicitar la generación de nuevos tipos de alarmas cuando así lo requiera.

Artículo 5°. Garantía de No Afectación del Servicio. El Sistema de Control y Vigilancia deberá disponer de toda la Infraestructura Tecnológica necesaria para su operación permanente y deberá garantizar su correcta operación, según lo establecido en la presente resolución, a todos los centros de reconocimiento de conductores, al RUNT, al actor del Sistema Financiero y a la Superintendencia de Puertos y Transporte.

Capítulo III

Disposiciones finales

Artículo 6°. Investigación Administrativa: Los Centros de Reconocimiento de Conductores deberán cumplir con las condiciones de seguridad señaladas en esta Resolución y las demás normas que la modifiquen, sustituyan o adicionen para la expedición y reporte de los certificados de aptitud física mental y de coordinación motriz como documento válido para obtener la licencia de conducción, so pena de iniciar por parte de esta Superintendencia las investigaciones administrativas a que haya lugar.

"Por la cual se reglamentan las características técnicas del sistema de seguridad documental denominado "sistema de control y vigilancia" para los Centros de Reconocimiento de Conductores para garantizar la legitimidad de los certificados y la protección al usuario de la falsificación y se realiza una derogatoria orgánica sobre la materia".

Artículo 7º. Anexo Técnico para la Validación del Sistema de Control y Vigilancia. Hace parte integral de la presente Resolución el Anexo Técnico para la Validación de los requisitos técnicos mínimos exigidos para poder entrar a operar el Sistema de Control y Vigilancia.

Artículo 8°. Vigencia: Esta Resolución rige a partir de su publicación, tal como lo determina el artículo 65 del Código de Procedimiento Administrativo.

Artículo 9°. Derogaciones: Deróguense a partir de la vigencia dispuesta en el artículo anterior todas las disposiciones que sean contrarias a esta Resolución, en especial, la Resolución N° 7034 de 2012, la Resolución N° 191 de 2013, la Resolución N° 917 de 2014, la Resolución 2193 de 2014 y la Resolución N° 4980 de 2014.

PUBLÍQUESE Y CÚMPLASE 28 MAY 2014 009699

JUAN MIGUEL DURÁN PRIETO
Superintendente de Puertos y Transporte

Proyectó: Alejandra Rojas Posada – Abogada Sistema de Control y Vigilancia
Revisó: Lina Marcela Cuadros - Jefe Oficina Asesora Jurídica
Mauricio Barón - Asesor Despacho
Fernando Martínez - Superintendente Delegado de Tránsito y Transporte
Hamid Bolívar – Sistema de Control y Vigilancia

Uptc
Universidad Pedagógica y Tecnológica de Colombia

DOCUMENTO DE REQUISITOS DE LOS ASPIRANTES A PROVEEDORES DEL SISTEMA DE CONTROL Y VIGILANCIA

Versión 2

DESTINATARIO:
SUPERINTENDENCIA DE PUERTOS Y TRANSPORTE

Mayo del 2014

Tunja–Boyacá Sede Central: Avenida Central del Norte. Edificio Administrativo Piso 5
PBX: (57) 8 7436236 7405626 Fax: 7436206

Bogotá D.C.: Carrera 14 No. 44-51 Teléfono: 5473588-2517283- 2855845
Telefax: 2853262

Uptc
Universidad Pedagógica y Tecnológica de Colombia

CONTROL DE VERSIONES

FECHA	DESCRIPCIÓN	RESPONSABLE
12/05/2014	Versión 2.0 Documento de Requisitos de los aspirantes a proveedores del Sistema de Control y Vigilancia	UPTC

Tunja–Boyacá Sede Central: Avenida Central del Norte. Edificio Administrativo Piso 5
PBX: (57) 8 7436236 7405626 Fax: 7436206

Bogotá D.C.: Carrera 14 No. 44-51 Teléfono: 5473588-2517283- 2855845
Telefax: 2853262

A continuación se establecen los procedimientos y requisitos que deberán cumplir los aspirantes a homologación para recibir la evaluación, informe de evaluación y acto administrativo de homologación en caso de cumplir con los requisitos.

1. **Solicitud de Aclaraciones:** A partir del día de publicación y durante un periodo de cinco (5) días calendario, los aspirantes podrán enviar solicitudes de aclaración sobre los requisitos de homologación. En este caso la UPTC tendrá un plazo máximo de cinco (5) días calendario para dar respuesta a las solicitudes de aclaración.

2. **Radicación de carta de interés**: El aspirante deberá radicar ante la Superintendencia de Puertos y Transporte en la oficina del Superintendente delegado de tránsito, una carta de intención de participar en el proceso de evaluación y homologación como proveedor del Sistema de Control y Vigilancia. Esta carta deberá estar firmada por el representante legal de la sociedad y tendrán hasta quince (15) días calendario después de radicada la carta para entregar los requisitos documentales. En el caso de no radicar los documentos en el periodo establecido se procederá a anular el proceso de evaluación y homologación del aspirante.

3. **Radicación de Requisitos Documentales:** El aspirante deberá dentro del plazo posterior a la radicación de carta de interés los siguientes documentos:

REQUISITOS DOCUMENTALES
a. Carta remisoria de radicación de requisitos con referencia "Requisitos documentales para el proceso de evaluación de aspirantes a proveedores del sistema de control y vigilancia", razón social, NIT, número de folios de documentación entregada y datos de contacto (teléfono, dirección, correo electrónico). Esta carta deberá estar firmada por el Representante legal de la sociedad aspirante.
b. Documento foliado y en sobre sellado junto con una copia que contenga los siguientes capítulos:
<u>Documentos generales de la sociedad:</u> 1. Certificado de Cámara de Comercio no mayor a 30 días 2. Registro único Tributario RUT 3. Carta de Presentación de la Sociedad. 4. Copia de la Cédula de Ciudadanía del representante legal. 5. Certificado de Antecedentes Judiciales del representante legal. 6. Certificado emitido por revisor fiscal o el representante legal según quien lo deba emitir basado en el tipo de sociedad, en el cual se certifique el cumplimiento del pago de los aportes parafiscales. 7. Las sociedades a participar deberán contar con alguna de las siguientes actividades económicas con base en el nuevo CIIU: Procesamiento de datos, consultoría informática y actividades de administración de instalaciones informáticas, actividades de desarrollo de sistemas informáticos. Las sociedades aspirantes deben tener una antigüedad mínima de 5 años a partir de su constitución. 8. En caso de participar en unión temporal cada sociedad deberá presentar los documentos

anteriores, presentar documento de conformación de la unión temporal con porcentaje de participación y responsabilidades de cada sociedad.

Requisitos Financieros:

El aspirante a proveedor deberá presentar los siguientes documentos.

1. Estados Financieros dictaminados de la Sociedad incluyendo como mínimo estado de resultados y Balance general.
2. Hoja de resumen de indicadores financieros que se detalla en el siguiente cuadro:

INDICADORES	CONCEPTO	REQUISITO	VALOR DEL ASPIRANTE
CAPITAL REAL	CAPITAL SOCIAL RESERVAS CONSTITUIDAS UTILIDADES RETENIDAS UTILIDADES DEL EJERCICIO	Mayor a $1.000.000.000	
LIQUIDEZ	ACTIVO CORRIENTE / PASIVO CORRIENTE	Mayor a 1	
NIVEL DE ENDEUDAMIENTO	PASIVO TOTAL ACTIVO TOTAL	Menor a 65%	
CAPITAL DE TRABAJO	ACTIVO CORRIENTE - PASIVO CORRIENTE	Mayor a 0	
EBITDA	UTILIDAD OPERACIONAL DEPRECIACIONES Y AMORTIZACIONES	Mayor a 0	
DE RIESGO	ACTIVO FIJO / PATRIMONIO NETO	Menor a 0,8	
INDICADOR DE CRECIMIENTO DEL EBITDA	EBITDA ULTIMO AÑO/ EBITDA AÑO ANTERIOR	Mayor a 0,8	

3. En caso de que el aspirante a proveedor sea evaluado antes del 30 de Marzo de 2013 y no cuente con los estados financieros dictaminados a corte de 31 de diciembre de 2012 podrá presentar los estados financieros a corte de 31 de diciembre del 2011.

4. En caso de participar en unión temporal o consorcio, sumadas todos los miembros que lo conforman, deberá cumplir con los indicadores financieros

Uptc
Universidad Pedagógica y Tecnológica de Colombia

Requisitos Administrativos:

Experiencia de la Compañía.

- Acreditar experiencia mediante certificación firmada por los clientes en proyectos de sistemas informáticos en máximo 4 certificaciones cuya sumatoria sea superior a ($5.000.000.000) cinco mil millones de pesos, en los últimos cuatro (4) años.
- Acreditar experiencia mediante certificación firmada por los clientes en por lo menos dos proyectos relacionados con sistemas que incluyan alguna de las siguientes funcionalidades: manejo de riesgo, protección de datos, cifrado de información, auditoria de bases de datos, correlación de eventos en proyectos en los últimos 4 años.
- Acreditar experiencia mediante certificación firmada por los clientes en por lo menos un proyecto donde se haya efectuado integración con los sistemas transaccionales de una entidad financiera vigilada por la Superintendencia Financiera de Colombia en proyectos en los últimos 4 años.
- El aspirante a proveedor del SCV deberá contar con por lo menos una de las siguientes certificaciones: CMMI, IT MARK, ISO 27001 o ISO 20000. Las certificaciones deberán estar vigentes a la fecha de evaluación. En el caso de unión temporal o consorcio al menos una de las sociedades que conforma la unión temporal deberá contar con por lo menos una de las certificaciones solicitadas y esta deberá tener el mayor porcentaje de participación en dicha unión temporal.

Experiencia del Equipo de Trabajo.

Equipo de Dirección:

- Gerente de Proyectos. 1 profesional en ingeniería de sistemas, industrial, electrónica o afines, con especialización en gerencia de proyectos o maestría en ingeniería de sistemas, con certificación de PMP.
- Con el fin de asegurar la idoneidad y estabilidad del equipo de trabajo se deberá adjuntar copia de título profesional, titulo de postgrado, certificaciones y 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.

