RESOLUCIÓN 13830 DE 2014

(septiembre 23)

Diario Oficial No. 49.289 de 29 de septiembre de 2014

SUPERINTENDENCIA DE PUERTOS Y TRANSPORTE

Por la cual se expide al anexo técnico para la implementación de los Sistemas de Control y Vigilancia ordenado a través de la Resolución número 9304 del 24 de diciembre de 2012.

Resumen de Notas de Vigencia

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 44del Decreto número 101 de 2000, la Ley 105 de 1993, Ley 336 de 1996, entre otras, y

CONSIDERANDO:

De conformidad con el artículo 41 del Decreto número 101 de 2000, modificado por el Decreto número 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**o** del artículo 3**o** 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 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 Diagnóstico Automotor definidos en el artículo 20 ibídem en los siguientes términos:

"Centro de diagnóstico automotor: Ente estatal o privado destinado al examen técnico-mecánico de vehículos automotores y a la revisión del control ecológico conforme a las normas ambientales.

Así mismo, el artículo 28 de la Ley 769 de 2002 (modificado por el artículo 8**o** de la ley 1383 de 2010) determina que:

“Para que un vehículo pueda transitar por el territorio nacional, debe garantizar como mínimo un perfecto funcionamiento de frenos, del sistema de dirección, del sistema de suspensión, del sistema de señales visuales y audibles permitidas y del sistema de escape de gases; y demostrar un estado adecuado de llantas, del conjunto de vidrios de seguridad y de los espejos y cumplir con las normas de emisiones contaminantes que establezcan las autoridades ambientales”.

Que el artículo 50 de la misma ley (modificado por el artículo 10 de la Ley 1383 de 2010) señala que:

“Por razones de seguridad vial y de protección al ambiente, el propietario o tenedor del vehículo de placas nacionales o extranjeras, que transite por el territorio nacional, tendrá la obligación de mantenerlo en óptimas condiciones mecánicas, ambientales y de seguridad”.

Conforme a lo previsto en el artículo 53 de la Ley 769 de 2002 (modificado por el artículo 203del Decreto número 019 de 2012):

“La revisión técnico-mecánica y de emisiones contaminantes se realizará en centros de diagnóstico automotor, legalmente constituidos, que posean las condiciones que determinen los reglamentos emitidos por el Ministerio de Transporte y el Ministerio de Ambiente y Desarrollo Sostenible, en lo de sus competencias. El Ministerio de Transporte habilitará dichos centros, según la reglamentación que para tal efecto expida. Los resultados de la revisión técnico-mecánica y de emisiones contaminantes, serán consignados en un documento uniforme cuyas características determinará el Ministerio de Transporte.

También en el artículo 54 de la precitada ley (modificado por el artículo 14 de la Ley 1383 de 2010) dispone que:

“Los Centros de Diagnóstico Automotor llevarán un registro computarizado de los resultados de las revisiones técnico-mecánicas y de emisiones contaminantes de cada vehículo, incluso de los que no la aprueben”.

De igual forma la Resolución número 3500 de 2005 en su artículo 31, modificado por el artículo 14 de la Resolución número 2200 de 2006, establece que:

“La Superintendencia de Puertos y Transporte será la entidad encargada de vigilar y controlar a los Centros de Diagnóstico Automotor y a los Organismos de certificación”.

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 documental 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.

En virtud de lo anterior, la Superintendencia de Puertos y Transporte expidió la Resolución número 9304 del 24 de diciembre de 2012, donde se reglamentan las medidas Tecnológicas

que deben implementar cada uno de los Centros de Diagnóstico Automotor, además del Sistema de Control y Vigilancia contemplado en el Capítulo II del referido acto administrativo.

En cumplimiento de la Ley 1450 de 2011 y la Resolución número 9304 del 24 de diciembre de 2012 y de conformidad con la Ley 80 de 1993 modificada por la Ley 1150 de 2007, su Decreto Reglamentario número 734 de 2012 y previo a la expedición por parte de la Entidad de la Resolución número 14181 del 22 de octubre de 2013, "por medio de la cual se justifica una contratación directa" la Superintendencia de Puertos y Transportes celebró el Contrato Interadministrativo número 321 del 23 de octubre de 2013 con la Universidad Pedagógica y Tecnológica de Colombia identificada con NIT 891.800.330-1, en la modalidad de contratación directa, por un término de tres (3) meses, cuyo objeto consiste en "prestación de servicios profesionales para la elaboración del anexo técnico para la homologación de los Sistemas de Control y Vigilancia ordenados mediante la Resolución número 9304 de 2012 expedida por la Supertransporte.

Mediante Radicado número 2014-560056900-2 del 04/09/2014 la Universidad Pedagógica y Tecnológica de Colombia hizo entrega, a la Superintendencia de Puertos y Transporte del objeto del Contrato número 321 del 23 de octubre de 2013, esto es del "Anexo Técnico para la homologación de los Sistemas de Control y Vigilancia".

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

RESUELVE:

ARTÍCULO 1o. Expedir el anexo técnico para la Verificación y Evaluación de los requisitos para la implementación de los Sistemas de Control y Vigilancia ordenado a través de la Resolución número 9304 del 24 de diciembre de 2012 proferida por la Superintendencia de Puertos y Transporte.

ARTÍCULO 2o. TÉRMINOS PARA LA EXIGIBILIDAD DE LAS DISPOSICIONES CONTENIDAS EN LA PRESENTE RESOLUCIÓN. Modificar el término inicial de seis (6) meses de que trata el artículo 7o de la Resolución número 9304 del 2012, en sentido de reducir a cuatro (4) meses la implementación y aplicación de todas las disposiciones técnicas del Sistema de Control y Vigilancia por parte de todos los centros de diagnóstico automotor, dicho término, comenzará a partir del momento en que el segundo proveedor haya cumplido a cabalidad el 100% del proceso de evaluación y verificación de los requisitos exigidos en esta resolución.

ARTÍCULO 2o. <sic, es 3o>. El Sistema de Control y Vigilancia (SICOV) para los Centros de Diagnóstico Automotor (CDA), solo comenzará a operar a partir de que existan como mínimo dos (2) proveedores que hayan cumplido a cabalidad el 100% de todos los requisitos exigidos en esta resolución, y el proceso de evaluación y verificación de los mismos. Y que además se

demuestre que los dos proveedores tengan contratación real con los CDA y no sólo cumplimiento de requisitos en documentos.

La presente resolución rige a partir de la fecha de su publicación.

Notifíquese y cúmplase.

23 de septiembre de 2014

El Superintendente de Puertos y Transporte (E),

GABRIEL OSVALDO ALBARRACÍN DÍAZ.

REQUISITOS TÉCNICOS INFRAESTRUCTURA TECNOLÓGICA Y DE COMUNICACIONES – SISTEMA DE CONTROL Y VIGILANCIA PARA LOS CENTROS DE DIAGNÓSTICO AUTOMOTOR.

PARA EL CDA

Rack de Equipos:

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

-- Altura mínimo de 1.80 metros, 38 Unidades de Rack.

-- Tendrán mínimo dos extractores debidamente conectados a un circuito normal.

-- Serán armados con sus respectivos organizadores y cuatro (4) rieles ajustables para equipos de 19” de ancho, además debe incluir un barraje de puesta a tierra (TGB).

-- Tendrán vidrio templado en la parte frontal de la puerta con posibilidad de desmontar sus tapas laterales y traseras.

-- El rack suministrará una multi-toma de mínimo (10 salidas eléctricas) con supresor de transientes conectado a la UPS a través de un circuito independiente de la red regulada, realizando las adecuaciones eléctricas requeridas.

-- Debe llevar bandejas porta equipos según la necesidad del sitio.

Estaciones de trabajo / Servidor o Terminales de Captura y Procesamiento de Video

DESCRIPCIÓN REQUERIMIENTOS MÍNIMOS.

Workstation o Servidor video

PROCESADOR Tecnología:

	-- INTEL Xeon® Processor o superior (64 bits) -- AMD Phenom X4 Quad (64 bits) Velocidad -- INTEL: =3.0 GHz o superior -- AMD: =2.6 GHz o superior
MEMORIA CACHE	10 MB o superior
Memoria RAM	16GB o superior
Almacenamiento Interno	2Tb SATA 6Gb/s 7200rpm o superior
Soporte para RAID	0, 1, 5, 10
TARJETA GRAFICADORA	-- Compatibilidad pantalla 100% -- Resolución. La misma de la pantalla o superior -- Memoria =1GB, independiente de la Board -- Arquitectura PCI EXPRESS -- Soporte para múltiples tarjetas de video -- Soporte para Nvidia SLI o ATI CrossFire
Interface de Red Ethernet LAN	-- 10/100/1000
Fuente de Poder	-- Mínimo 500W reales
Garantía para Soporte en Sitio y repuestos	-- 3 años
Monitor	Alto desempeño 17” o Superior

CÁMARAS PARA ANALÍTICA DE VIDEO UBICADAS EN LOS CDA'S

Las siguientes son las características Mínimas que deberán tener las cámaras:

-- Formato 1080 progresivo (HD) 1920 * 1080.

-- Iluminadores de 25 metros.

-- Cámara día / noche.

-- Protección contra agua y polvo IP66 y/o NEMA 4X

-- Protección de impactos IK08.

-- Compensación de contraluz.

-- Detección de saboteo.

-- Análisis de video por movimiento.

-- Temperatura de operación de -30 oC a +50 oC (de -22 oF a +122 oF).

-- Humedad relativa de 90%.

-- Opción de encripción AES de 128 o 256 Bits.

-- Certificación CE, FCC, UL, Onvif.

-- Protocolos soportados mínimo: IPv4, IPv6, RTP, RTSP, HTTP, SNMP, Telnet.

-- Soportando flujos multimedia en los siguientes formatos: H.264, MJPEG.

-- Eliminación de ruido para mejorar rendimiento en condiciones de baja iluminación.

EQUIPOS DE COMUNICACIONES, - CONECTIVIDAD

Switches de Red:

-- Nivel 3 Administrable

-- Mínimo 12 puertos Fast Ethernet

-- Velocidad 10/100/1000 Mbps

-- Apilable, o para Rack

-- Sin Ventiladores

-- Debe manejar cifrado integrado por capa de sockets seguros (SSL)

-- Debe ofrecer manejo de listas de control de acceso (ACL)

-- Funcionalidad VLAN

-- Debe usar la inspección dinámica del protocolo de resolución de direcciones (ARP), protección de IP de origen y detección del protocolo DHCP, que permiten detectar y bloquear ataques deliberados de la red.