Equipo de trabajo de seguridad:

- Gerente de SOC. 1 profesional en ingeniería de sistemas, industrial, electrónica o afines, con especialización en gerencia de proyectos o maestría en ingeniería de sistemas, con certificación de PMP , certificación ITIL y certificación como auditor interno de ISO-27001.
- Oficial de Seguridad. 1 profesional en ingeniería de sistemas, electrónico, de redes o afines con postgrado en gerencia de proyectos, gerencia de proyectos en teleinformática, seguridad de la información o maestría en seguridad informática, certificado como CISSP o CISM.
- Especialista en Hacking. 1 profesional en ingeniería de sistemas, electrónico, de redes o afines, certificado como CEH.
- Especialistas DAM. 1 profesional en ingeniería de sistemas, electrónica, de redes o afines con certificación técnica emitida por el fabricante de la solución DAM utilizada en la solución presentada por el aspirante.
- Especialista de IPS. 1 profesional en ingeniería de sistemas, electrónico, de redes o afines con certificación técnica emitida por el fabricante de la solución de IPS utilizada en la

solución presentada por el aspirante.

- Especialista ENDPOINT. 1 profesional en ingeniería de sistemas, electrónico, de redes o afines con certificación técnica emitida por el fabricante de la solución de protección ENDPOINT utilizada en los servidores de la solución presentada por el aspirante.
- Auditor interno. 1 profesional en ingeniería de sistemas, industrial, electrónica, de redes o afines con 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, certificaciones y 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.

Equipo de trabajo de desarrollo:

- Ingenieros de desarrollo. 2 profesionales en ingeniería de sistemas, certificados en lenguajes de programación en los cuales se encuentra construida la aplicación presentada por el aspirante para la solución de SCV.
- Con el fin de asegurar la idoneidad y estabilidad del equipo de trabajo se deberá adjuntar copia de título profesional, titulo de postgrado cuando aplique, certificaciones y 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.

Equipo de trabajo de soporte:

- Ingenieros de soporte. 2 profesionales en ingeniería de sistemas, electrónica o redes.
- Técnicos de soporte. 4 técnicos, tecnólogos o ingenieros de sistemas, electrónica, redes, telecomunicaciones o afines.
- Con el fin de asegurar la idoneidad y estabilidad del equipo de trabajo se deberá adjuntar copia de título profesional o técnico, certificaciones y 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.
- El aspirante a homologación podrá tener subcontrado 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 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.
- El aspirante 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:
    - Establecer un canal dedicado con el sistema RUNT
    - Establecer las siguientes integraciones requeridas con el sistema RUNT:
        - Solicitud de certificado médico
        - Solicitud de Cargue de certificado médico
        - Apertura de interfaces para validación de candidato y médico o especialista
        - Recepción de certificados médicos
        - Recepción de licencias de conducción
        - Recepción de FUPAS
    - Realizar los procedimientos de conexión y validación de identidad en línea con la Registraduría Nacional del Estado Civil una vez la requiera la Superintendencia de

Puertos y Transporte.

- Establecer un canal dedicado con el centro de monitoreo de la Superintendencia de Puertos y Transporte
- Establecer las siguientes integraciones requeridas con el centro de monitoreo de la Superintendencia de Puertos y Transporte:
  - Envío de archivo de recaudo
  - Envío de archivo de eventos
  - Acceso a software de Posicionamiento Centros de Reconocimiento de Conductores
  - Generación y envío de archivo de conciliación de actores del proceso

La Superintendencia de Puertos y Transporte se encargara de gestionar las autorizaciones con la Registraduría Nacional del Estado Civil y con el RUNT para establecer los procesos de conexión.

Requisitos Técnicos:

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 y copia del certificado de registro de soporte lógico de la Dirección Nacional de Derechos de Autor de la compañía fabricante.
2. Adjuntar copia de la solicitud presentada ante la Superintendencia de Industria y Comercio del registro de invención o de modelo de utilidad de un sistema, estructura o dispositivo que tenga relación con el objeto de sistemas de transmisión segura, sistemas de validación de identidad o sistemas de validación de sitios remotos. La solicitud presentada podrá estar en estado de trámite o en estado de concedido el derecho.
   En caso de no contar con la solicitud anterior el aspirante deberá presentar un documento técnico que permita garantizar la idoneidad del aspirante. El documento técnico deberá contar con los siguientes capítulos: Descripción General del Sistema, Descripción General de Subsistemas, Diagrama de red, arquitectura de servidores, arquitectura general de la aplicación, arquitectura de seguridad en sitios remotos y geo-posicionamiento satelital, esquema de correlación de eventos, esquema para el control de ataques informáticos, esquema de auditoria de bases de datos, esquema de verificación de código fuente, esquema de protección de datos sensibles y de transmisión segura de datos, esquema de intercambio transaccional para el recaudo, diagrama E-R (Entidad Relación) de las principales entidades, documento modelo de arquitectura de software, esquema de alta disponibilidad y continuidad de negocio, en el caso en que el representante legal de la compañía no sea ingeniero de sistemas o electrónico deberá una carta de aval de un ingeniero de sistemas o electrónico.
3. Adjuntar copia de contrato de centro de cómputo en caso de que el centro de cómputo se encuentre subcontratado. Los contratos deberán tener una duración mínima de veinticuatro meses.
4. Adjuntar copia de manifiesto de importación de las soluciones de servidores, IPS, Firewall, Herramienta DAM, Herramienta SIEM, SAN, Escáner de Vulnerabilidades, Application Delivery Controller.
5. Adjuntar copia de las facturas de compra 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 copia de las facturas presentadas podrán ser del

proveedor contratado.

6. Adjuntar copia de certificación o indicaciones de como verificar que la herramienta de mesa de ayuda a utilizar cuente con por lo menos 5 procesos de ITIL certificados.
7. Diligenciar el siguiente cuadro de requisitos tecnológicos:

SOLUCION	REQUISITO MINIMO	NOMBRE DEL FABRICANTE	PRODUCTO, MODELO O VERSION
IPS	**Solución de propósito específico basado en hardware (appliance) diferente a soluciones UTM, debe tener como mínimo 1 Gbps de throughput y fuente redundante.** **La solución utilizada deberá encontrarse en el cuadrante de Leaders o Visionaries del Magic Quadrant for Intrusion Prevention Systems de Gartner mas reciente.**		
DAM	**Solución basada en hardware o software para la protección, auditoria, monitoreo de la base de datos del sistema de información que contenga el SCV.** **La solución utilizada deberá encontrarse en el nivel de Strong Performers o Leaders del Forrester Wave-Database Auditing and realtime protection más reciente.**		
SIEM	**Solución basada en hardware o software para la administración de logs y la correlación de eventos de la plataforma tecnológica del SCV.** **La solución utilizada deberá encontrarse en el cuadrante de Leaders o Visionaries del Magic Quadrant Security Information and Event Management de Gartner mas reciente.**		
Protección de ENDPOINT	**Solución basada en software para protección antimalware de los servidores utilizados del SCV.** **La solución utilizada deberá encontrarse en el cuadrante de Leaders o Visionaries del Magic Quadrant for Endpoint Protection Platforms de Gartner mas reciente.**		
FIREWALL/UTM	**Solución basada en hardware de propósito**		

	PERIMETRAL	específico, debe tener como mínimo 1 Gbps de throughput y fuente redundante. La solución utilizada deberá encontrarse en el cuadrante de Leaders o Visionaries del Magic Quadrant for Unified Thread Management de Gartner o en el cuadrante de Leaders o Visionaries del Magic Quadrant for Enterprise Network Firewalls más reciente.		
	Application Delivery Controller	Solución basada en hardware de propósito específico, debe tener como mínimo funcionalidad de balanceo de cargas y de web application firewall, 1 Gbps de throughput y fuente redundante. La solución utilizada deberá encontrarse en el cuadrante de Leaders o Visionaries del Magic Quadrant for Application Delivery Controller de Gartner más reciente.		
	Escaner de Vulnerabilidades de Red	Solución basada en hardware de propósito específico. La solución utilizada deberá consultar la base de datos del CVE (Common Vulnerabilities and Exposures).		
	Dynamic Application Security Testing	Solución basada en software que permita realizar pruebas de seguridad a la aplicación. La solución utilizada deberá encontrarse en el cuadrante de Leaders o Visionaries del Magic Quadrant for Dynamic Application Security Testing de Gartner más reciente.		
	Static Application Security Testing	Solución basada en software que permita realizar pruebas de seguridad al código fuente de la aplicación. La solución utilizada deberá encontrarse en el cuadrante de Leaders o Visionaries del Magic Quadrant for Static Application Security Testing de Gartner más reciente.		
	Servidor de Comunicaciones seguras y de validación de	Solución basada en hardware y software que permita: • Registrar ubicaciones geofísicas de los centros de reconomiento de		

	geo-posicionamiento.	**conductores.** • **Validar la ubicación de origen de la información que se transmita al SCV.** • **Establecer conexiones seguras entre cada uno de los PCs de los centros de reconocimiento de conductores, estas conexiones se podrán establecer a través de protocolos seguros (SSH o IPSec).** • **Visualizar un mapa de Colombia con las ubicaciones de los CRC´s y el estado de conexión de los PC´s con el SCV.**		

4. La UPTC Universidad Pedagógica y Tecnológica de Colombia delegada por la Superintendencia de Puertos y Transporte, evaluará los documentos presentados en un periodo no mayor a cinco días calendario. Posterior a la validación de la documentación radicada se entregará al aspirante el informe del resultado de la evaluación documental indicando si requiere aclaraciones o complemento de documentos, en este caso el aspirante a proveedor tendrá máximo tres días hábiles para dar respuesta a la solicitud.

   En el caso que el aspirante a proveedor no responda las aclaraciones en el plazo de los tres días, la UPTC procederá a anular el proceso de evaluación y homologación del aspirante.
   En el caso que un aspirante, haya recibido anulación del proceso de evaluación en esta etapa, deberá reiniciar el proceso de evaluación desde el punto 2 (Radicación de carta de interés). Un aspirante a proveedor podrá máximo dos intentos de proceso de evaluación.

   En el caso que el informe de evaluación concluya que el aspirante a homologación cumple con todos los requisitos documentales se entregara un oficio por parte de la UPTC indicando las fechas programadas de visita de verificación establecidas en el siguiente numeral (no serán superior a tres (3) días, posterior a la entrega del informe de resultado de la evaluación documental).

5. 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:

Visita a la mesa de ayuda. Se verificaran los siguientes aspectos: 1. La herramienta presentada en la etapa documental para mesa de ayuda deberá estar instalada y se debe mostrar la radicación de una solicitud de soporte. 2. Se debe mostrar la evidencia de los requerimientos que se encuentran en la lista de chequeo en el ítem de "solución de soporte de aspirante a proveedor". 3. La mesa de ayuda deberá estar conformada por el equipo de trabajo presentado en la etapa documental. 4. La mesa de ayuda deberá estar ubicada en territorio nacional.

Visita al Centro de Operaciones de Seguridad.

1. El centro de operaciones de seguridad deberá contar con un control de acceso biométrico.
2. El centro de operaciones de seguridad deberá contar con un sistema de circuito cerrado de televisión.
3. El centro de operaciones de seguridad deberá estar ubicada en territorio nacional.
4. El centro de operaciones de seguridad deberá contar con un video Wall con mínimo cuatro pantallas.
5. 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 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) Prueba de auditoria de base de datos. Se deberá disponer de un cliente del motor de base de datos que permita realizar la modificación en un registro en la tabla en la cual se almacene información biométrica. El evaluador procederá a alterar un registro en la base de datos. Posterior a esto la solución DAM deberá notificará la modificación del registro enviando una alerta al sistema SIEM con la información detallada del incidente.
    c) Verificación de información biométrica cifrada. El aspirante deberá mostrar la ubicación en la cual almacene la información biométrica con el fin de verificar que esta se encuentre cifrada.
    d) Verificación de Endpoint. Se deberá demostrar que se encuentran instaladas en los servidores la solución de antimalware.
    e) Verificación de herramientas de pruebas de seguridad. Se deberá demostrar que están instaladas las herramientas de pruebas de seguridad de aplicación dinámica y estática.
    f) 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.

Nota: Los PCs de los CRC´s que intervendrán en la conexión con los Sistemas de Control y Vigilancia homologados y con el sistema del RUNT, deberán contar como

mínimo con los requerimientos técnicos actuales de Hardware, Software y Comunicaciones solicitados por el RUNT y los que requieran los Sistemas de Control y Vigilancia. Se recomienda como mínimo: 1. Sistema Operativo: Windows Vista, Windows 7 o Windows 8 con la última actualización o parche de seguridad. 2. Memoria RAM: 1 GB o superior. 3. Disco Duro: 20 GB con espacio disponible como mínimo de 5GB. 4. Canal de Internet Dedicado o Canal de Datos Dedicado: Capacidad 2 Mbps o superior rehuso 1:1, con una IP pública fija.
Visita al Centro de Cómputo. 1. El centro de operaciones de seguridad deberá estar ubicada en territorio nacional. 2. Se verificará que en el centro de cómputo se encuentren ubicados todos los equipos de hardware solicitados. 3. En el caso de que los equipos se encuentren en más de un datacenter, se coordinará la visita a todos los datacenter para verificar la totalidad de los equipos solicitados.
Visita a un centro de reconocimiento de conductores en el cual se muestre el funcionamiento del sistema de control y vigilancia. Se procederá a realizar visita aun CRC en el cual se encuentre instalada la solución y se permita verificar los siguientes escenarios: a) 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 sector financiero. Esto deberá cumplir con todos los requerimientos exigidos en la lista de chequeo del anexo técnico. En el caso de requerirse participación de la entidad financiera para realizar esta verificación, el aspirante será el encargado de coordinar todos los requisitos para poder realizar la prueba. b) Verificación del proceso de enrolamiento de candidato. Se deberá demostrar que una aplicación integrada con todo el sistema, realice el registro y toma de información con los dispositivos de captura de información del candidato (lector biométrico de huellas homologado por el RUNT, cámara digital, pistola o escáner de lectura de código bidimensional, pad de firmas). c) Verificación de validación de identidad. Se deberá demostrar que una aplicación integrada con todo el sistema, realice la validación con el procedimiento alternativo temporal de validación de

identidad definido.

d) Aseguramiento de la presencia del candidato y médico o especialista 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 en el sistema a homologar.
e) Los Centros de Reconocimiento de Conductores por protocolo de seguridad, solo se conectarán a través de red física LAN con el Sistema de Control y Vigilancia, no se permitirán conexiones inalámbricas o WIFI. Se verificará técnicamente que el sistema a homologar cumpla con estas validaciones.
f) Verificación de validación de equipos. Se deberá demostrar que una aplicación integrada con todo el sistema, realice la validación los PCS registrados. Se realizarán pruebas con otros PC´s no registrados para verificar la validación.
g) Verificación de validación de posición geofísica. Se deberá demostrar que una aplicación integrada con todo el sistema, realice la validación de la geo-posición satelital de dos CRC´s. Se realizaran pruebas técnicas para verificar la validación.

6. La UPTC tendrá un (1) día hábil para entregar el informe de evaluación final en el cual se indicará si el aspirante a homologación cumple con los requisitos exigidos.

7. En el caso que el aspirante haya recibido en la evaluación el concepto de que cumple con los requisitos exigidos, la Superintendencia de Puertos y Transporte en un plazo máximo de cinco (5) días hábiles procederá a emitir un acto administrativo en el cual se autoriza al aspirante como proveedor homologado del sistema de control y vigilancia.

ANÉXO TÉCNICO DE REQUISITOS DE LOS ASPIRANTES A PROVEEDORES DEL SISTEMA DE CONTROL Y VIGILANCIA PARA LOS CENTROS DE RECONOCIMIENTO DE CONDUCTORES - Versión 2 - Mayo 2014

ITEM	SOLUCIÓN	PROCESO/ APLICACIÓN	FUNCIONALIDAD / HERRAMIENTA / REQUERIMIENTO	MODO DE VERIFICACIÓN	OBSERVACIÓN	Cumple	No Cumple	No Aplica	Registro (Foto, Filmación)
1		Solicitud	Existencia de carta remisoria	- Compruebe la existencia de la carta remisoria de radicación de requisitos con referencia "Requisitos documentales para el proceso de evaluación de aspirantes a proveedores del sistema de control y vigilancia", razón social, NIT, número de folios de documentación entregada y datos de contacto (teléfono, dirección, correo electrónico). - Compruebe que la carta este firmada por el Representante legal de la sociedad aspirante.					
2			Documentos generales de la sociedad	- Compruebe la existencia de los siguientes documentos por parte del aspirante a proveedor: 1. Certificado de Cámara de Comercio no mayor a 30 días 2. Registro único Tributario RUT 3. Carta de Presentación de la Sociedad. 4. Copia de la Cédula de Ciudadanía del representante legal. 5. Certificado de Antecedentes Judiciales del representante legal. 6. Certificado emitido por revisor fiscal o el representante legal según quien lo deba emitir basado en el tipo de sociedad, en el cual se certifique el cumplimiento del pago de los aportes parafiscales. 7. Las sociedades a participar deberán contar con alguna de las siguientes actividades económicas con base en el nuevo CIIU: Procesamiento de datos, consultoría informática y actividades de administración de instalaciones informáticas, actividades de desarrollo de sistemas informáticos. 8. Las sociedades aspirantes deben tener una antigüedad mínima de 5 años a partir de su constitución. 9. En caso de participar en unión temporal cada sociedad deberá presentar los documentos anteriores, presentar documento de conformación de la unión temporal con porcentaje de participación y responsabilidades de cada sociedad.	Foliado y en sobre sellado junto con una copia				
3			Requisitos Financieros	- Compruebe la existencia de los siguientes documentos por parte del aspirante a proveedor: 1. Estados Financieros dictaminados de la Sociedad incluyendo como mínimo estado de resultados y Balance general. 2. Diligenciamiento de la hoja de resumen de indicadores financieros que se detalla en el Excel hoja "Requerimientos Financieros" 3. En caso de que el aspirante a proveedor sea evaluado antes del 30 de Marzo de 2013 y no cuente con los estados financieros dictaminados a corte de 31 de diciembre de 2012 podrá presentar los estados financieros a corte de 31 de diciembre del 2011. 4. En caso de participar en unión temporal o consorcio, sumadas todos los miembros que lo conforman, deberá cumplir con los indicadores financieros.	Foliado y en sobre sellado junto con una copia				

ITEM	SOLUCIÓN	PROCESO/ APLICACIÓN	FUNCIONALIDAD / HERRAMIENTA / REQUERIMIENTO	MODO DE VERIFICACIÓN	OBSERVACIÓN	Cumple	No Cumple	No Aplica	Registro (Foto, Filmación)
4			Requisitos Administrativos	- Compruebe la Experiencia de la Compañía con los siguientes documentos: * Acreditar experiencia mediante certificación firmada por los clientes en proyectos de sistemas informáticos en máximo 4 certificaciones cuya sumatoria sea superior a ($5.000.000.000) cinco mil millones de pesos, en los últimos cuatro (4) años. * Acreditar experiencia mediante certificación firmada por los clientes en por lo menos dos proyectos relacionados con sistemas que incluyan alguna de las siguientes funcionalidades: manejo de riesgo, protección de datos, cifrado de información, auditoria de bases de datos, correlación de eventos en proyectos en los últimos 4 años. * Acreditar experiencia mediante certificación firmada por los clientes en por lo menos un proyecto donde se haya efectuado integración con los sistemas transaccionales de una entidad financiera vigilada por la Superintendencia Financiera de Colombia en proyectos en los últimos 4 años. * El aspirante a proveedor del SCV deberá contar con por lo menos una de las siguientes certificaciones: CMMI, IT MARK, ISO 27001 o ISO 20000. Las certificaciones deberán estar vigentes a la fecha de evaluación. En el caso de unión temporal o consorcio al menos una de las sociedades que conforma la unión temporal deberá contar con por lo menos una de las certificaciones solicitadas y esta deberá tener el mayor porcentaje de participación en dicha unión temporal.	Foliado y en sobre sellado junto con una copia				
5			Requisitos Administrativos	- Compruebe la Experiencia del Equipo de trabajo con los siguientes documentos: <u>Equipo de Dirección</u>: * Gerente de Proyectos. 1 profesional en ingeniería de sistemas, industrial, electrónica o afines, con especialización en gerencia de proyectos o maestría en ingeniería de sistemas, con certificación de PMP. * Con el fin de asegurar la idoneidad y estabilidad del equipo de trabajo se deberá adjuntar copia de título profesional, titulo de postgrado, certificaciones y 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.	Foliado y en sobre sellado junto con una copia				