-- Compatibilidad con IPv6

Firewall:

Prestaciones de Software

-- Gestión Unificada de Amenazas (antivirus en pasarela, antispyware, prevención de intrusiones, Application Intelligence and Control, antispam, filtrado de contenido, Enforced Client Anti-Virus y antispyware)

-- Comprehensive Anti-Spam Service

-- SSL VPN e IPSec VPN

-- Sistema de Gestión Global

-- Throughput superior a 500 Mbps

-- Para VPN

- Rendimiento 3DES/AES 75 Mbps

- Túneles VPN entre emplazamientos

- Permitir Cifrado/autenticación/grupo DH DES, 3DES, AES (128, 142, 256 bits), MD5, SHA-1/grupo DH 1, 2, 5, 14

- Permitir Intercambio de claves IKE, clave manual, Certificados (X.509), L2TP sobre IPSec

- Soporte de certificados

- Prestaciones VPN Dead Peer Detection, DHCP a través de VPN, IPSec NAT Traversal, pasarela VPN redundante, VPN basada en enrutamiento.

- Plataformas Global VPN Client soportadas Microsoft® Windows 2000, Windows XP, Vista 32 bits/64 bits, Windows 7 32/64 bits

- Plataformas SSL VPN para Sistemas Operativos Microsoft Windows XP, Vista, 7, MacOS 10.4 y sistemas operativos Linux.

- Plataforma Mobile Connect soportada iOS 4.2 y superior

-- Prestaciones Servicios de seguridad:

- Servicios de inspección profunda de paquetes Gateway Anti-Virus, Anti-Spyware and Intrusion Prevention

- Servicios de filiado Web basada en categorías y filtrado de contenido para tráfico http y https con la posibilidad de aplicar a un usuario o grupos de usuarios con controles de ancho de banda a cada uno de estos perfiles.

-- Prestaciones de Red

- Asignación de direcciones IP Estática, (cliente DHCP, PPPoE, L2TP y PPTP), servidor DHCP interno

- Modos NAT 1:1, 1:muchos, muchos:1, muchos: muchos, NAT flexible (IPs solapadas), PAT, modo transparente

- VLANS

- DHCP Servidor interno

- Enrutamiento

- Autenticación Radius, LDAP, Base de datos local y la posibilidad de soportar SSO con directorios externos como Active Directory y Novell.

Prestaciones de Hardware

-- Interfaces Ethernet – Wan / Lan

-- 3G inalámbrico (opcional)

-- Puertos USB

-- Potencia de entrada 100 a 240 VAC, 50-60 Hz, 1 A

-- Certificaciones Common Criteria EAL4+, FIPS 140-2, ICSA Firewall 4.1

-- Conformidad con normas FCC Class B, CE, C-Tick, VCCI Class B, TÜV/GS, CB

Entorno/humedad 32-105o F, 0-40o C/ 5-95% sin condensación

SISTEMA DE SUMINISTRO DE CORRIENTE

SAI o UPS:

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

A esta UPS se deben conectar y debe soportar el rack de comunicaciones que contiene los equipos que integran el SISTEMA DE CONTROL Y VIGILANCIA PARA LOS CENTROS DE DIAGNÓSTICO AUTOMOTOR.

PARA EL SOC

Rack de Equipos:

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

-- Altura mínimo de 1.8 metros, 38 Unidades de Rack

-- Tendrán mínimo dos extractores debidamente conectados a un circuito normal.

-- Serán armados con sus respectivos organizadores y cuatro (4) rieles ajustables para equipos de 19” de ancho, además debe incluir un barraje de puesta a tierra (TGB).

-- Tendrán malla en la parte frontal de la puerta con posibilidad de desmontar sus tapas laterales y traseras.

-- Doble multitoma de mínimo (10 salidas eléctricas) con supresor de transiente conectado a la UPS a través de un circuito independiente de la red regulada, realizando las adecuaciones eléctricas requeridas.

-- Debe llevar bandejas porta equipos según la necesidad del sitio.

EQUIPOS DE COMUNICACIONES, - CONECTIVIDAD

Switches de Red:

-- Nivel 3 Administrable

-- Mínimo 24 puertos Fast Ethernet

-- Velocidad 10/100/1000 Mbps

-- Para Rack

-- Debe manejar cifrado integrado por capa de sockets seguros (SSL)

-- Debe ofrecer manejo de listas de control de acceso (ACL)

-- Funcionalidad VLAN

-- Debe usar la inspección dinámica del protocolo de resolución de direcciones (ARP), protección de IP de origen y detección del protocolo DHCP, que permiten detectar y bloquear ataques deliberados de la red.

-- Compatibilidad con IPv6

Firewall:

-- Gestión Unificada de Amenazas (antivirus en pasarela, antispyware, prevención de intrusiones, Application Intelligence and Control, antispam, filtrado de contenido, Enforced Client Anti-Virus y antispyware)

-- Comprehensive Anti-Spam Service

-- SSL VPN e IPSec VPN

-- Sistema de Gestión Global

-- Throughput superior a 500 Mbps

-- Para VPN

- Rendimiento 3DES/AES4 75 Mbps

- Túneles VPN entre emplazamientos

- Permitir Cifrado/autenticación/grupo DH DES, 3DES, AES (128, 142, 256 bits), MD5, SHA-1/grupo DH 1, 2, 5, 14

- Permitir Intercambio de claves IKE, clave manual, Certificados (X.509), L2TP sobre IPSec

- Soporte de certificados Verisign, Thawte, Cybertrust, RSA Keon, Entrust y Microsoft CA para VPN, SCEP

- Prestaciones VPN Dead Peer Detection, DHCP a través de VPN, IPSec NAT Traversal, pasarela VPN redundante, VPN basada en enrutamiento

- Plataformas Global VPN Client soportadas Microsoft® Windows 2000, Windows XP, Vista 32 bits/64 bits, Windows 7 32/64 bits

- Plataformas SSL VPN Microsoft Windows 2000/ XP/ Vista 32 bits/64 bits/Windows 7, Mac OSX 10.4+, Linux FC3+/ Ubuntu 7+/ OpenSUSE

- Plataforma Mobile Connect soportada iOS 4.2 y superior

-- Prestaciones Servicios de seguridad:

- Servicios de inspección profunda de paquetes Gateway Anti-Virus, Anti-Spyware and Intrusion Prevention

- Content Filtering Service (CFS) Rastreo por HTTP URL, HTTPS IP, palabra clave y contenido, bloqueo de ActiveX, Java Applet, y cookies, gestión del ancho de banda según categorías de filtrado, listas de admitidos/bloqueados.

-- Prestaciones de Red

- Asignación de direcciones IP Estática, (cliente DHCP, PPPoE, L2TP y PPTP), servidor DHCP interno.

- Modos NAT 1:1, 1:muchos, muchos:1, muchos:muchos, NAT flexible (IPs solapadas), PAT, modo transparente.

- VLANS

- DHCP Servidor interno

- Enrutamiento

- Autenticación XAUTH/RADIUS, Active Directory, SSO, LDAP, Novell, base de datos interna.

Prestaciones de Hardware

-- Interfaces Ethernet – Wan / Lan

-- Memoria Flash RAM 16 MB como mínimo

-- 3G inalámbrico (opcional)

-- Puertos USB

-- Potencia de entrada 100 a 240 VAC, 50-60 Hz, 1 A

-- Certificaciones Common Criteria EAL4+, VPNC, FIPS 140-2, ICSA Firewall 4.1

-- Conformidad con normas FCC Class B, ICES Class B, CE, C-Tick, VCCI Class B, MIC, NOM, UL, cUL, TÜV/GS, CB, DEEE, RoHS

-- Entorno/humedad 32-105o F, 0-40o C/ 5-95% sin condensación

SERVIDORES (configurados para alta disponibilidad)

-- Sistema que funcionará en Cluster alta disponibilidad

-- Tipo Rack

-- Procesador: Intel o AMD

-- Velocidad Procesador: 2.6 GHz como mínimo - 8 core como mínimo

-- MEMORIA RAM: 128GB mínimo

-- PUERTOS DE RED: 4 puertos Ethernet de 1Gb

-- CONTROLADORA DE DISCOS: Smart Array P420i/512MB FBWC (RAID 0/1/1+0/5/5+0/6/6+0)

-- Conectividad con la SAN: iSCSI o Fibra Óptica, con tarjetas internas en el servidor redundantes

-- Almacenamiento interno: 2 discos x 500Gb SAS, en Raid 1.

-- Doble Fuente Redundante

-- Sistema Operativo: Windows Server 2012 Español Enterprise u otro sistema operativo en la versión Enterprise o Datacenter.

ALMACENAMIENTO:

SISTEMA DE ALMACENAMIENTO CENTRALIZADO

-- Tipo SAN para Rack

-- Almacenamiento inicial mínimo 10TB disponibles

-- Capacidad Soportada mínimo 16 TB (para crecimiento futuro)

-- Configuración Raid 5

-- Fuentes redundantes

-- Controladoras Redundantes

-- Interconexión con servidores

-- Interfaces para discos: RAID 0, 1, 3, 5, 6 y 10, SATA (hot swap) o SAS (hot swap)

-- Chasis MONTAJE EN RACK DE 19”

-- Consumo máximo 650 WATIOS

-- Conexión con los servidores Gigabit Ethernet o Fibra óptica o SAS o mini-SAS o iSCSI

SISTEMA DE SUMINISTRO DE CORRIENTE

SAI o UPS:

-- UPS's con capacidad de 6 a 14 Kva

-- Se suministrará, instalará, configurará y dejará en perfecto funcionamiento la totalidad de las UPS's requeridas.

-- Se realizará las adecuaciones eléctricas necesarias para la instalación y puesta en funcionamiento de cada una de las UPS en los sitios requeridos.

-- Voltaje de Entrada: 160-256V (208V±23%) o 220V

-- Voltaje de Salida: 120/240V o 115/230V o 110/220V, con posibilidad de conectar el UPS de la siguiente manera Conexión Bifásica 208/120 VAC Dos Fases + Neutro + Tierra, conexión Monofásico Europea 220 VAC Fase + Neutro + Tierra o Monofásico a 120 VAC Fase + Neutro + Tierra.

-- Bypass: Automático y Manual

-- Frecuencia de Entrada: 60Hz ± 3Hz o 50Hz ± 3Hz

-- Frecuencia de Salida: 60Hz (Autodetección) o 50Hz

-- Factor de Potencia de entrada: =0.98 a 100% de carga.

-- Factor de Potencia de salida: 0.7

-- No. Fases Entrada/Salida: Bifásica

-- Arquitectura: Online doble conversión

-- Tipo Onda: Senosoidal.

-- Baterías: selladas, libres de mantenimiento

-- THDI Entrada: <15%

-- Capacidad Sobrecarga: 105% Durante 10 Segundos

-- IGBT: Inversor/Rectificador

-- Conexión Externa Baterías: Capacidad Expansión Módulos Baterías

-- Puerto de Comunicación RJ 45 en agente SNMP

-- Agente SNMP con software para administración WEB

-- Autonomía: 5 minutos plena carga

-- Eficiencia > 85%

-- Transformador de Aislamiento de Salida original de fábrica: Interno (dentro de la UPS).