ITEM	SOLUCIÓN	PROCESO/ APLICACIÓN	FUNCIONALIDAD / HERRAMIENTA / REQUERIMIENTO	MODO DE VERIFICACIÓN	OBSERVACIÓN	Cumple	No Cumple	No Aplica	Registro (Foto, Filmación)
		Documentos por parte del aspirante a homologar	Requisitos Administrativos	Equipo de trabajo de seguridad: * Gerente de SOC. 1 profesional en ingeniería de sistemas, industrial, electrónica o afines, con especialización en gerencia de proyectos o maestría en ingeniería de sistemas, con certificación de PMP , certificación ITIL y certificación como auditor interno de ISO-27001. * Oficial de Seguridad. 1 profesional en ingeniería de sistemas, electrónico, de redes o afines con postgrado en gerencia de proyectos, gerencia de proyectos en teleinformática, seguridad de la información o maestría en seguridad informática, certificado como CISSP o CISM. * Especialista en Hacking. 1 profesional en ingeniería de sistemas, electrónico, de redes o afines, certificado como CEH. * Especialistas DAM. 1 profesional en ingeniería de sistemas, electrónica, de redes o afines con certificación técnica emitida por el fabricante de la solución DAM utilizada en la solución presentada por el aspirante. * Especialista de IPS. 1 profesional en ingeniería de sistemas, electrónico, de redes o afines con certificación técnica emitida por el fabricante de la solución de IPS utilizada en la solución presentada por el aspirante. * Especialista ENDPOINT. 1 profesional en ingeniería de sistemas, electrónico, de redes o afines con certificación técnica emitida por el fabricante de la solución de protección ENDPOINT utilizada en los servidores de la solución presentada por el aspirante. * Auditor interno. 1 profesional en ingeniería de sistemas, industrial, electrónica, de redes o afine con 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, certificaciones y 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.	Foliado y en sobre sellado junto con una copia				
			Requisitos Administrativos	Equipo de trabajo de desarrollo: * Ingenieros de desarrollo. 2 profesionales en ingeniería de sistemas, certificados en lenguajes de programación en los cuales se encuentra construida la aplicación presentada por el aspirante para la solución de SCV. * Con el fin de asegurar la idoneidad y estabilidad del equipo de trabajo se deberá adjuntar copia de título profesional, titulo de postgrado cuando aplique, certificaciones y 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. Equipo de trabajo de soporte: * Ingenieros de soporte. 2 profesionales en ingeniería de sistemas, electrónica o redes. * Técnicos de soporte. 4 técnicos, tecnólogos o ingenieros de sistemas, electrónica, redes, telecomunicaciones o afines. * Con el fin de asegurar la idoneidad y estabilidad del equipo de trabajo se deberá adjuntar copia de título profesional o técnico, certificaciones y 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.	Foliado y en sobre sellado junto con una copia				

ITEM	SOLUCIÓN	PROCESO/ APLICACIÓN	FUNCIONALIDAD / HERRAMIENTA / REQUERIMIENTO	MODO DE VERIFICACIÓN	OBSERVACIÓN	Cumple	No Cumple	No Aplica	Registro (Foto, Filmación)
	Proceso de Homologación del Aspirante		Requisitos Administrativos	* El aspirante a homologación podrá tener subcontrato 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 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. * El aspirante 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: o Establecer un canal dedicado con el sistema RUNT o Establecer las siguientes integraciones requeridas con el sistema RUNT: Solicitud de certificado médico, Solicitud de Cargue de certificado médico, Apertura de interfaces para validación de candidato y médico o especialista + Recepción de certificados médicos + Recepción de licencias de conducción + Recepción de FUPAS o Realizar los procedimientos de conexión y validación de identidad en línea con la Registraduría Nacional del Estado Civil una vez la requiera la Superintendencia de Puertos y Transporte. o Establecer un canal dedicado con el centro de monitoreo de la Superintendencia de Puertos y Transporte o Establecer las siguientes integraciones requeridas con el centro de monitoreo de la Superintendencia de Puertos y Transporte: + Envío de archivo de recaudo + Envío de archivo de eventos + Acceso a software de Posicionamiento Centros de Reconocimiento de Conductores + Generación y envío de archivo de conciliación de actores del proceso *La Superintendencia de Puertos y Transporte se encargara de gestionar las autorizaciones con la Registraduría Nacional del Estado Civil y con el RUNT para establecer los procesos de conexión.*	Foliado y en sobre sellado junto con una copia				

ITEM	SOLUCIÓN	PROCESO/ APLICACIÓN	FUNCIONALIDAD / HERRAMIENTA / REQUERIMIENTO	MODO DE VERIFICACIÓN	OBSERVACIÓN	Cumple	No Cumple	No Aplica	Registro (Foto, Filmación)
6			Requisitos Técnicos	- Compruebe la existencia de los siguientes documentos por parte del aspirante a proveedor: 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 y copia del certificado de registro de soporte lógico de la Dirección Nacional de Derechos de Autor de la compañía fabricante. 2. Adjuntar copia de la solicitud presentada ante la Superintendencia de Industria y Comercio del registro de invención o de modelo de utilidad de un sistema, estructura o dispositivo que tenga relación con el objeto de sistemas de transmisión segura, sistemas de validación de identidad o sistemas de validación de sitios remotos. La solicitud presentada podrá estar en estado de trámite o en estado de concedido el derecho. En caso de no contar con la solicitud anterior el aspirante deberá presentar un documento técnico que permita garantizar la idoneidad del aspirante. El documento técnico deberá contar con los siguientes capítulos: Descripción General del Sistema, Descripción General de Subsistemas, Diagrama de red, arquitectura de servidores, arquitectura general de la aplicación, arquitectura de seguridad en sitios remotos y geo-posicionamiento satelital, esquema de correlación de eventos, esquema para el control de ataques informáticos, esquema de auditoria de bases de datos, esquema de verificación de código fuente, esquema de protección de datos sensibles y de transmisión segura de datos, esquema de intercambio transaccional para el recaudo, diagrama E-R (Entidad Relación) de las principales entidades, documento modelo de arquitectura de software, esquema de alta disponibilidad y continuidad de negocio, en el caso en que el representante legal de la compañía no sea ingeniero de sistemas o electrónico deberá una carta de aval de un ingeniero de sistemas o electrónico.	Foliado y en sobre sellado junto con una copia				
			Requisitos Técnicos	3. Adjuntar copia de contrato de centro de cómputo en caso de que el centro de cómputo se encuentre subcontratado. Los contratos deberán tener una duración mínima de veinticuatro meses. 4. Adjuntar copia de manifiesto de importación de las soluciones de servidores, IPS, Firewall, Herramienta DAM, Herramienta SIEM, Switch de Core, SAN, Escáner de Vulnerabilidades, Application Delivery Controller. 5. Adjuntar copia de las facturas de compra 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 copia de las facturas presentadas podrán ser del proveedor contratado. 6. Adjuntar copia de certificación o indicaciones de como verificar que la herramienta de mesa de ayuda a utilizar cuente con por lo menos 5 procesos de ITIL certificados. 7. Diligenciar el siguiente cuadro de que se encuentra en la hoja "Requerimientos Tecnológicos":					

ITEM	SOLUCIÓN	PROCESO/ APLICACIÓN	FUNCIONALIDAD / HERRAMIENTA / REQUERIMIENTO	MODO DE VERIFICACIÓN	OBSERVACIÓN	Cumple	No Cumple	No Aplica	Registro (Foto, Filmación)
7		Visitas de homologación al aspirante a homologar	Mesa de ayuda	- Compruebe la existencia de los siguientes requerimientos por parte del aspirante a proveedor: 1. La herramienta presentada en la etapa documental para mesa de ayuda deberá estar instalada y se debe mostrar la radicación de una solicitud de soporte. 2. Se debe mostrar la evidencia de los requerimientos que se encuentran en la lista de chequeo en el ítem de "solución de soporte de aspirante a proveedor". 3. La mesa de ayuda deberá estar conformada por el equipo de trabajo presentado en la etapa documental. 4. La mesa de ayuda deberá estar ubicada en territorio nacional.	Evidencia, fotográfica y fílmica				
8			Centro de Operaciones de Seguridad	- Compruebe la existencia de los siguientes requerimientos por parte del aspirante a proveedor: 1. El centro de operaciones de seguridad deberá contar con un control de acceso biométrico. 2. El centro de operaciones de seguridad deberá contar con un sistema de circuito cerrado de televisión. 3. El centro de operaciones de seguridad deberá estar ubicada en territorio nacional. 4. El centro de operaciones de seguridad deberá contar con un video Wall con mínimo cuatro pantallas. 5. 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 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) Prueba de auditoria de base de datos. Se deberá disponer de un cliente del motor de base de datos que permita realizar la modificación en un registro en la tabla en la cual se almacene información biométrica. El evaluador procederá a alterar un registro en la base de datos. Posterior a esto la solución DAM deberá notificará la modificación del registro enviando una alerta al sistema SIEM con la información detallada del incidente. c) Verificación de información biométrica cifrada. El aspirante deberá mostrar la ubicación en la cual almacene la información biométrica con el fin de verificar que esta se encuentre cifrada. d) Verificación de Endpoint. Se deberá demostrar que se encuentran instaladas en los servidores la solución de antimalware. e) Verificación de herramientas de pruebas de seguridad. Se deberá demostrar que están instaladas las herramientas de pruebas de seguridad de aplicación dinámica y estática. f) 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.	Evidencia, fotográfica y fílmica				
9			Centro de Computo	- Verificar que en el centro de cómputo esté en territorio nacional y que esten ubicados todos los equipos de hardware solicitados. En el caso de que los equipos se encuentren en más de un datacenter, se coordinará la visita a todos los datacenter para verificar la totalidad de los equipos solicitados.	Evidencia, fotográfica y fílmica				

ITEM	SOLUCIÓN	PROCESO/ APLICACIÓN	FUNCIONALIDAD / HERRAMIENTA / REQUERIMIENTO	MODO DE VERIFICACIÓN	OBSERVACIÓN	Cumple	No Cumple	No Aplica	Registro (Foto, Filmación)
10			Centro de Reconocimiento de Conductores	- Verificar el funcionamiento del SCV a evaluar. Se procederá a realizar visita aun CRC en el cual se encuentre instalada la solución y se permita verificar los siguientes escenarios: a) Previo a la visita al CRC, se deberá realizar las pruebas de la solución de recaudo con el actor del sistema financiero que se encuentra en la lista de chequeo ítem "Solución con actor del sector financiero". En el caso de requerirse participación de la entidad financiera para realizar esta verificación, el aspirante será el encargado de coordinar todos los requisitos para poder realizar la prueba. b) Verificación del proceso de enrolamiento de candidato. Se deberá demostrar que una aplicación integrada con todo el sistema, realice el registro y toma de información con los dispositivos de captura de información del candidato (lector biométrico de huellas homologado por el RUNT, cámara digital, pistola o escáner de lectura de código bidimensional, pad de firmas). c) Verificación de validación de identidad. Se deberá demostrar que una aplicación integrada con todo el sistema, realice la validación con el procedimiento alternativo temporal de validación de identidad definido. d) Aseguramiento de la presencia del candidato y médico o especialista 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 en el sistema a homologar. e) Los CRC´s por protocolo de seguridad, solo se conectarán a través de red física LAN con el Sistema de Control y Vigilancia, no se permitirán conexiones inalámbricas o WIFI. Se verificará técnicamente que el sistema a homologar cumpla con estas validaciones. f) Verificación de validación de equipos. Se deberá demostrar que una aplicación integrada con todo el sistema, realice la validación los PCS registrados. Se realizarán pruebas con otros PC´s no registrados para verificar la validación. g) Verificación de validación de posición geofísica. Se deberá demostrar que una aplicación integrada con todo el sistema, realice la validación de la geo-posición satelital de dos CRC´s. Se realizaran pruebas técnicas para verificar la validación.	Evidencia, fotográfica y fílmica				
11		Recaudo con actor del sector financiero	Actor vigilado por la Superintendencia Financiera de Colombia	- Compruebe que el actor financiero es vigilado por la Superintendencia Financiera de Colombia a través de la página web www.superfinanciera.gov.co en la sección de "entidades supervisadas" o, certificación entregada directamente por la Superintendencia Financiera de Colombia	Aplicación de Software integrada con la IT, de comunicaciones y dispositivos				
12		Red de	Red de recaudo en territorio nacional	- Compruebe que el actor del sector financiero provea una red de recaudo en territorio nacional propio o en convenio con un corresponsal u aliado de recaudo a través de un certificado emitido por la entidad.	Plataforma directa del actor del sector financiero				

ITEM	SOLUCIÓN	PROCESO/ APLICACIÓN	FUNCIONALIDAD/ HERRAMIENTA / REQUERIMIENTO	MODO DE VERIFICACIÓN	OBSERVACIÓN	Cumple	No Cumple	No Aplica	Registro (Foto, Filmación)
13	Solución con actor del sector financiero	recaudo	Pago del valor del examen de aptitud	- Compruebe que el actor del sector financiero o a través de un corresponsal o aliado de recaudo, adicional al recaudo captura el numero de identificación del candidato. - Compruebe que el actor del sector financiero o a través de un corresponsal o aliado de recaudo, entrega un comprobante con la información de: Numero único de pago, valor de recaudo, numero de identificación del candidato y fecha y hora del pago.	Plataforma directa del actor del sector financiero				
14		Notificación en línea	Notificación de pago del valor del examen de aptitud	- Compruebe que el actor del sector financiero o a través de un corresponsal o aliado de recaudo, envía la notificación en línea del pago al Sistema Central de Control y Vigilancia verificando el almacenamiento de la transacción directamente en la base de datos. - Compruebe que la transacción contenga la siguiente información: * Número Único de Registro o Pago * Fecha de Registro o Pago * Hora de Registro o Pago * Número de identificación del candidato * Valor de Pago * Estado (pago o utilizado) * CRC donde fue utilizado.	Aplicación de Software integrada con la IT, de comunicaciones y dispositivos				
15		Reporte de transacciones	Envío de archivo de recaudo	- Compruebe que el actor del sector financiero o a través de un corresponsal o aliado de recaudo,envía el archivo de recaudo a través de protocolos de intercambio seguro: FTPS, SFTP o HTTPS. - Compruebe que la estructura del archivo que entrega el actor del sistema financiero contenga la siguiente información del recaudo: * Número Único de Registro o Pago * Fecha de Registro o Pago * Hora de Registro o Pago * Número de Identificación del candidato * Valor del Pago * Estado (pago o utilizado) * Fecha del uso del servicio * Hora del uso del servicio * Número Único de Uso - Compruebe que el Sistema Central de Control y Vigilancia almacene toda la información entregada por el actor del sector financiero directamente en la base de datos. - Verifique que el actor del sector financiero envía el archivo de recaudo con periodicidad diaria de todos los pagos realizados	Plataforma directa del actor del sector financiero				

ITEM	SOLUCIÓN	PROCESO/ APLICACIÓN	FUNCIONALIDAD / HERRAMIENTA / REQUERIMIENTO	MODO DE VERIFICACIÓN	OBSERVACIÓN	Cumple	No Cumple	No Aplica	Registro (Foto, Filmación)
16		Administración Básica de Operación	Centros de Reconocimiento de Conductores	- Verifique que la aplicación cuenta con una interfaz de software para administrar Centros de Reconocimiento de Conductores - Compruebe que el registro básico de los Centros de Reconocimiento de Conductores se realice a través de la siguiente información: * Nit * Nombre o Razón Social * Ciudad o municipio de ubicación * Dirección * Teléfono * Correo electrónico * Representante Legal. * Cupos diarios autorizados - Compruebe que la información se encuentra almacenada en la base de datos	Aplicación de Software integrada con la IT de comunicaciones y dispositivos				
17			Excepciones Discapacidades	- Compruebe que la aplicación cuenta con una interfaz de software para administrar excepciones para aspirantes con discapacidades	Aplicación de Software integrada con la IT, de comunicaciones y dispositivos				
18			Información básica	- Verifique que la aplicación cuenta con una interfaz de software para administrar médicos o especialistas - Compruebe que el registro básico de los médicos o especialistas se realice a través de la siguiente información: * Nombres * Apellidos * Identificación * Rol al que corresponde * Centro de Reconocimiento de Conductores al que pertenece - Compruebe que la información se encuentra almacenada en la base de datos	Aplicación de Software integrada con la IT, de comunicaciones y dispositivos				
19			Captura de información dactilar	- Verifique que la aplicación permita seleccionar el dedo para verificar la identidad del médico o especialista. - Compruebe que la aplicación captura la huella de los dedos índice derecho e izquierdo del médico o especialista a través de un lector biométrico de dedo vivo.	Aplicación de Software integrada con la IT, de comunicaciones y dispositivos				

ITEM	SOLUCIÓN	PROCESO/ APLICACIÓN	FUNCIONALIDAD / HERRAMIENTA / REQUERIMIENTO	MODO DE VERIFICACIÓN	OBSERVACIÓN	Cumple	No Cumple	No Aplica	Registro (Foto, Filmación)
20	Solución de soporte	Enrolamiento de médico o especialista	Captura de foto	- Verifique que la aplicación captura la foto del médico o especialista a través de cámara digital. - Compruebe que la aplicación acepta la foto del médico o especialista basado en el estándar ISO/IEC 19794-5, realizando pruebas para determinación de características físicas del rostro de una persona	Aplicación de Software integrada con la IT, de comunicaciones y dispositivos				
21			Protección de información sensible	- Compruebe que la foto, huellas y firma manuscrita digitalizada del médico o especialista que se encuentra en el repositorio de información (base de datos, sistema de archivos), está debidamente cifrada con alguno de los siguientes algoritmos: PGP, AES o RSA	Aplicación de Software integrada con la IT, de comunicaciones y dispositivos				
22			Captura de información biográfica	- Verifique que la aplicación permita capturar y visualizar la información biográfica a través del lector o escáner de código de barras de la cedula de ciudadanía del médico o especialista . - Compruebe que la aplicacion permita seleccionar el dedo con el que se verifica la identidad del médico o especialista. - Compruebe que la aplicación NO permita modificar la información capturada del lector o escáner de código de barras realizando intentos de alteración de datos directamente sobre la interfaz del software	Aplicación de Software integrada con la IT, de comunicaciones y dispositivos				

ITEM	SOLUCIÓN	PROCESO/ APLICACIÓN	FUNCIONALIDAD / HERRAMIENTA / REQUERIMIENTO	MODO DE VERIFICACIÓN	OBSERVACIÓN	Cumple	No Cumple	No Aplica	Registro (Foto, Pimación)
23			Entrega de fotos al Centro de Monitoreo de la SPT	- Compruebe que la aplicación realiza la entrega en línea de las fotos de los médicos o especialistas al centro de monitoreo de la Superintendencia de Puertos y Transporte a través de los siguientes protocolos de intercambio seguro: FTPS, SFTP, HTTP o la designada por la SPT	No se requiere para homologación. Este ITEM se realizara el seguimiento cuando se encuentre homologado el aspirante a prov.				
25		Posicionamiento Centros de Reconocimiento de Conductores	Geo posicionamiento del CRC	- Compruebe que la aplicación registre y almacene el geo posicionamiento del Centro de Reconocimiento de Conductores a través de una interfaz de software donde se visualice por medio de un mapa la posicion geografica del centro.	Aplicación de Software integrada con la IT				
26			Estado de conexión de Centros de Reconocimiento de Conductores y computadores	- Compruebe que la aplicación visualice el estado de conexión del dispositivo de comunicaciones remoto y de cada uno de los computadores del Centro de Reconocimiento de Conductores a través de una interfaz de software.	Aplicación de Software integrada con la IT, de comunicaciones y dispositivos				
27			Validación de pago del valor del examen de aptitud	- Compruebe que la aplicación permite corroborar la veracidad del pago sobre la plataforma del actor del sistema financiero o a través de un corresponsal o aliado de recaudo, en línea ingresando la información del comprobante entregado al candidato al momento del pago.	Aplicación de Software integrada con la IT, de comunicaciones y dispositivos				

ITEM	SOLUCIÓN	PROCESO/ APLICACIÓN	FUNCIONALIDAD / HERRAMIENTA / REQUERIMIENTO	MODO DE VERIFICACIÓN	OBSERVACIÓN	Cumple	No Cumple	No Aplica	Registro (Foto, Filmación)
28		Enrolamiento de candidato	Captura de información dactilar	- Verifique que la aplicación permita seleccionar el dedo para verificar la identidad del candidato. - Compruebe que la aplicación captura la huella de los dedos índice derecho e izquierdo del candidato a través de un lector biométrico de dedo vivo.	Aplicación de Software integrada con la IT, de comunicaciones y dispositivos				
29			Captura de foto	- Verifique que la aplicación captura la foto del candidato a través de cámara digital. - Compruebe que la aplicación acepta la foto del candidato basado en el estándar ISO/IEC 19794-5, realizando pruebas para determinación de características físicas del rostro de una persona	Aplicación de Software integrada con la IT, de comunicaciones y dispositivos				
30			Captura de firma manuscrita digitalizada	- Verifique que la aplicación captura la firma manuscrita digitalizada a través de pad de firmas	Aplicación de Software integrada con la IT, de comunicaciones y dispositivos				
31			Protección de información sensible	- Compruebe que la foto, huellas y firma manuscrita digitalizada del candidato que se encuentra en el repositorio de información (base de datos, sistema de archivos), está debidamente cifrada con alguno de los siguientes algoritmos: PGP, AES o RSA	Aplicación de Software integrada con la IT, de comunicaciones y dispositivos				