-- Nivel de ruido: <= 60 decibeles a 1.5 metros de distancia.

-- Panel Frontal: Display Digital indicador de Línea, bypass, inversor, respaldo, falla, capacidad de batería, tensión de entrada y salida, frecuencia de entrada y salida, temperatura interna y código/estado de falla.

-- Operación sobre el nivel de mar hasta 3000 metros @ 25oC.

-- Debe tener Certificado RETIE

-- El Representante de la marca en Colombia debe contar con los certificados ISO 9001, ISO 14001

CORRIENTE REGULADA Y NORMAL:

Se debe contar con sistema de alimentación regulada que proteja los equipos del SOC de picos de voltaje controlado a la UPS en caso de falla en el sistema de alimentación externo.

Se debe contar con tableros de distribución para la corriente normal y regulada del SOC.

Todas las conexiones eléctricas normales y reguladas deberán estar debidamente identificadas (marquilladas) tanto en tableros como en puntos de conexión.

Se debe contar con un sistema de cableado eléctrico regulado y normal para el SOC que ofrezca las condiciones de seguridad necesaria y de disponibilidad para atender el servicio.

SISTEMA DE PUESTA A TIERRA:

Se debe contar con un sistema de puesta a tierra que garantice la protección de los equipos del SOC ante descargas y sobre tensiones.

SISTEMA DE AIRE ACONDICIONADO:

Se suministrará, instalará y dejará en perfecto funcionamiento, aires acondicionados requeridos los cuales serán instalados en los centros de cableado y racks de los equipos.

SISTEMA DE MEDICIÓN DE CONDICIONES AMBIENTALES:

Se deben instalar los sistemas necesarios para medir las condiciones de temperatura y humedad dentro del centro de cableado y racks de los equipos.

CENTROS DE CABLEADO Y CUARTOS DE EQUIPOS:

Se deben ofrecer los centros de cableado y cuartos de equipos o centros de cómputo que cumplan con las garantías suficientes en espacio, suministro de energía regulada y UPS, condiciones ambientales, físicas y de seguridad para proteger la información en el SOC.

SISTEMA DE VIDEOANALÍTICA

Software de detección de placas:

Este software debe cumplir con:

Proveer de librerías (SDK) para integración con terceros.

Fuente de video

-- Codec, formato de video, MJPEG/H264/YUV424/RBG/BN 8 bpp.

-- Formato de video, progresivo o entralazado.

Condiciones para la lectura

-- Min Altura de caracteres: 13 pixeles.

-- Max. Rotación X (pitch) ± 42o.

-- Max. Rotación Y (yaw) ± 44o.

-- Max. Rotación Z (roll) ± 15o.

Capacidades y funcionamiento

-- 24/7 trabajando en modo síncrono o asíncrono.

-- Modo de procesamiento cooperativo, múltiples instancias para una misma fuente de vídeo o independiente, una instancia por fuente de vídeo.

-- Modo multi-lectura (>1 lectura por vehículo).

-- Control de lecturas duplicadas y discriminación por gramática.

-- Activación por detección inteligente de movimiento.

-- Activación por trigger externo (espira magnética).

-- Transmisión remota TCP (IP, puerto) de cada lectura Información base (matrícula, precisión, tamaño, time stamp).

-- Proporcionar Imagen original de la cámara, Imagen con overlay (time stamp, descripción), Imagen de la matrícula y vehículo aislado.

Tasas de acierto

-- > 98,5% en parado.

-- > 98,0% en movimiento (condiciones normales).

-- > 97,0% en movimiento (condiciones adversas lluvia).

Software de Grabación

El software encargado de la grabación deberá cumplir con los siguientes requisitos:

-- Grabación automática por eventos de contenido procedente de cámaras IP, estando perfectamente integrado con el software de detección de placas, que será una de las fuentes de eventos para la automatización.

-- Grabación programada de contenido generando un periodo de grabación desatendido y con procesos de borrado automáticos preservando un periodo programado de caducidad del contenido.

-- Volcado del contenido del stream IP generado por las cámaras en cualquiera de los casos de grabación, reduciendo así las características de cómputo de los servidores necesarios para cada instalación.

-- Extracción automática de fotogramas significativos del archivo final generado y definitivo. La calidad (resolución) del fotograma debe poder ser definida por el administrador del sistema.

-- Extracción de los fotogramas e incorporación al archivo de video correspondiente en el momento de la detección de placa.

-- La codificación del contenido debe ser capaz de soportar bit rates o rata de bit CBR y VBR.

-- Los codecs que deben ser compatibles con el sistema serán H264, MPEG4, MPEG2, DV, WM, MPEG TS.

Software de gestión

El software de gestión es el que coordinará todos los parámetros necesarios para la automatización de todo el flujo:

-- Deberá proporcionar los Servicios Web (WSDL) y las herramientas necesarias para que se puedan automatizar todos los flujos programados. Integración completa con todos los sistemas de medición del CDA para la documentación automática.

-- Deberá proporcionar herramientas de creación, edición, modificación, borrado y visualización de metadata o definición de campos de contenido para inclusión de los parámetros contemplados en el análisis de un vehículo en la inspección de un CDA. Esta metadata deberá ser capaz de incorporar campos de fecha, booleanos, hora, desplegables, desplegables múltiples, de texto libre.

-- Contemplará herramientas profesionales de gestión de usuarios y grupos de usuarios a la hora de darlos de alta y de asignar funcionalidades restrictivas cada uno de ellos, así como permisos de acceso a parte del contenido gestionado por la herramienta.

-- Se deberá proporcionar una funcionalidad de LOG de uso de la herramienta para monitorizar cualquier uso de ella. Deberá quedar reflejado mediante este log cualquier actividad hecha mediante la herramienta de gestión, distinguiendo qué usuario la hizo y en qué fecha y hora la realizó.

-- La información relacionada con la inspección deberá ser integrada de forma automática, sin ser editada por medios manuales, siendo únicamente proporcionada en modo lectura.

-- Deberán proporcionar herramientas de borrado automático de contenido.

-- Deberá de forma automática unir todos los videos generados en la inspección de un vehículo en un solo video, al cual se le adicionarán las fotos de las cámaras de detección de placas y la documentación de la inspección. Esta unión deberá consumir pocos recursos de cómputo, y debe hacerse de forma nativa dentro de la herramienta o el software.

-- Se deberá proporcionar la herramienta de visualización de la documentación de cada vehículo, por diferentes campos.

-- Búsquedas complejas a través de cualquiera de los campos de documentación de la ficha de la inspección con operadores lógicos Booleanos, tales como and (&), or (|) y not (!).

-- Proporcionar Alarmas cuando no se hayan cumplido algunos requisitos en una inspección, comparando los resultados obtenidos con una pauta establecida por el organismo competente.

-- El sistema deberá proporcionar las herramientas necesarias para la generación de estadísticas de los resultados obtenidos, proporcionando informes detallados de cualquier consulta.

-- El sistema deberá consolidar toda la información documental en un repositorio central. A este repositorio le llegarán todos los datos de cada uno de los CDAs y sobre este repositorio común igualmente se podrán realizar búsquedas, estadísticas, etc.

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 del Magic Quadrant Security Information and Event Management de Gartner mas reciente.

REQUISITOS DE LOS ASPIRANTES A PROVEEDORES DE LOS SISTEMAS DE CONTROL Y VIGILANCIA CENTROS DE DIAGNÓSTICO AUTOMOTOR (CDAS).

INTRODUCCIÓN

El presente documento define los requerimientos que deben cumplir aquellos aspirantes a proveedores del sistema de control y vigilancia. El documento se estructura de la siguiente manera:

El Título I describe el objetivo del documento, los sistemas de control y vigilancia, el marco legal sobre el cual se desarrolla todo el proceso, así como el alcance del presente documento.

El Título II, define los requerimientos técnicos, administrativos, financieros y jurídicos para la homologación de los aspirantes a proveedores de los sistemas de control y vigilancia, así como los procesos de verificación que cada uno de ellos debe cumplir.

El Título III, describe el procedimiento de homologación respecto a los plazos para la radicación de documentos o solicitudes de aclaraciones y demás.

1 TÍTULO I.

INFORMACIÓN GENERAL.

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

1.1 OBJETIVO DEL DOCUMENTO.

El presente documento tiene por objetivo: DEFINIR LOS REQUERIMIENTOS QUE DEBEN CUMPLIR Y SE EVALUARÁN A LOS ASPIRANTES PARA PROVEEDORES DE LOS SISTEMAS DE CONTROL Y VIGILANCIA DE LOS CENTROS DE DIAGNOSTICO AUTOMOTOR.

1.2 SISTEMAS DE CONTROL Y VIGILANCIA DE LOS CENTROS DE DIAGNÓSTICO AUTOMOTOR.

“El Sistema de Control y Vigilancia es una infraestructura tecnológica operada por cualquier ente público o privado que el CDA contrate y que será previamente homologado por la Superintendencia de Puertos y Transporte o por quien esta delegue, para asegurar el cumplimiento de los parámetros 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; la presencia del vehículo en el Centro de Diagnóstico Automotor; la realización de las pruebas; que el certificado se expida desde la ubicación geográfica del Centro de Diagnóstico y que las pruebas se hagan desde los computadores de los Centros de Diagnóstico con el fin de evitar un posible fraude en la expedición del mencionado certificado; el registro del pago; la correlación o trazabilidad para el cruce de información y que estén conectados con el centro de monitoreo de la Superintendencia de Puertos y Transporte y el RUNT”. (Resolución número 9304 del 2012, artículo 2o expedida por la Superintendencia de Puertos y Transporte para los CDA).

A partir de la anterior definición, se evidencia que los sistemas de control y vigilancia para los Centros de Diagnóstico Automotor, buscan esencialmente garantizar la legitimidad a través de la realización del proceso de revisión técnico mecánica, con el fin de proteger al usuario de la ilegalidad en el proceso de evaluación, a través de la implementación de características técnicas y de seguridad adecuadas.

1.3 MARCO LEGAL.

En concordancia con las facultades otorgadas al Presidente de la republica de acuerdo al numeral 16 del artículo 189 de la Constitución Política y desarrolladas por el artículo 37 de la Ley 105 de 1993 y por el artículo 54 de la Ley 489 de 1998, se delegan las funciones de control, inspección y vigilancia otorgadas al Presidente según el numeral 22 del artículo 189de la Constitución, a la Superintendencia de Puertos y Transporte con el objeto de inspeccionar, vigilar y controlar la aplicación y el cumplimiento de las normas que rigen el sistema de tránsito y transporte, de la misma manera inspeccionar, vigilar y controlar la permanente, eficiente y segura prestación del servicio de transporte. De esta manera mediante los Decretos número 101 de 2000, Decreto número 1016 de 2000 y Decreto número 2741 de 2001, la Superintendencia de Puertos y Transporte expide la Resolución número 9304 el 24 de diciembre de 2012 donde se reglamentan la creación de los Sistemas de Control y Vigilancia determinando las exigencias tecnológicas que deben implementar los Centros de Diagnóstico Automotor.

En el mismo sentido se acoge a lo dispuesto en el artículo 4o del Decreto número 2741 de 2001 donde se determinó que los sujetos de control y vigilancia podían ser personas naturales o jurídicas que las normas determinen, en este caso la reglamentación establece como tales sujetos a los aspirantes a proveedores de los sistemas de control vigilancia, dado que en consonancia con el concepto emitido por el Consejo de Estado en cuanto a los sujetos objeto de vigilancia de la Superintendencia de Puertos y transporte, dentro del ejercicio de las funciones delegadas y de las otorgadas en virtud de la ley, la Superintendencia puede, examinar y comprobar la transparencia en el manejo de las distintas operaciones y actividades que desarrolla, en cumplimiento de su objeto social, y de las entidades sometidas a su inspección, vigilancia y control. Es así que la Superintendencia de Puertos y Transporte se encuentra dotada para reglamentar aspectos administrativos o que tengan que ver con su funcionamiento, bajo el entendido del artículo 66 de la Ley 489 de 1998 donde consagra que: “Las superintendencias son organismos creados por la ley, con la autonomía administrativa y financiera que aquella les señale, sin personería jurídica, que cumplen funciones de inspección y vigilancia atribuidas por la ley o mediante delegación que haga el Presidente de la República previa autorización legal”.

No obstante, a partir de la promulgación de la Ley 1450 del 2011 por medio de la cual se expidió el Plan Nacional de Desarrollo 2010-2014, se estableció en el parágrafo del artículo 89facultar a la Superintendencia de Puertos y Transporte para expedir la reglamentación de las características técnicas de los sistemas de seguridad documental que deberán implementar cada uno de los vigilados.

Para el desarrollo de esta reglamentación y atendiendo a los principios de coordinación y colaboración de las autoridades administrativas se suscribió el Contrato Interadministrativo

número 321 con la Universidad Pedagógica y Tecnológica de Colombia, el 23 de octubre del 2013, con el objeto de elaborar el anexo técnico de Homologación de los Sistemas de Control y Vigilancia, donde se describen las obligaciones específicas que se deben contemplar en el anexo técnico, así:

*"**1. Proceso de verificación de la presencia del vehículo en las instalaciones del CDA a través de captura de video "registro fílmico"** a) Verificación del vehículo donde se cubra el 100% de la inspección técnico mecánica y de emisiones contaminantes efectuada y se permita la visualización de la placa para su plena identificación; b) Verificación del ingreso y salida del vehículo donde se permita la visualización de la placa para su plena identificación; c) Verificación de los registros de video el cual debe ser compatible con el sistema de intercambio de información de la Superintendencia; d) Verificar la auditoría transaccional y de base de datos presente en este proceso. **2. Proceso de verificación de la realización de las pruebas y expedición del certificado.** a) Verificación de los resultados de la revisión que emitió cada uno de los equipos en el proceso de inspección, sin que en este proceso intervenga el Centro de Diagnóstico; b) Verificación de los instructores y Director técnico y/o Jefe de Línea encargado de la realización de cada una de las pruebas realizadas al vehículo durante el proceso de inspección; c) Verificación de los registros de video, el cual debe ser compatible con los registros de captura, donde se tenga la función analítica para detección de placa; d) Verificación de coordenadas del sitio en donde se realizan las inspecciones; e) Verificación de los equipos requeridos para el funcionamiento y operación autorizados por la entidad competente se encuentren dentro de las instalaciones del CDA; f) Verificación de comunicaciones a través de redes privadas establecidas por el Sistema de Control y Vigilancia con los Centros de Diagnóstico Automotor; g) Verificar el registro y envío de los resultados de cada una de las pruebas efectuadas al vehículo por parte del Centro de Diagnóstico Automotor al Sistema de Control y Vigilancia. Garantizando que se encuentren la totalidad de los campos establecidos en el formato uniforme de resultados de revisión técnico mecánica y de emisiones contaminantes; h) Verificar la auditoría transaccional y de base de datos presente en este proceso. **3. Proceso de Registro de Pago.** a) Verificación del actor del sector financiero esté vigilado por la Superintendencia financiera de Colombia; c) Verificación que el actor financiero provea cobertura nacional; c) Verificación que el actor financiero cuente con bases de datos de todos los pagos realizados y su discriminación según el estado en que se encuentre de los servicios prestados por los CDA; d) Verificar la auditoría transaccional y de base de datos presente en este proceso. **4. Proceso de Cruce de información e interconexión.** a) Superintendencia de Puertos y Transporte con el actor del sistema financiero; b) Superintendencia de Puertos y Transporte con el RUNT; c) Verificación de canales de comunicaciones dedicados y sistemas óptimos conforme a la cantidad de conexiones y el número de sitios a homologar; d) Verificar que el Sistema de Control y Vigilancia realice el cruce de información generado por cada uno de los entes involucrados (actor del sector financiero, RUNT y Superintendencia de Puertos y Transporte); e) Verificar la auditoría transaccional y de base de datos presente en este proceso. **5. De igual manera el contratista cumplirá con las siguientes obligaciones:** a) El contratista definirá los requisitos y procedimiento de homologación de los aspirantes a prestar el servicio de operar el sistema de control y vigilancia de que trata la Resolución número 9304 de 2012; b) El contratista deberá definir los requerimientos técnicos, administrativos, financieros y jurídicos para homologar a los aspirantes a proveedores del Sistema de Control y Vigilancia y el Sistema de Captura de Video".*

1.4 ALCANCES DEL DOCUMENTO.

El alcance de este documento incluye la definición de los requisitos a nivel jurídico, administrativo, financiero y técnico que deben cumplir las entidades aspirantes a operar los sistemas de control y vigilancia para los Centros de Diagnóstico Automotor.

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

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

Los requisitos jurídicos, buscan principalmente garantizar la legalidad de las entidades a homologarse, de sus representantes.

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

Este documento contiene los requerimientos generales que deben seguir las entidades aspirantes a homologarse para conseguir esta meta, y presenta diferentes alternativas para el cumplimiento de los requisitos con el fin de garantizar pluralidad de oferentes, es así como se incluye por ejemplo alternativas de conformación de uniones temporales o consorcios, entre otras.

Conforme al Decreto número 1510 del 2013 y al manual de Colombia Compra Eficiente: *"Si en el Proceso de Contratación no es obligatorio que los oferentes cuenten con RUP, la Entidad Estatal de forma autónoma debe definir la forma de acreditar los requisitos habilitantes de experiencia, capacidad jurídica, capacidad financiera y capacidad organizacional"*.

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

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

2 TÍTULO II.

REQUISITOS DOCUMENTALES.

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

2.1 CARTA DE INTERÉS Y RADICACIÓN DE REQUISITOS DOCUMENTALES.

La carta de interés y radicación de requisitos documentales, permitirá iniciar el proceso de validación de los requisitos para homologarse como proveedor de los Sistemas de Control y Vigilancia en los Centros de Diagnóstico Automotor (CDAs). *Ver numeral 2.1.2: Modelo Carta de Interés y Radicación de Requisitos Documentales*.

2.1.1 Especificaciones de la entrega del documento

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

-- Debe imprimirse en tamaño carta.

-- Debe ir en papel membrete de la compañía.

-- "[NOMBRES APELLIDOS DEL SUPERINTENDENTE DELEGADO]" Debe ser reemplazado por los nombres y apellidos del Superintendente Delegado nombrado al momento de presentar este documento.

-- [RAZÓN SOCIAL EMPRESA, CONSORCIO O UNIÓN TEMPORAL], debe ser reemplazado por el nombre o razón social del ente aspirante.

-- [Número del NIT], debe ser reemplazado con el Número de Identificación Tributaria de la Empresa o Consorcio. En caso de Unión Temporal deberá colocar el nombre de la Unión temporal y el nombre o razón social de cada una de las empresas que la conforman con su número de Nít.

-- "Resolución NN de 2014", donde NN debe ser reemplazada por el número de resolución que expida la Superintendencia de Puertos y Transporte con el Anexo Técnico de Requisitos y Requerimientos para los Sistemas de Control y Vigilancia de los Centros de Diagnóstico Automotor.

-- "NN Folios" donde NN debe ser reemplazado por el número de folios entregados en el medio físico.

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

2.1.2. Modelo Carta de Interés y Radicación de Requisitos Documentales

Ciudad, Fecha (dd/mm/aaaa)

Doctor(a)

[NOMBRES APELLIDOS DEL SUPERINTENDENTE DELEGADO]

Superintendente Delegado de Tránsito y Transporte Terrestre Automotor

SUPERINTENDENCIA DE PUERTOS Y TRANSPORTE

Calle 63 No 9A-45.

Bogotá, D. C.

Referencia: Carta de interés para participar en el proceso de validación de requisitos para homologarse como proveedor de los sistemas de control y vigilancia para los CDAs.

Respetado doctor:

Mediante el presente oficio deseo manifestar que la *empresa (unión temporal o consorcio)*[RAZÓN SOCIAL EMPRESA, CONSORCIO O UNIÓN TEMPORAL] con NIT No [Número del NIT], la intención de participar en el proceso que adelanta la Superintendencia de Puertos y Transporte para prestar el servicio a los Centros de Diagnóstico Automotor (CDAs) como proveedor de los Sistemas de Control y Vigilancia.

Se anexa los requerimientos documentales exigidos en la Resolución NN de 2014 expedida por la Superintendencia de Puertos y Transportes, así:

-- Medio Físico, 2 tomos de NN Folios.

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

Agradezco la atención prestada.

Cordialmente,

[NOMBRES APELLIDOS]

REPRESENTANTE LEGAL

[RAZÓN SOCIAL EMPRESA, CONSORCIO O UNIÓN TEMPORAL]

2.2 REQUISITOS DEL ASPIRANTE.

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

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

Con el fin de estandarizar la entrega de documentos se define a continuación las características como deben ser presentados:

-- Técnica de empaste: Unibind

-- Color de las Tapas: Transparentes

-- Foliación: El foliado debe quedar en un lugar visible, y que no quede cubierto por ningún texto o membrete.

-- Idioma: El idioma para presentación de los requisitos documentales debe ser en español.

-- Papel: Tamaño carta 8.1/2”x11”

2.2.2 Portada

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

2.2.2.1 Especificaciones de la entrega del documento

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

-- Debe colocarse al inicio del documento.