ITEM	SOLUCIÓN	PROCESO/ APLICACIÓN	FUNCIONALIDAD / HERRAMIENTA / REQUERIMIENTO	MODO DE VERIFICACIÓN	OBSERVACIÓN	Cumple	No Cumple	No Aplica	Registro (Foto, Filmación)
32			Captura de información biográfica	- Verifique que la aplicación permita capturar y visualizar la información biográfica a través del lector o escáner de código de barras de la cedula de ciudadanía y/o la tarjeta de identidad azul del candidato. - Compruebe que la aplicacion permita seleccionar el dedo con el que se verifica la identidad del candidato. - Compruebe que la aplicación NO permita modificar la información capturada del lector o escáner de código de barras realizando intentos de alteración de datos directamente sobre la interfaz del software	Aplicación de Software integrada con la IT, de comunicaciones y dispositivos				
33			Entrega de fotos al Centro de Monitoreo de la SPT	- Compruebe que la aplicación realiza la entrega en línea de las fotos de los aspirantes al centro de monitoreo de la Superintendencia de Puertos y Transporte a través de los siguientes protocolos de intercambio seguro: FTPS, SFTP, HTTP o la designada por la SPT	No se requiere para homologación. Este ITEM se realizara el seguimientcuando se encuentre homologado el aspirante a prov.				
34			Validación de identidad con la Registraduría Nacional del Estado Civil	- Verifique que el proveedor homologado o a través de un tercero homologado por la RNEC, haya superado las pruebas tecnicas que exige la Registraduría Nacional del Estado Civil para el uso de su infraestructura tecnológica con fines de validación de identidad en línea. - Compruebe que la aplicación se encuentra integrada al AFIS de la Registraduría Nacional del Estado Civil o a través de un tercero homologado por la RNEC, confirmando que existe un enlace de comunicación con la infraestructura física del proveedor homologado y que se visualiza el(los) servicio(s) de validación de identidad en línea - Compruebe que la aplicación utiliza la validación de identidad en línea con la Registraduría Nacional del Estado Civil o a través de un tercero homologado por la RNEC, realizando pruebas con huellas que pertenecen y NO pertenecen al portador del documento de identidad, directamente o a través de un tercero homologado por la RNEC	No se requiere para homologación. Este ITEM se realizara el seguimientcuando se encuentre homologado el aspirante a prov.				

ITEM	SOLUCIÓN	PROCESO/ APLICACIÓN	FUNCIONALIDAD / HERRAMIENTA / REQUERIMIENTO	MODO DE VERIFICACIÓN	OBSERVACION	Cumple	No Cumple	No Aplica	Registro (Foto, Filmación)
35				- Verifique que solo se inicia el procedimiento con el original del documento de identidad. - Compruebe que la aplicación realiza el escaneo del anverso y reverso del documento a mínimo 600 dpi (pixeles por pulgada). - Compruebe que la aplicación almacena las imágenes como soporte del documento presentado por el candidato. - Compruebe que se extrae la información legible del documento con tecnología de reconocimiento de caracteres "OCR". - Verifique que los datos del anverso del documento obtenido por OCR sean como mínimo: *Número de CC *Nombres *Apellidos - Verifique que los datos del reverso del documento obtenido por OCR sean como mínimo: *Fecha de nacimiento *Grupo sanguíneo y RH *Sexo *Código de seguridad.	Aplicación de Software integrada con la infraestructura tecnológica, de comunicaciones y dispositivos				
36				- Compruebe que la aplicación extrae la información que contiene el código de barras bidimensional de la CC. - Verifique que los datos obtenidos del código de barras bidimensional sean como mínimo: *Número de CC *Nombres *Apellidos *Fecha de nacimiento *Grupo sanguíneo y RH *Sexo *Código de seguridad - Compruebe que la información obtenida por la tecnología OCR se compare con la información obtenida del código de barras bidimensional y como mínimo con los siete (7) campos mencionados anteriormente. - Verifique que si existe coincidencias entre los datos comparados, se considere el documento válido para continuar con el proceso de certificación. - Verifique que si no se cumple con la coincidencia de los datos comparados, la aplicación alerte al usuario final (rol de recepcionista) la no coincidencia de datos del OCR comparado con los datos del código de barras. - Verifique que se continúe con el proceso de validación de identidad en cualquiera de los dos casos (comparación exitosa de datos y comparación errada de datos).	Aplicación de Software integrada con la IT, de comunicaciones y dispositivos				

ITEM	SOLUCIÓN	PROCESO/ APLICACIÓN	FUNCIONALIDAD / HERRAMIENTA / REQUERIMIENTO	MODO DE VERIFICACIÓN	OBSERVACIÓN	Cumple	No Cumple	No Aplica	Registro (Foto, Filmación)
37			Validación de identidad con el proceso alternativo temporal para cédulas de ciudadanía "CC"	- Compruebe que existe una extracción de la imagen de la huella dactilar del documento de identidad escaneado. - 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. - Compruebe que se realiza una comparación de las huellas dactilares (huella extraída de la CC contra la huella capturada por el lector biométrico). - Verifique que se obtiene una calificación (score) que se determina por el número de minucias o coincidencias de la comparación, en donde deberá ser mínimo de catorce (14) coincidencias, que es el valor que debe tener el matcher de la aplicación para hacer la comparación y considerar que el portador del documento es el mismo titular, es decir, que la aplicación debe iniciar el proceso de certificación. - Compruebe que el Matcher utilizado deberá contener un algoritmo capaz de resolver la concordancia de huellas dactilares compatible con NIST MINEX. - Verifique que la aplicación continúe con el proceso de validación de identidad si no se cumple con la catorce (14) coincidencias.	Aplicación de Software integrada con la IT, de comunicaciones y dispositivos				
38				- Verifique que la aplicación continúa dentro del proceso de validación de identidad cuando no se pueda realizar la comparación de huellas dactilares para determinar la identidad del candidato (porque carece de la falange del dedo que indica la CC, porque padece de dermatitis, porque la huella impresa en la CC es una huella de baja calidad en la impresión y fue capturada con tinta, porque la huella fue rechazada después de tres intentos de captura o por cualquier otra causa que impida su comparación). - Verifique que la aplicación realice como mínimo cuatro (4) preguntas socio-demográficas del candidato. - Verifique que las preguntas contengan un grupo de posibles respuestas en donde solo una es la correcta. - Verifique que la aplicación inicie el proceso de certificación si el candidato respondió las preguntas. - 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. - Verifique que la aplicación no realice más de dos intentos para validar la identidad del candidato por preguntas socio-demográficas.	Aplicación de Software integrada con la IT, de comunicaciones y dispositivos				

ITEM	SOLUCIÓN	PROCESO/ APLICACIÓN	FUNCIONALIDAD / HERRAMIENTA / REQUERIMIENTO	MODO DE VERIFICACIÓN	OBSERVACIÓN	Cumple	No Cumple	No Aplica	Registro (Foto, Filmación)
39				- Compruebe que la aplicación después de realizar dos intentos de validación de identidad por preguntas socio-demográficas y si a el candidato no se le pudo validar su identidad, la aplicación debe alertar que se podrá iniciar el proceso de certificación, pero no se podrá cargar el certificado obtenido al Registro Único Nacional de Tránsito – RUNT hasta confirmar la identidad del candidato frente al documento presentado. - Compruebe que el proceso de validación de identidad sea ejecutado manualmente por un (1) experto en peritazgo de documentos, grafología y/o dactiloscópia que realizará un proceso de validación de legitimidad del documento de identidad y una comparación dactilar de la huella impresa en la CC contra la capturada por el dispositivo biométrico. - Compruebe que el proceso de validación de identidad manual se realizará con las imágenes de la CC escaneadas (anverso y reverso) y la imagen capturada por el lector biométrico. - Verifique que el proceso de validación de identidad manual no dure más de 24 horas para proporcionar una respuesta a la validación.	Aplicación de Software integrada con la IT, de comunicaciones y dispositivos				
40		Validación de identidad del		- Verifique que solo se inicia el procedimiento con el original de la tarjeta de identidad azul (tarjeta de identidad biométrica) - Compruebe que la aplicación realiza el escaneo del anverso y reverso del documento a mínimo 600 dpi (pixeles por pulgada). - Compruebe que la aplicación almacena las imágenes como soporte del documento presentado por el candidato. - Compruebe que se extrae la información legible del documento con tecnología de reconocimiento de caracteres "OCR". - Verifique que los datos del anverso del documento obtenido por OCR sean como mínimo: *Número de TI *Nombres *Apellidos - Verifique que los datos del reverso del documento obtenido por OCR sean como mínimo: *Fecha de nacimiento *Grupo sanguíneo y RH *Sexo *Código de seguridad.	Aplicación de Software integrada con la IT, de comunicaciones y dispositivos				

ITEM	SOLUCIÓN	PROCESO/ APLICACIÓN	FUNCIONALIDAD / HERRAMIENTA / REQUERIMIENTO	MODO DE VERIFICACIÓN	OBSERVACIÓN	Cumple	No Cumple	No Aplica	Registro (Foto, Filmación)
41		candidato	Validación de identidad con el proceso alternativo temporal para tarjetas de identidad "TI"	- Compruebe que la aplicación extrae la información que contiene el código de barras bidimensional de la TI. - Verifique que los datos obtenidos del código de barras bidimensional sean como mínimo: *Número de TI *Nombres *Apellidos *Fecha de nacimiento *Grupo sanguíneo y RH *Sexo *Código de seguridad - Compruebe que la información obtenida por la tecnología OCR se compare con la información obtenida del código de barras bidimensional y como mínimo con los siete (7) campos mencionados anteriormente. - Verifique que si existe coincidencias entre los datos comparados, se considere el documento como valido para continuar con el proceso de certificación. - Verifique que si no se cumple con la coincidencia de los datos comparados, la aplicación alerte al usuario final (rol de recepcionista) la no coincidencia de datos del OCR comparado con los datos del código de barras. - Verifique que se continúe con el proceso de validación de identidad en cualquiera de los dos casos (comparación exitosa de datos y comparación errada de datos).	Aplicación de Software integrada con la IT, de comunicaciones y dispositivos				
42				- Compruebe que existe una extracción de la imagen de la huella dactilar del documento de identidad escaneado. - Verifique que se obtiene una imagen de la huella dactilar indicada en el documento de identidad con un lector biométrico que posea función de captura de dedo vivo. - Compruebe que se realiza una comparación de las huellas dactilares (huella extraída de la TI contra la huella capturada por el lector biométrico). - Verifique que se obtiene una calificación (score) que se determina por el número de minucias o coincidencias de la comparación, en donde deberá ser minimo de catorce (14) coincidencias, que es el valor que debe tener el matcher de la aplicación para hacer la comparación y considerar que el portador del documento es el mismo titular, es decir, que la aplicación debe iniciar el proceso de certificación. - Compruebe que el Matcher utilizado deberá contener un algoritmo capaz de resolver la concordancia de huellas dactilares compatible con NIST MINEX. - Verifique que la aplicación continúe con el proceso de validación de identidad si no se cumple con la catorce (14) coincidencias.	Aplicación de Software integrada con la IT, de comunicaciones y dispositivos				