-- Su número de Folio debe ser 1.

-- “RESOLUCIÓN NN DEL **DD** DEL MES DE **MM** DE 2014”, debe colocarse el número de la resolución y la fecha de cuando se expida por parte de la Superintendencia de Puertos y Transporte la reglamentación para el proceso de evaluación y homologación de los aspirantes de los sistemas de control y vigilancia de los CDA, donde “NN” es el número de la resolución, “DD” es el día y “MM” es el Mes de expedición de la resolución.

-- [RAZÓN SOCIAL EMPRESA, CONSORCIO O UNIÓN TEMPORAL], debe ser reemplazado por el nombre o razón social del ente aspirante.

-- [CIUDAD] Ciudad donde se origina la documentación.

-- “201**N**”, donde “N” es el último dígito del año en el que se radican los documentos.

2.2.2.2 Modelo de la Portada General

PRESENTACIÓN DE REQUISITOS DOCUMENTALES SEGÚN
RESOLUCIÓN **NN** DEL **DD** DEL MES **MM** DE 2014

EXPEDIDA POR LA SUPERINTENDENCIA DE PUERTOS Y TRANSPORTE

ASPIRANTE:

[RAZÓN SOCIAL EMPRESA, CONSORCIO O UNIÓN TEMPORAL]

[CIUDAD]

201**N**

2.2.3 Índice General

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

2.2.3.1 Especificaciones de la entrega del documento

-- "#" significa que se debe colocar el número de folio en donde se encuentra ubicado.

-- Requerimiento técnico AAA: significa que se debe reemplazar con el nombre del requerimiento.

-- "n" significa el consecutivo del requerimiento.

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

ÍNDICE GENERAL

No de Folio

3.2.	Requerimiento financiero BBB	#
3.n.	Requerimiento financiero nnn	#
4.	REQUERIMIENTOS TÉCNICOS	
4.1.	Requerimiento técnico AAA	#
4.2.	Requerimiento técnico BBB	#
4.n.	Requerimiento técnico nnn	#

2.3 LISTA DE REQUISITOS JURÍDICOS.

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

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

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

c) Inhabilidades e incompatibilidades

-- Las inhabilidades e incompatibilidades están establecidas para asegurar los intereses públicos y proteger la transparencia, objetividad e imparcialidad en las relaciones entre el Estado y los particulares.

-- El régimen de inhabilidades e incompatibilidades es de aplicación restrictiva, por lo cual cuando existen varias interpretaciones posibles sobre una inhabilidad o incompatibilidad, debe preferirse la que menos limita los derechos de las personas.

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

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

– Las personas que se hallen inhabilitadas para contratar por la Constitución y las leyes.

– Quienes participaron en las licitaciones o celebraron los contratos de que trata el literal anterior estando inhabilitados. Esta inhabilidad se extenderá por el término de 5 años a partir de la participación en la licitación.

– Quienes dieron lugar a la declaratoria de caducidad. Esta inhabilidad se extenderá por el término de 5 años contados a partir de la fecha de declaratoria del acto de caducidad.

– Quienes han sido condenados por sentencia judicial a la pena accesoria de interdicción de derechos y funciones públicas y quienes hayan sido sancionados disciplinariamente con destitución. Esta inhabilidad se extenderá por el término de 5 años contados a partir de la ejecutoria de la sentencia que impuso la pena.

– Quienes sin justa causa se abstengan de suscribir el contrato estatal adjudicado. Esta inhabilidad se extenderá por el término de 5 años a partir de la fecha en que expiró el plazo para la firma.

– Los servidores públicos.

2.3.1 Certificado de Cámara de Comercio

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

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

2.3.1.1 Especificaciones de la entrega del documento

-- Se debe presentar en original.

-- Su expedición debe ser igual o inferior a 30 días calendario al de la fecha de radicación.

-- Si la propuesta es presentada en Unión Temporal o en Consorcio, se debe adicionar el certificado de Cámara de Comercio de cada una de la personas naturales y/o jurídicas que lo(a) conformen.

2.3.2 Registro Único Tributario

Es el mecanismo único para identificar, ubicar y clasificar a las personas y entidades que tengan la calidad de contribuyentes declarantes del impuesto sobre la renta y no

contribuyentes declarantes de ingresos y patrimonio; los responsables del régimen común y los pertenecientes al régimen simplificado; los agentes retenedores; los importadores, exportadores y demás usuarios aduaneros, y los demás sujetos de obligaciones administradas por la U.A.E. Dirección de Impuestos y Aduanas Nacionales DIAN, respecto de los cuales esta requiera su inscripción. Sirve para cerciorarse e identificar la actividad económica ante terceros con quienes sostenga una relación comercial, laboral o económica en general y ante los diferentes entes de supervisión y control, a su vez, este documento le señala sus obligaciones frente al Estado colombiano.

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

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

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

2.3.2.1 Especificaciones de la entrega del documento.

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

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

-- Deben estar presentes los códigos CIIU de la actividad económica, con la versión vigente. Las siguientes son las actividades económicas según el CIIU en su última versión

consolidadas por grupo, división y clase que serán la base de este requisito, los aspirantes a proveedores deberán tener al menos una de las siguientes actividades:

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

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

Esta clase incluye:

– El análisis, diseño de la estructura, el contenido y/o escritura del código informático necesario para crear y poner en práctica programas de sistemas operativos, aplicaciones de programas informáticos (incluyendo actualizaciones y parches de corrección), también bases de datos.

– El desarrollo de soluciones web (sitios y páginas web) y personalización de programas informáticos a clientes, es decir, modificar y configurar una aplicación existente a fin de que sea funcional con los sistemas de información de que dispone el cliente.

Esta clase excluye:

– La edición de paquetes de software o programas informáticos comerciales. Se incluye en la clase 5820, “Edición de programas de informática (software)”.

– La planificación y diseño de sistemas que integren el equipo de hardware, software y tecnologías de la comunicación, aunque el suministro del software se constituya como una parte integral del servicio. Se incluye en la clase 6202, “Actividades de consultoría de informática y actividades de administración de instalaciones informáticas”.

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

Esta clase incluye:

– La planificación y el diseño de los sistemas informáticos que integran el equipo (hardware), programas informáticos (software) y tecnologías de las comunicaciones (incluye redes de área local [LAN], red de área extensa [WAN], entre otras).

– Las unidades clasificadas en esta clase pueden proporcionar los componentes de soporte físico y lógico (como pueden ser el hardware y software) como parte de sus servicios integrados o estos componentes pueden ser proporcionados por terceras partes o vendedores. En muchos casos las unidades clasificadas en esta clase suelen instalar el sistema, capacitar y apoyar a los usuarios del sistema.

– Los servicios de gerencia y operación en sitio, de sistemas informáticos y/o instalaciones informáticas de procesamiento de datos de los clientes, así como también servicios de soporte relacionados.

– Los servicios de consultoría en el diseño de sistemas de administración de información y en equipos de informática.

– Los servicios de consultoría para sistemas de ingeniería y fabricación asistida por computador.

– El servicio de análisis de requerimientos para la instalación de equipos informáticos.

Esta clase excluye:

– La venta por separado de equipos o programas informáticos. Se incluye en la clase 4651, “Comercio al por mayor de computadores, equipo periférico y programas de informática” y en la clase 4741, “Comercio al por menor de computadores, equipos periféricos, programas de informática y equipos de telecomunicaciones en establecimientos especializados”, según corresponda.

– La instalación de computadores centrales y equipos similares. Se incluye en la clase 3320, “Instalación especializada de maquinaria y equipo industrial”.

– La instalación por separado (configuración) de los computadores personales e instalación por separado de software. Se incluye en la clase 6209, “Otras actividades de tecnologías de información y actividades de servicios informáticos”.

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

Esta clase incluye:

– El suministro de infraestructura para servicios de hosting, servicios de procesamiento de datos y actividades conexas relacionadas.

– Las actividades especializadas en alojamiento de: sitios web, servicios de transmisión de secuencias de video por internet (streaming), aplicaciones, entre otros.

– El suministro de servicios de aplicación.

– El suministro a los clientes de acceso en tiempo compartido a servicios centrales.

– Las actividades de procesamiento de datos: elaboración completa de datos facilitados por los clientes y generación de informes especializados a partir de los datos facilitados por los clientes.

– El suministro de servicio de registro de datos.

– La tabulación y la digitación de todo tipo de datos.

– El escaneo óptico de datos y de documentos.

– El funcionamiento de oficinas de servicio de informática dedicadas al procesamiento de datos y alojamiento web.

Esta clase excluye:

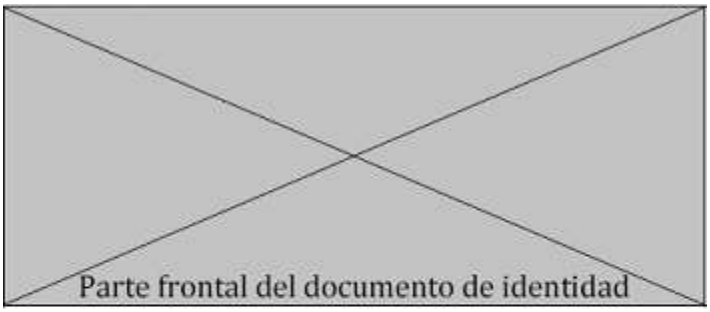
La explotación de los sitios web. Se incluye en la clase 6312, “Portales web”.

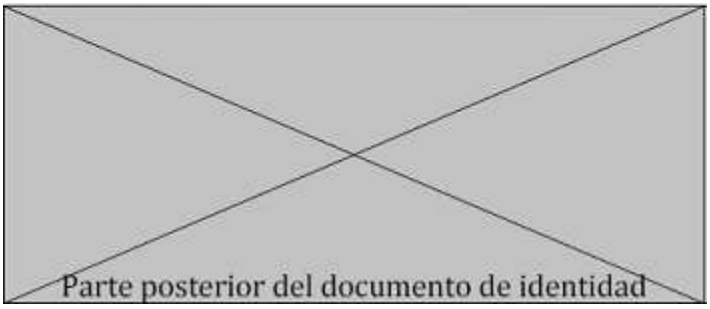
2.3.3 Copia de Documento de Identidad del Representante Legal

El documento de identidad es llamado Cédula de Ciudadanía o C.C., para el caso de los ciudadanos colombianos mayores de edad. Este es el único documento de identificación válido para todos los actos civiles, políticos, administrativos y judiciales según la Ley 39 de 1961. Se expide para los ciudadanos colombianos al cumplir los 18 años de edad (mayoría de edad en Colombia). El organismo encargado para realizar las tareas de expedición de cédulas es la Registraduría Nacional del Estado Civil de Colombia. En el caso de los extranjeros, existe la Cédula de Extranjería que expide Migración de Colombia a manera de documento de identificación, con los mismos efectos que la Cédula de Ciudadanía. *Ver Numeral 2.3.3.1: Modelo Copia de Documento de Identidad del Representante Legal.*

2.3.3.1 Modelo Copia de Documento de Identidad del Representante Legal

Esta copia está dirigida al archivo de los requisitos documentales presentados por [RAZÓN SOCIAL EMPRESA, CONSORCIO O UNIÓN TEMPORAL], en su intención de participar en el proceso que adelanta la Superintendencia de Puertos y Transporte para prestar el servicio a los Centros de Diagnóstico Automotor (CDA) como proveedor de los Sistemas de Control y Vigilancia.





_____

Firma.

VÁLIDA ÚNICAMENTE COMO REQUISITO DOCUMENTAL PARA PROCESO DE EVALUACIÓN SUPERTRANSPORTE.

2.3.3.2 Especificaciones de la entrega del documento

- La copia del documento de identidad debe estar a una ampliación de 150%.

- La firma es de la persona que aparece en el documento de identidad.

- En caso de ser el representante legal de una persona parte de una unión temporal o consorcio debe escribir: [RAZÓN SOCIAL UNIÓN TEMPORAL O CONSORCIO (RAZÓN SOCIAL EMPRESA)]

2.3.4 Certificado del Pago de aportes parafiscales

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

Acorde con lo señalado en el artículo 50 de la Ley 789 de 2002 y en el artículo 23 de la Ley 1150 de 2007 el aspirante, deberá entregar una certificación de cumplimiento de sus obligaciones con los sistemas de salud, riesgos profesionales, pensiones y aportes a las Cajas

de Compensación Familiar, Instituto Colombiano de Bienestar Familiar y Servicio Nacional de Aprendizaje, expedida por el revisor fiscal, cuando exista según los requerimientos de ley, o por el representante legal de la sociedad interesada, en la que se acredite que dicha compañía se encuentra al día en el pago de aportes al Sistema de Seguridad Social Integral (EPS, AFP, ARP, Caja de Compensación Familiar, ICBF y Sena) durante los últimos (6) seis meses, anteriores a la fecha de radicación de la carta de interés y de los requisitos documentales.

2.3.4.1 Especificaciones de la entrega del documento

- Certificado emitido por revisor fiscal o representante legal según corresponda, basado en el tipo de persona.

- Su expedición debe ser igual o inferior a 30 días calendario al de la fecha de radicación.

- Si la propuesta es presentada en Unión Temporal o en Consorcio, se debe adicionar el certificado de pago de aportes parafiscales de cada una de la personas naturales y/o jurídicas que lo(a) conformen.

- En caso de ser un revisor fiscal el obligado a emitir el certificado deberá anexar fotocopia de la cédula de ciudadanía, fotocopia de la tarjeta profesional y antecedentes disciplinarios de la Junta Nacional de Contadores.

2.3.5 Certificación de composición de socios o accionistas

Certificado firmado por el representante legal o el revisor fiscal dependiendo del tipo de empresa, en el que se relacione los socios y o accionistas o asociados que tengan directa o indirectamente el 5% o más del capital social, aporte o participación. Cuando esta información no conste en el certificado de existencia o representación expedido por la Cámara de Comercio. La certificación debe tener corte de la información en un término no superior a noventa días de la fecha de presentación de la propuesta. Si dentro de la composición accionaria de la empresa se encuentra una persona jurídica cuya participación sea igual o superior al 5% del capital, esta debe aportar la composición de participación accionaria, proceso que debe repetirse hasta que los accionistas sean personas naturales. De cada accionista se debe incluir: Nombre o razón social, identificación y porcentaje de participación, siempre y cuando esta sea igual o superior al 5%. Ver numeral 2.3.5.1: Modelo de Certificación de Composición Accionaria.

2.3.5.1 Especificaciones de la entrega del documento

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

-- El certificado deberá ser autenticado con firma y huella.

- [RAZÓN SOCIAL EMPRESA, CONSORCIO O UNIÓN TEMPORAL], deberá reemplazarse por el nombre del ente.

- [Número de NIT], debe ser reemplazado con el Número de Identificación Tributaria de la Empresa o Consorcio. En caso de Unión Temporal deberá colocar el nombre de la Unión temporal y el nombre o razón social de cada una de las empresas que la conforman con su número de NIT, el revisor fiscal de cada empresa deberá expedir el certificado de la composición accionaria.

- Deberá certificar el 100% de las acciones de la compañía.

- [NN], debe reemplazarse por el día en número que se expide el certificado.

- [Mes en Letras], debe reemplazarse por el mes que se expide el certificado, descrito en letras.

- [AAAA], debe reemplazarse por el año en que se expide el certificado, descrito en cuatro dígitos.

- [Número de la Tarjeta Profesional], debe reemplazarse por el número de la Tarjeta Profesional del Revisor Fiscal Vigente.

- Huella del Revisor Fiscal o Representante Legal dependiendo el tipo de empresa, debe colocarse la huella del revisor fiscal la cual debe ir autenticada.

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

2.3.5.2 Modelo de Certificación de Composición Accionaria

Ciudad, Fecha (dd/mm/aaaa)

Composición accionaria

CERTIFICACIÓN DEL REVISOR FISCAL

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

CERTIFICA QUE:

La composición accionaria es la siguiente:

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

Se expide a los [NN] días del mes de [Mes en Letras] de [AAAA], con destino a proceso de evaluación y homologación como aspirante a proveedor de los sistemas de control y vigilancia para los CDA.

Cordialmente,

[NOMBRES Y APELLIDOS DEL REVISOR FISCAL] **Huella del Revisor Fiscal**

Revisor Fiscal
T.P. [Número de la Tarjeta Profesional]
[RAZÓN SOCIAL O NOMBRE DE LA EMPRESA O CONSORCIO]

2.4 LISTA DE REQUISITOS ADMINISTRATIVOS.

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

2.4.1 Experiencia de la Compañía

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

Los aspirantes deben presentar los contratos que hayan celebrado para prestar los bienes y servicios que pretenden ofrecer y esta puede ser experiencia adquirida de forma directa o a través de la participación del aspirante en consorcios o uniones temporales. Esta experiencia se obtiene con contratantes públicos, privados, nacionales o extranjeros.

La experiencia requerida debe ser adecuada y proporcional a la naturaleza del contrato y su valor. La experiencia es adecuada cuando es afín al tipo de actividades previstas en el objeto

del contrato a celebrar. La experiencia es proporcional cuando tiene relación con el alcance, la cuantía y complejidad del contrato a celebrar.

La experiencia del oferente plural (unión temporal, consorcio y promesa de sociedad futura) corresponde a la suma de la experiencia que acredite cada uno de los integrantes del aspirante plural.

Por otra parte, cuando un aspirante adquiere experiencia en un contrato como integrante de un contratista plural, la experiencia derivada de ese contrato corresponde a la ponderación del valor del contrato por el porcentaje de participación.

La experiencia a acreditar debe estar compuesta de una combinación de actividades que garantice la cobertura de todos los aspectos que intervienen en la conformación de los sistemas de control y vigilancia, los grupos de actividades que cumplen esta meta son: seguridad de la información, sistemas de video analítica y desarrollo de software, es de resaltar que todos tienen el mismo nivel de importancia.

Conforme a lo establecido en el Decreto número 1510 del 2013: “Si en el Proceso de Contratación no es obligatorio que los oferentes cuenten con RUP, la Entidad Estatal de forma autónoma debe definir la forma de acreditar los requisitos habilitantes de experiencia, capacidad jurídica, capacidad financiera y capacidad organizacional”. En este caso, la Entidad considera que los requisitos exigidos a continuación aseguran la idoneidad de los posibles proveedores.

a) Cuantía total de la experiencia requerida. La cuantía de la experiencia requerida será la sumatoria total (de los tres grupos de actividades), debe ser igual o superior a 6.494 smmlv (salarios mínimos mensuales legales vigentes).

Cuando las certificaciones expresen su valor en dólares, se tendrá en cuenta la TRM a la fecha en que se celebró el contrato certificado.

En caso de presentar certificaciones globales deberán desglosar el monto y objeto para el cual aplica dicha certificación.

Cuando los miembros del consorcio o de la unión temporal acrediten experiencia igualmente en contratos ejecutados bajo estas modalidades, solo se tendrá en cuenta como experiencia de aquellos, la referida al porcentaje de participación que hubieren tenido en el grupo o asociación que ejecutó el contrato;

b) Número de contratos a certificar: Los aspirantes deberán acreditar experiencia mediante certificación firmada por los contratantes en mínimo una (1), máximo dos (2) certificaciones por cada grupo de actividades;

c) Antigüedad en celebración de contratos: Las certificaciones de los contratos de experiencia deberán tener una antigüedad máxima de cinco (5) años contada a partir de la fecha de terminación a satisfacción de cada contrato y hasta la fecha de radicación de la carta de interés y de los requisitos documentales;

d) Acreditación de la experiencia: Los aspirantes deberán acreditar experiencia en cada uno de los grupos de actividades requeridos descritos en el literal “f)” de este numeral, ninguno podrá tener menos del (25%) del total de la experiencia equivalente a 1624 smmlv (salarios mínimos mensuales legales vigentes). En caso de unión temporal o consorcio cada sociedad deberá aportar al menos el 100% de un grupo de las certificaciones de experiencia;

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

f) Actividades por grupo requeridas: A continuación se describen las actividades por grupo a tener en cuenta para acreditar la experiencia de la compañía, se tendrá en cuenta que esta se encuentre en los siguientes grupos:

– Seguridad de la Información: Protección de datos y/o cifrado de información y/o auditoría de bases de datos y/o correlación de eventos.

– Sistemas de video: Suministro, implementación y mantenimiento de soluciones de video, centros de monitoreo de video y/o sistemas de circuitos cerrados de televisión (CCTV) con analítica de video.

– Desarrollo de Software: Desarrollo y/o implantación de software, Desarrollo e implantación de software.