ITEM	SOLUCIÓN	PROCESO/ APLICACIÓN	FUNCIONALIDAD / HERRAMIENTA / REQUERIMIENTO	MODO DE VERIFICACIÓN	OBSERVACIÓN	Cumple	No Cumple	No Aplica	Registro (Foto, Filmación)
43	Solución en el Centro de Reconocimiento de Conductores			- Compruebe que la aplicación después de realizar dos intentos de validación de identidad por preguntas socio-demográficas y si a el candidato no se le pudo validar su identidad, la aplicación debe alertar que se podrá iniciar el proceso de certificación, pero no se podrá cargar el certificado obtenido al Registro Único Nacional de Tránsito – RUNT hasta confirmar la identidad del candidato frente al documento presentado. - Compruebe que el proceso de validación de identidad sea ejecutado manualmente por un (1) experto en peritazgo de documentos, grafología y/o dactiloscópia que realizará un proceso de validación de legitimidad del documento de identidad y una comparación dactilar de la huella impresa en la TI contra la capturada por el dispositivo biométrico. - Compruebe que el proceso de validación de identidad manual se realizará con las imágenes de la TI escaneadas (anverso y reverso) y la imagen capturada por el lector biométrico. - Verifique que el proceso de validación de identidad manual no dure más de 24 horas para proporcionar una respuesta a la validación.	Aplicación de Software integrada con la IT, de comunicaciones y dispositivos				
44			Validación de identidad con	- Verifique que solo se inicia el procedimiento con el original del documento de identidad expedido por Migración Colombia. - Compruebe que la aplicación realiza el escaneo del anverso y reverso del documento a mínimo 600 dpi (pixeles por pulgada). - Compruebe que la aplicación almacena las imágenes como soporte del documento presentado por el candidato. - Compruebe que existe una extracción de la imagen de la huella dactilar del documento de identidad escaneado. - Verifique que se obtiene una imagen de la huella dactilar indicada en el documento de identidad con un lector biométrico que posea función de captura de dedo vivo. - Compruebe que se realiza una comparación de las huellas dactilares (huella extraída de la CE contra la huella capturada por el lector biométrico). - Verifique que se obtiene una calificación (score) que se determina por el número de minucias o coincidencias de la comparación. en donde ésta deberá superar las catorce (14) coincidencias que es el valor mínimo que se debe tener el matcher de la aplicación para hacer la comparación y considerar que el portador del documento es el mismo titular, es decir que la aplicación debe iniciar el proceso de certificación. - Verifique que la solución de los aspirantes a proveedores no exceda un máximo de tres intentos de captura y comparación antes de descartar éste mecanismo como una validación de identidad. - Compruebe que el Matcher utilizado deberá contener un algoritmo capaz de resolver la concordancia de huellas dactilares compatible con NIST MINEX. - Verifique que la aplicación continúe con el proceso de validación de identidad si no se cumple con las catorce (14) coincidencias.	Aplicación de Software integrada con la IT, de comunicaciones y dispositivos				

ITEM	SOLUCIÓN	PROCESO/ APLICACIÓN	FUNCIONALIDAD / HERRAMIENTA / REQUERIMIENTO	MODO DE VERIFICACIÓN	OBSERVACIÓN	Cumple	No Cumple	No Aplica	Registro (Foto, Filmación)
45			identidad con el proceso alternativo temporal para cédulas de extranjería "CE"	- Verifique que la aplicación continúa dentro del proceso de validación de identidad cuando no se pueda realizar la comparación de huellas dactilares para determinar la identidad del candidato (porque carece de la falange del dedo que indica la CE, porque padece de dermatitis, porque la huella impresa en la CE es una huella de baja calidad en la impresión y fue capturada con tinta, porque la huella fue rechazada después de tres intentos de captura o por cualquier otra causa que impida su comparación). - Verifique que la aplicación realice como mínimo cuatro (4) preguntas socio-demográficas del candidato. - Verifique que las preguntas contengan un grupo de posibles respuestas en donde solo una es la correcta. - Verifique que la aplicación inicie el proceso de certificación si el candidato respondió las preguntas. - 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. - Verifique que la aplicación no realice más de dos intentos para validar la identidad del candidato por preguntas socio-demográficas.	Aplicación de Software integrada con la IT, de comunicaciones y dispositivos				
46				- Compruebe que la aplicación después de realizar dos intentos de validación de identidad por preguntas socio-demográficas y si a el candidato no se le pudo validar su identidad, la aplicación debe alertar que se podrá iniciar el proceso de certificación, pero no se podrá cargar el certificado obtenido al Registro Único Nacional de Tránsito – RUNT hasta confirmar la identidad del candidato frente al documento presentado. - Compruebe que el proceso de validación de identidad sea ejecutado manualmente por un (1) experto en peritazgo de documentos, grafología y/o dactiloscópia que realizará un proceso de validación de legitimidad del documento de identidad y una comparación dactilar de la huella impresa en la CE contra la capturada por el dispositivo biométrico. - Compruebe que el proceso de validación de identidad manual se realizará con las imágenes de la CE escaneadas (anverso y reverso) y la imagen capturada por el lector biométrico. - Verifique que el proceso de validación de identidad manual no dure más de 24 horas para proporcionar una respuesta a la validación.	Aplicación de Software integrada con la IT, de comunicaciones y dispositivos				
47			Uso de pago del valor del examen de aptitud	- Compruebe que la aplicación consume el pago del examen de aptitud después de obtener la validación de identidad como exitosa y/o pendiente de comprobar validación. - Compruebe el estado del pago nuevamente en la interfaz de "Validación de pago del valor del examen de aptitud". El mensaje debe indicar al usuario que el pago ya fue consumido con anterioridad.	Aplicación de Software integrada con la IT, de comunicaciones y dispositivos				

ITEM	SOLUCIÓN	PROCESO/ APLICACIÓN	FUNCIONALIDAD / HERRAMIENTA / REQUERIMIENTO	MODO DE VERIFICACIÓN	OBSERVACIÓN	Cumple	No Cumple	No Aplica	Registro (Foto, Filmación)
48		Aseguramiento de presencia del candidato y mpedico o especialista en el proceso de evaluación médica	Verificación de identidad al inicio y al final de cada evaluación médica	- Verifique que la interfaz de validación de identidad del candidato y del médico o especialista se despliega al momento de iniciar el proceso de evaluación médica - Verifique que la interfaz de validación de identidad del candidato y del médico o especialista se despliega al momento de finalizar el proceso de evaluación médica - Compruebe la validación dactilar exitosa cuando se ingresa sobre el biométrico la misma huella de un candidato registrada al momento de su enrolamiento - Compruebe la validación dactilar exitosa cuando se ingresa sobre el biométrico la misma huella de un médico o especialista registrada en al momento de su enrolamiento - Compruebe la validación dactilar fallida cuando se ingresa sobre el biométrico una huella diferente del candidato (de otro dedo o de otra persona) de la registrada al momento de su enrolamiento - Compruebe la validación dactilar fallida cuando se ingresa sobre el biométrico una huella diferente del médico o especialista (de otro dedo o de otra persona) de la registrada al momento de su enrolamiento	Aplicación de Software integrada con la IT, de comunicaciones y dispositivos				
49			Envío de resultados de evaluación médica	- Compruebe que la aplicación de software del Centro de Reconocimiento de Conductores que almacena los resultados de la evaluación médica del candidato, envía la información correspondiente segun los criterios de evaluación . Esta información debe estar alojada en la Base de Datos del Sistema Central de Control y Vigilancia.	Aplicación de Software integrada con la IT, de comunicaciones y dispositivos				
50			Solicitud de certificado médico	- Verifique que la apertura de la interfaz "solicitud de certificado médico" del sistema RUNT se realice desde el Sistema de Control y Vigilancia	No se requiere para homologación. Este ITEM se realizara el seguimiento cuando encuentre homologado el aspirante a prov.				

ITEM	SOLUCIÓN	PROCESO/ APLICACIÓN	FUNCIONALIDAD / HERRAMIENTA / REQUERIMIENTO	MODO DE VERIFICACIÓN	OBSERVACIÓN	Cumple	No Cumple	No Aplica	Registro (Foto, Filmación)
51			Solicitud de cargue de certificado médico	- Compruebe que la aplicación permita la apertura de la interfaz "cargue de certificado médico" del sistema RUNT una vez se encuentren realizadas todas las pruebas médicas. - Verifique que la apertura de la interfaz "cargue de certificado médico" del sistema RUNT a través del Sistema de Control y Vigilancia	No se requiere para la homologación. Este ITEM se realizara el seguimiento cuando se encuentre homologado el aspirante a prov.				
52			Apertura de interfaces para validación de candidato y médico o especialista	- Compruebe que la aplicación permita la apertura de la interfaz de "validación de médico o especialista" del sistema RUNT a través del Sistema de Control y Vigilancia	No se requiere para homologación. Este ITEM se realizara el seguimiento cuando se encuentre homologado el aspirante a prov.				

ITEM	SOLUCIÓN	PROCESO/ APLICACIÓN	FUNCIONALIDAD / HERRAMIENTA / REQUERIMIENTO	MODO DE VERIFICACIÓN	OBSERVACIÓN	Cumple	No Cumple	No Aplica	Registro (Foto, Filmación)
53		Integración con Sistema RUNT	Recepción de certificados médicos	- Compruebe que la aplicación recibe el archivo de certificados cargados en el sistema RUNT a través de protocolos de intercambio seguro: FTPS, SFTP o HTTPS. - Compruebe que la aplicación recibe el archivo de certificados cargados en el RUNT basado en la siguiente estructura: * Número de Solicitud * Número de Certificado * Fecha de expedición del Certificado * Fecha de Registro de la Solicitud * Estado del Trámite * Número de FUPAS del Consumo * ID del CRC * Nombre del CRC * NIT del CRC * Nombres del Candidato * Documento del Candidato * Categoría del Certificado * Nombre del Trámite * Estado del Certificado * Decisión de certificación	No se requiere para la homologación. Este ITEM se realizara el seguimiento una vez se encuentre homologado el aspirante a proveedor.				
54			Recepción de licencias de conducción	- Compruebe que la aplicación recibe el archivo de licencias de conducción cargadas en el sistema RUNT a través de protocolos de intercambio seguro: FTPS, SFTP o HTTPS. - Compruebe que la aplicación recibe el archivo de licencias de conducción cargadas en el sistema RUNT basado en la siguiente estructura: * Tipo documento de identificación del candidato * Número de Documento de identificación del candidato * Nombres del Candidato * Apellidos del Candidato * Estado Candidato * Número Licencia conducción * Categoría antigua * Categoría actual * Fecha vencimiento * Estado de la licencia * OT que expide la licencia * Fecha refrendación * Vigencia examen médico.	No se requiere para homologación. Este ITEM se realizara el seguimientc uando se encuentre homologado el aspirante a prov.				