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

2.4.1.1 Especificaciones de la entrega del documento

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

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

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

2.4.1.2 Modelo de Certificaciones de Experiencia del Aspirante

Modelo de Certificaciones de Experiencia del Aspirante

EMPRESA CONTRATISTA	
FECHA DE EXPEDICIÓN DE LA CERTIFICACIÓN	DD/MM/AAAA
NOMBRE O RAZÓN SOCIAL DEL CLIENTE	
NIT DEL CLIENTE	
OBJETO DEL CONTRATO	
NOMBRES Y APELLIDOS DE QUIEN EXPIDE LA CERTIFICACIÓN	
Grupo y Actividad al que pertenece esta experiencia	Seguridad de la Información: Protección de datos Cifrado de información Auditoría de bases de datos Correlación de eventos Sistemas de video: Sistemas de video: Suministro, implementación y mantenimiento de soluciones de video Centro de monitoreo de video Sistemas de Circuitos Cerrados de Televisión (CCTV) con analítica de video Desarrollo y/o implantación de Software: Desarrollo Implantación de soluciones de software Desarrollo e implantación de software
FECHA DE INICIACIÓN DEL CONTRATO (Mes/Año)	
SI ACTUÓ EN UNIÓN TEMPORAL O CONSORCIO INDICAR EL % DE PARTICIPACIÓN	
FECHA TERMINACIÓN DEL CONTRATO	MM/AAAA
VALOR DEL CONTRATO	COP vigencia 2014 – SMMLV vigencias posteriores.
PORCENTAJE DE EJECUCIÓN	
PÁGINA WEB DEL CLIENTE	
CORREO ELECTRÓNICO DEL CONTACTO-CLIENTE	
TELÉFONO DEL CONTACTO-CLIENTE	
CIUDAD Y DIRECCIÓN DEL CLIENTE	

_____

Firma y Huella Representante Legal del Aspirante

2.4.2 Certificaciones exigibles a la Compañía

El aspirante a proveedor del SCV deberá contar con certificación de Sistema de gestión de la calidad. En caso de unión temporal o consorcio cada una de las sociedades deberá contar con la certificación de calidad. La certificación deberá estar vigente a la fecha de evaluación.

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

El aspirante a proveedor del SCV deberá contar por lo menos con una de las siguientes certificaciones: CMMI nivel 3 o superior en cualquiera de sus áreas, IT MARK, ISO 27001, ISO 20000, ISO 15504, ISO 9001 alcance en: desarrollo y/o implantación de software.

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

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

A grandes rasgos, estas son las características de cada nivel:

NIVEL 1: En este Nivel se encuentra la mayoría de las organizaciones. Los procesos son impredecibles, pobremente controlados y reactivos.

NIVEL 2: Las áreas de proceso de este Nivel están orientadas a la gestión. Los procesos son definidos, documentados, utilizados y medidos.

NIVEL 3: En este Nivel los procesos se encuentran estandarizados y documentados a nivel organizacional. Las áreas de proceso que se incorporan están orientadas a la ingeniería.

NIVEL 4: En este Nivel los procesos son Predecibles Medibles y Controlables. La Calidad y productividad son predecibles cuantitativamente.

NIVEL 5: Las organizaciones que se encuentran en este Nivel ponen foco en el mejoramiento continuo de sus procesos.

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

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

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

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

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

-- ISO 15504: Es un estándar internacional de evaluación y determinación de la capacidad y mejora continua de procesos de ingeniería del software, con la filosofía de desarrollar un conjunto de medidas de capacidad estructuradas para todos los procesos del ciclo de vida y para todos los participantes. Es el resultado de un esfuerzo internacional de trabajo y colaboración y tiene la innovación, en comparación con otros modelos, del proceso paralelo de evaluación empírica del resultado. Norma que trata los procesos de ingeniería, gestión, relación cliente-proveedor, de la organización y del soporte. Se creó por la alta competencia del mercado de desarrollo de software, a la difícil tarea de identificar los riesgos, cumplir con el

calendario, controlar los costos y mejorar la eficiencia y calidad. Este engloba un modelo de referencia para los procesos y sus potencialidades sobre la base de la experiencia de compañías grandes, medianas y pequeñas.

En caso de unión temporal o consorcio cada una de las sociedades debe contar con la certificación en sistema de gestión de la calidad ISO 9001 y por lo menos uno de los miembros deberá contar con alguna de las certificaciones solicitadas (CMMI Nivel 3 o superior, IT MARK, ISO 27001, ISO 20000, ISO 15504, ISO 9001 alcance en: desarrollo y/o implantación de software). La certificación deberá estar vigente a la fecha de evaluación.

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

2.4.2.1 Especificaciones de la entrega del documento.

- Cada formato de certificaciones exigibles a la compañía del aspirante deberá estar diligenciado y también firmado con huella legible por el Representante Legal del aspirante debidamente autenticado en Notaría con firma y huella.

- Deberá aportar la(s) certificación(es) en ISO 9001 expedidas por las entidades certificadoras autorizadas y alguna de las siguientes certificaciones solicitadas: IT MARK, CMMI nivel 3 o superior, ISO 27001, ISO 20000, ISO 15504, ISO 9001 alcance en: desarrollo y/o implantación de software. Las certificaciones deberán estar vigentes a la fecha de evaluación.

- Si la propuesta es presentada en Unión Temporal o en Consorcio, se debe presentar el Modelo de certificaciones exigibles a la compañía de cada una de las empresas que lo(a) conformen y todas deberán cumplir con el certificado de calidad ISO 9001.

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

2.4.2.2 Modelo de Certificaciones Exigibles a la compañía del aspirante

Modelo de Certificaciones exigibles a la compañía del Aspirante

NOMBRE O RAZÓN SOCIAL DE LA COMPAÑÍA DEL ASPIRANTE	
NIT DE LA COMPAÑÍA DEL ASPIRANTE	
NOMBRES Y APELLIDOS DEL REPRESENTANTE LEGAL DE LA COMPAÑÍA DEL ASPIRANTE	
CERTIFICACIONES APORTADAS	Sistema Gestión de la Calidad: ISO-9001 GP-1000 entidades públicas Alguna o Varias de las siguientes Certificaciones: ISO 27001

ISO 20000
ISO 15504
CMMI
IT MARK
ISO-9001 Desarrollo y/o implantación de software.

Modelo de Certificaciones exigibles a la compañía del Aspirante

Certificación **ISO 9001**

Certificado No_____

Fecha de Expedición: DDMMAAAA

Fecha de Vencimiento: DDMMAAAA

Entidad Certificadora: _____

Teléfono Contacto Ent. Certificadora:_____

Web Consulta Ent. Certificadora:_____

e-mail contacto Ent. Certificadora:_____

Certificación **ISO 27001**

Certificado No._____

Fecha de Expedición: DDMMAAAA

Fecha de Vencimiento: DDMMAAAA

Entidad Certificadora: _____

Teléfono Contacto Ent. Certificadora:_____

Web Consulta Ent. Certificadora:_____

e-mail contacto Ent. Certificadora:_____

Certificación **ISO 20000**

Certificado No._____

Fecha de Expedición: DDMMAAAA

Fecha de Vencimiento: DDMMAAAA

Entidad Certificadora: _____

Teléfono Contacto Ent. Certificadora:_____

Certificación **ISO 15504**

Certificado No._____

Fecha de Expedición: DDMMAAAA

Fecha de Vencimiento: DDMMAAAA

Entidad Certificadora: _____

Teléfono Contacto Ent. Certificadora:_____

Web Consulta Ent. Web Consulta Ent.

Certificadora:_____ Certificadora:_____

e-mail contacto Ent. e-mail contacto Ent.

Certificadora:_____ Certificadora:_____

Certificación **CMMI** Nivel_____ Certificación **IT** **MARK**

Certificado No._____ Certificado No._____

Fecha de Expedición: DDMMAAAA Fecha de Expedición: DDMMAAAA

Fecha de Vencimiento: DDMMAAAA Fecha de Vencimiento: DDMMAAAA

Entidad Entidad

Certificadora: Certificadora:

_____ _____

Teléfono Contacto Ent. Teléfono Contacto Ent.

Certificadora:_____ Certificadora:_____

Web Consulta Ent. Web Consulta Ent.

Certificadora:_____ Certificadora:_____

e-mail contacto Ent. e-mail contacto Ent.

Certificadora:_____ Certificadora:_____

Certificación **ISO** **9001**

Alcance en: Desarrollo y/o Implantación de Software

Certificado No._____

Fecha de Expedición: DDMMAAAA

Fecha de Vencimiento: DDMMAAAA

Entidad Certificadora: _____

Teléfono Contacto Ent. Certificadora:_____

Web Consulta Ent. Certificadora:_____

e-mail contacto Ent. Certificadora:_____

_____

Firma y Huella Representante Legal del Aspirante

2.4.3 Equipo de Trabajo exigible a la compañía

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

2.4.3.1 Equipo de Dirección

2.4.3.1.1 Gerente de Proyectos

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

Se requerirá 1 (un) profesional en ingeniería de sistemas, industrial, electrónica o afines, con especialización en gerencia de proyectos o maestría en ingeniería de sistemas o con certificación de PMP y experiencia certificada en la dirección de proyectos en los últimos 3 años. Con el fin de asegurar la idoneidad y estabilidad del equipo de trabajo se deberá adjuntar copia de título profesional, matrícula profesional vigente, certificaciones y demostrar que tienen algún tipo de contrato con el aspirante a proveedor.

2.4.3.2 Equipo de trabajo de seguridad

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

2.4.3.2.1 Gerente de SOC

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

1 (un) profesional en ingeniería de sistemas, industrial, electrónica o carreras afines, con especialización o maestría en seguridad informática o certificación como auditor interno de ISO-27001. Con el fin de asegurar la idoneidad y estabilidad del equipo de trabajo se deberá

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

2.4.3.2.2 Oficial de Seguridad

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

1 (un) profesional en ingeniería de sistemas, electrónico, de redes o afines con posgrado en seguridad de la información o maestría en seguridad informática o certificado como CISSP o CISM. Con el fin de asegurar la idoneidad y estabilidad del equipo de trabajo se deberá adjuntar copia de título profesional, Matrícula Profesional Vigente, certificaciones y demostrar que tienen algún tipo de contrato con el aspirante a proveedor.

2.4.3.2.3 Especialista DAM o DBA

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

1 (un) 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 o certificación como DBA de las Base de Datos utilizadas en la solución presentada por el aspirante.

2.4.3.2.4 Especialista en Ethical Hacking

Tiene a su cargo adelantar las actividades tendientes a detectar las debilidades y vulnerabilidades en los sistemas, utilizando para ello, el mismo conocimiento y herramientas de un hacker malicioso, con el fin de generar las herramientas de prevención que requiere el sistema.

Se requerirá 1 (un) profesional en ingeniería de sistemas, electrónico, de redes o afines, certificado como CEH, o contrato con una compañía para la prestación de servicios de Ethical Hacking. Con el fin de asegurar la idoneidad y estabilidad del equipo de trabajo se deberá adjuntar copia de título profesional, matrícula profesional vigente, certificaciones y demostrar que tienen algún tipo de contrato con el aspirante a proveedor.

2.4.3.3 Equipo de trabajo de desarrollo

2.4.3.3.1 Ingenieros o tecnólogos de desarrollo

Se hace necesario para la integración de las diferentes áreas del sistema de control y vigilancia para los CDA, una aplicación o software.