ITEM	SOLUCIÓN	PROCESO/ APLICACIÓN	FUNCIONALIDAD / HERRAMIENTA / REQUERIMIENTO	MODO DE VERIFICACIÓN	OBSERVACIÓN	Cumple	No Cumple	No Aplica	Registro (Foto, Filmación)
55			Recepción de FUPAS	- Compruebe que la aplicación recibe el archivo de FUPAS consumidas en el sistema RUNT a través de protocolos de intercambio seguro: FTPS, SFTP o HTTPS. - Compruebe que la aplicación recibe el archivo de FUPAS consumidas en el sistema RUNT basado en la siguiente estructura: * NIT del CRC * Identificador de FUPAS * Numero de certificado asociado	No se requiere para homologación. Este ITEM se realizara el seguimiento cuando se encuentre homologado el aspirante a prov.				
56		Conexión segura con Sistema Central de	Comunicación con Sistema Central de Control y Vigilancia	- Verifique que el Centro de Reconocimiento de Conductores cuente con internet y Red LAN física. - Verifique que el Centro de Reconocimiento de Conductores cuente con una IP Publica Fija - Compruebe que la comunicación de los computadores del Centro de Reconocimiento de Conductores al Sistema Central de Control y Vigilancia se realice a través de una conexión segura (Tunel SSH o IPSec) verificando a través de la consola de administración del Firewall ubicado en el centro de datos del aspirante a proveedor	Requerido para homologación				
57			Dispositivo de comunicaciones remoto	- Verifique que en las instalaciones del Centro de Reconocimiento de Conductores se encuentre instalado físicamente un dispositivo de comunicaciones remoto - Compruebe que el dispositivo de comunicaciones remoto se encuentra activo, conectado a una fuente de energía y a la red interna del Centro de Reconocimiento de Conductores, validando el estado de conexión del centro en la interfaz de software de soporte del aspirante a proveedor. - Compruebe que el dispositivo de comunicaciones remoto genera desconexión del Centro de Reconocimiento de Conductores por movimiento del dispositivo, por perdida de energía y por perdida de red interna del centro, verificando a través de una interfaz de software de soporte del aspirante a proveedor validando el estado y el log de evento de dicha desconexión.	Requerido para homologación				

ITEM	SOLUCIÓN	PROCESO/ APLICACIÓN	FUNCIONALIDAD / HERRAMIENTA / REQUERIMIENTO	MODO DE VERIFICACIÓN	OBSERVACIÓN	Cumple	No Cumple	No Aplica	Registro (Foto, Filmación)
58		Control y Vigilancia	ID's de componentes de computadores	- Verifique que el agente de software que realiza la captura de los ID's de componentes de los computadores del Centro de Reconocimiento de Conductores se encuentra instalado en cada PC. - Compruebe que los ID's de los componentes (tarjeta madre, disco duro, tarjeta de red física, BIOS y Sistema Operativos) de los computadores del Centro de Reconocimiento de Conductores se encuentran en el Sistema Central de Control y Vigilancia, verificando su almacenamiento a través de la interfaz de software de soporte o directamente en la base de datos del aspirante a proveedor - Compruebe que al NO efectuar cambios físicos a los componentes (tarjeta madre, disco duro, tarjeta de red física, BIOS y/o Sistema Operativos) de los computadores del Centro de Reconocimiento de Conductores NO genera desconexión con el Sistema Central de Control y Vigilancia, validando el estado en una interfaz de software de soporte del aspirante a proveedor. - Compruebe que los cambios físicos a los componentes (tarjeta madre, disco duro, tarjeta de red física, BIOS y/o Sistema Operativos) de los computadores del Centro de Reconocimiento de Conductores genera desconexión al Sistema Central de Control y Vigilancia, validando el estado y el log del evento en una interfaz de software de soporte del aspirante a proveedor.	Aplicación de Software integrada con la IT, de comunicaciones y dispositivos				

ITEM	SOLUCIÓN	PROCESO/ APLICACIÓN	FUNCIONALIDAD / HERRAMIENTA / REQUERIMIENTO	MODO DE VERIFICACIÓN	OBSERVACIÓN	Cumple	No Cumple	No Aplica	Registro (Foto, Filmación)
59	Solución de Conciliación	Conciliación de los actores del proceso	Generación de archivo de conciliación	- Compruebe que la aplicación genera el archivo de conciliación de actores del proceso basado en la siguiente estructura: * Tipo identificación del candidato * Numero identificación del candidato * Fecha de registro o pago en la entidad financiera * Hora de registro o pago en la entidad financiera * Nombre de la entidad financiera * Departamento de pago * Municipio de pago * Medio de pago * Valor de pago * Tipo de Servicio prestado en el Centro de Reconocimiento (moto, automóvil, moto y automóvil) * Categoría de la licencia * Tipo de trámite (refrendación, re-categorización, nueva licencia) * Nombre del Centro de Reconocimiento de Conductores * Nombre del Organismo Certificador de Personas * Nombre de especialistas que participaron en el proceso de certificación * Resultado del proceso de certificación (atestación) * Numero de certificado emitido en el Sistema de Control y Vigilancia * Numero de certificado emitido en el RUNT * Decisión de certificación en el RUNT * Decisión de certificación en el Sistema de Control y Vigilancia	No se requiere para la homologación. Este ITEM se realizara el seguimiento cuando se encuentre homologado el aspirante a prov.				
60		Conexión con el actor del sistema financiero	Canal dedicado con actor del sector financiero	- Compruebe que el aspirante a proveedor cuenta con un canal dedicado con el actor del sector financiero a través del contrato con el proveedor tecnológico - Verifique que la capacidad mínima del canal dedicado es de 1 Mbps - Verifique que el canal dedicado es VPN Site to Site	Requerido para homologación				

ITEM	SOLUCIÓN	PROCESO/ APLICACIÓN	FUNCIONALIDAD / HERRAMIENTA / REQUERIMIENTO	MODO DE VERIFICACIÓN	OBSERVACIONES	Cumple	No Cumple	No Aplica	Registro (Foto, Filmación)
61	Solución de Comunicaciones con actores del proceso	Conexión con el sistema RUNT	Canal dedicado con concesión RUNT	- Compruebe que el aspirante a proveedor cuenta con un canal dedicado con el sistema RUNT a través del contrato con el proveedor tecnológico - Verifique que la capacidad mínima del canal dedicado es de 2 Mbps	No se requiere para homologación. Este ITEM se realizara el seguimiento cuando se encuentre homologado el aspirante a prov.				
62		Conexión con los CRC's	Canal de internet con los CRC	- Compruebe que el aspirante a proveedor cuenta con un canal de internet con los Centros de Reconocimiento basado en el siguiente calculo: * 250 Kbps x Cantidad de Centros de Reconocimiento de Conductores esperados a integrarse con la plataforma del aspirante a proveedor	Requerido para homologación				
63		Conexión con la Superintendencia de Puertos y Transporte	Canal dedicado con la Superintendencia de Puertos y Transporte	- Compruebe que el aspirante a proveedor cuenta con un canal dedicado con el centro de monitoreo de la Superintendencia de Puertos y Transporte a través del contrato con el proveedor tecnológico - Verifique que la capacidad mínima del canal dedicado es de 1 Mbps	No se requiere para la homologación. Este ITEM se realizara el seguimiento una vez se encuentre homologado el aspirante a prov.				

ITEM	SOLUCIÓN	PROCESO/ APLICACIÓN	FUNCIONALIDAD / HERRAMIENTA / REQUERIMIENTO	MODO DE VERIFICACIÓN	OBSERVACIÓN	Cumple	No Cumple	No Aplica	Registro (Foto, Filmación)
64	Solución integración al Centro	Reporte de transacciones de recaudo	Envío de archivo de recaudo	- Compruebe que la aplicación envía los reportes de recaudo a través de protocolos de intercambio seguro: FTPS, SFTP o HTTPS. - Compruebe que la aplicación envía los reportes de recaudo basado en la periodicidad exigida por la Superintendencia de Puertos y Transporte.	No se requiere para homologación. Este ITEM se realizara el seguimiento cuando se encuentre homologado el aspirante a prov.				
65		Reporte de eventos del sistema	Envío de archivo de eventos	- Compruebe que la aplicación envía los reportes de eventos del sistema SIEM a través de protocolos de intercambio seguro: FTPS, SFTP o HTTPS. - Compruebe el cumplimiento de la siguiente estructura del archivo: * Id evento (consecutivo) * Cuando (fecha y hora) * Quien (nombre de la persona, usuario de red ó usuario de la aplicación) * Que hizo (tipo de evento) * Resultado (exitoso , fallido, alerta) * Donde (aplicación destino, s.o. destino, nombre máquina destino) * Desde donde (ip origen, nombre máquina origen) * Hacia a donde (aplicación destino, s.o destino, nombre máquina destino) * Sobre que (protocolo, puertos, aplicación, script, archivo, path)	No se requiere para homologación. Este ITEM se realizara el seguimiento cuando se encuentre homologado aspirante a prov.				

ITEM	SOLUCIÓN	PROCESO/ APLICACIÓN	FUNCIONALIDAD / HERRAMIENTA / REQUERIMIENTO	MODO DE VERIFICACIÓN	OBSERVACIÓN	Cumple	No Cumple	No Aplica	Registro (Foto, Filmación)
66	de Monitoreo de la SPT	Solución de ubicación de Centros de Reconocimiento de Conductores	Acceso a software de Posicionamiento Centros de Reconocimiento de Conductores	- Compruebe que desde la Superintendencia de Puertos y Transporte se permite el acceso al Sistema de Posicionamiento Centros de Reconocimiento de Conductores que se encuentra en la solución de soporte del aspirante a proveedor. - Compruebe que tiene acceso a las funcionalidades de "Geo posicionamiento del Centro de Reconocimiento de Conductores" y "Estado de conexión de Centros de Reconocimiento de Conductores y computadores"	No se requiere para homologación. Este ITEM se realizara el seguimiento cuando se encuentre homologado el aspirante a prov.				
67		Reporte de conciliación	Envío de archivo de conciliación de actores del proceso	- Compruebe que la aplicación envía el reporte de conciliación de actores del proceso (descrita en la Solución de Conciliación) a través de protocolos de intercambio seguro: FTPS, SFTP o HTTPS	No se requiere para homologación. Este ITEM se realizara el seguimiento cuando se encuentre homologado el aspirante a prov.				