Se requerirá un (1) profesional en ingeniería de sistemas o tecnólogo en sistemas con certificación en los lenguajes de programación donde se encuentra construida la aplicación presentada por el aspirante para la solución del Sistema de Control y Vigilancia.

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

En caso que el desarrollo sea de una fábrica de software deberá tener un contrato con dicha fábrica, las licencias de uso y el personal certificado por la casa de software.

2.4.3.4 Equipo de trabajo de soporte

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

2.4.3.4.1 Coordinador de Soporte

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

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

2.4.3.5 Mesa de Ayuda

(en inglés: Help Desk, mal traducido como 'Ayuda de Escritorio'), o Mesa de Servicio (Service Desk) es un conjunto de recursos tecnológicos y humanos, para prestar servicios con la posibilidad de gestionar y solucionar todas las posibles incidencias de manera integral, junto con la atención de requerimientos relacionados a las Tecnologías de la Información y la Comunicación (TIC). El personal o recurso humano encargado de Mesa de Ayuda (MDA) debe proporcionar respuestas y soluciones a los usuarios finales, clientes o beneficiarios (destinatarios del servicio), y también puede otorgar asesoramiento en relación con una organización o institución, productos y servicios. Generalmente, el propósito de MDA es solucionar problemas o para orientar acerca de computadoras, equipos electrónicos o software. El aspirante a homologación debe entregar el esquema de atención de la mesa de ayuda firmado por un Ingeniero con ITIL intermedio o superior, quien avale que los procesos de mesa de ayuda han sido diseñados basados en las mejores prácticas de ITIL.

Al entrar en operación, el equipo de mesa de ayuda será el necesario para el cumplimiento de los ANS (ACUERDO DE NIVELES DE SERVICIO) solicitados conforme al número de CDA's contratados.

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

2.4.3.6 Especificaciones de la entrega del documento

- Cada Formato Modelo de Equipo de trabajo exigible a la compañía, deberá estar diligenciado y también firmado con huella legible por el Representante Legal del aspirante debidamente autenticado en Notaría con firma y huella.

- Deberá aportar para cada perfil: *Cargo, copia de título profesional, título de posgrado, certificaciones, experiencia comprobada y certificada, contrato laboral directo con el aspirante a proveedor y copia de la planilla del último mes en donde se evidencie el pago de los parafiscales de todos los profesionales.*

- En caso de subcontratar el servicio de SOC, se deberá anexar el contrato con la empresa que presta el servicio y las hojas de vida del personal solicitado.

2.4.3.7 Modelo de Certificaciones Exigibles a la compañía del aspirante

Modelo de Certificaciones exigibles a la compañía del Aspirante

NOMBRE O RAZÓN SOCIAL DE LA COMPAÑÍA DEL ASPIRANTE

NIT DE LA COMPAÑÍA DEL ASPIRANTE

NOMBRES Y APELLIDOS DEL REPRESENTANTE LEGAL DE LA COMPAÑÍA DEL ASPIRANTE

Equipo de Dirección Gerente de Proyectos.	Título profesional en: (especifique el título de grado) Ingeniería de Sistemas, Industrial, Electrónica Carreras Afines Posgrado o certificación: (especifique el

	título de posgrado) En gerencia de proyectos Maestría en ingeniería de sistemas Certificación de PMP Experiencia: Dirección de proyectos en los últimos 3 años. Tipo de Contrato: (especifique el tipo de contrato) Pago de Aportes Parafiscales: (Especifique el o los números de folio donde aporta la planilla con dicho pago)
Equipo de trabajo de seguridad **Gerente de SOC.**	Título profesional en: (especifique el título de grado) Ingeniería de Sistemas, Industrial, Electrónica Carreras Afines Posgrado certificación: (especifique el título de posgrado) En seguridad informática Certificación Auditor Interno ISO-27001 Tipo de Contrato: (especifique el tipo de contrato) Pago de Aportes Parafiscales: (Especifique el o los números de folio donde aporta la planilla con dicho pago)
Equipo de trabajo de seguridad **Oficial de Seguridad.**	Título profesional en: (especifique el título de grado) Ingeniería de Sistemas, Industrial,

	Electrónica Carreras Afines Posgrado certificación: (especifique el título de posgrado) En seguridad informática Certificado como CISSP Certificado como CISM Tipo de Contrato: (especifique el tipo de contrato) Pago de Aportes Parafiscales: (Especifique el o los números de folio donde aporta la planilla con dicho pago)
Equipo de trabajo de seguridad **Especialista DAM o DBA.**	Título profesional en: (especifique el título de grado) Ingeniería de Sistemas, Industrial, Electrónica Carreras Afines Certificación técnica: (especifique el fabricante de la herramienta DAM o de la Base de Datos) DAM DBA Tipo de Contrato: (especifique el tipo de contrato) Pago de Aportes Parafiscales: (Especifique el o los números de folio donde aporta la planilla con dicho pago)
Equipo de trabajo de seguridad **Especialista en Ethical Hacking.**	Título profesional en: (especifique el título de grado) Ingeniería de Sistemas, Industrial,

	Electrónica
	Carreras Afines
	Certificación técnica: (especifique el fabricante de la herramienta DAM o de la Base de Datos)
	CEH
	Contrato con una compañía para la prestación de Servicios de Ethical Hacking.
	Tipo de Contrato: (especifique el tipo de contrato)
	Pago de Aportes Parafiscales: (Especifique el o los números de folio donde aporta la planilla con dicho pago)
Equipo de trabajo de desarrollo	Título en: (especifique el título de grado)
Ingenieros o tecnólogos de desarrollo.	Ingeniería de Sistemas,
	Tecnólogo de Sistemas
	Certificación técnica: (especifique el lenguaje de desarrollo en que se encuentra construida la aplicación)
	Aplica (deberá adjuntar las respectivas certificaciones)
	No aplica
	Contrato con una fábrica de software: (especifique el contrato con dicha fábrica, licencias de uso y el personal certificado por la casa de software)
	Aplica (deberá adjuntar el contrato, licencias de uso y certificaciones del personal de la fábrica de software)
	No aplica
	Tipo de Contrato: (especifique el tipo de contrato)
	Pago de Aportes Parafiscales: (Especifique el

	o los números de folio donde aporta la planilla con dicho pago)
Equipo de trabajo de soporte **Coordinador de Soporte.**	Título profesional en: (especifique el título de grado) Ingeniería de Sistemas, Industrial, Electrónica Carreras Afines Experiencia como Líder de Soporte: (especifique el o los números de folio donde aporta la experiencia) Tipo de Contrato: (especifique el tipo de contrato) Pago de Aportes Parafiscales: (especifique el o los números de folio donde aporta la planilla con dicho pago)
Mesa de Ayuda	Esquema de atención de la mesa de ayuda firmado por un Ingeniero con ITIL intermedio o superior, quien avale que los procesos de mesa de ayuda han sido diseñados basados en las mejores prácticas de ITIL: (especifique el o los números de folio donde aporta la experiencia)

_____

Firma y Huella Representante Legal del Aspirante

2.4.4 Aliado u Operador de Recaudo

<Numeral modificado por el artículo 1 de la Resolución 5786 de 2016. El nuevo texto es el siguiente:> El aspirante a proveedor deberá contar con uno o más aliados u operadores de recaudo que deberán cumplir con los siguientes requisitos y requerimientos:

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

2. Ser un miembro del Sistema Financiero Colombiano (en el caso de los bancos deberá ser calificado como de bajo riesgo), u operador postal de pago habilitado o autorizado en

Colombia y que tenga convenio para este proyecto por lo menos con una entidad financiera vigilada por la Superintendencia Financiera de Colombia.

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

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

– Actualización en línea de lo recaudado.

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

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

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

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

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

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

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

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

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

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

5. El o los aliados de Recaudo, deberán generar una póliza de cumplimiento a favor de cada Centro de Diagnóstico Automotor y del homologado por el buen manejo del dinero recaudado.

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

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

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

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

En cualquier momento, el aspirante a proveedor o el proveedor autorizado de los sistemas de control y vigilancia de los centros de diagnóstico automotor, podrá solicitar la ampliación del número de aliados de recaudo, cumpliendo con los requisitos antes señalados.

Notas de Vigencia

Legislación Anterior

2.5 LISTA DE REQUISITOS FINANCIEROS.

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

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

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

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

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

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

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

Razón de Cobertura de Intereses = Utilidad Operacional / Gastos de Intereses, el cual refleja la capacidad del aspirante de cumplir con sus obligaciones financieras. A mayor cobertura de intereses, menor es la probabilidad de que el aspirante incumpla sus obligaciones financieras.

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

Indicador	Si el indicador es mayor,la probabilidad de Riesgo es	Límite
Índice de liquidez	Menor	Mínimo
Índice de endeudamiento	Mayor	Máximo
Razón de cobertura de intereses	Menor	Mínimo

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

La siguiente tabla presenta algunos indicadores adicionales de capacidad financiera:

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

a) Balance General, Estado de Resultados y las Notas a los Estados Financieros, con corte a 31 de diciembre de 2012 y a 31 de diciembre de 2013 aprobados por el órgano competente, **debidamente certificados y dictaminados** (Decreto número 2649 de 1993, Ley 222 de 1995 y Decreto número 1406 de 1999).

El artículo 37 de la Ley 222 de 1995 y la Circular Externa número 037 de 2001 de la Junta Central de Contadores establece en relación con los estados financieros certificados que: *"El representante legal y el contador público bajo cuya responsabilidad se hubiesen preparado los estados financieros deberán certificar aquellos que se pongan a disposición de los asociados o terceros. La certificación consiste en declarar que se han verificado previamente las afirmaciones contenidas en ellos, conforme al reglamento y que las mismas se han tomado fielmente de los libros"*.

Así mismo, los balances estarán discriminados de la siguiente manera:

ACTIVOS: Corriente, no corriente y total

PASIVOS: Corriente, no corriente, total, y

PATRIMONIO

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

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

b) Fotocopia de la tarjeta profesional del contador, revisor fiscal o contador independiente, según corresponda;

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

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

INDICADORES	CONCEPTO	REQUISITO
CAPITAL REAL	CAPITAL SOCIAL RESERVAS CONSTITUIDAS UTILIDADES RETENIDAS UTILIDADES DEL EJERCICIO	> $4.000.000.000
LIQUIDEZ	ACTIVO CORRIENTE / PASIVO CORRIENTE	>=1,0 y <= 2,0
NIVEL DE ENDEUDAMIENTO	PASIVO TOTAL / ACTIVO TOTAL	<= al 70%
CAPITAL DE TRABAJO	ACTIVO CORRIENTE - PASIVO CORRIENTE	> $2.223.000.000
EBITDA	UTILIDAD OPERACIONAL + DEPRECIACIONES Y AMORTIZACIONES	> a 0
DE RIESGO	ACTIVO FIJO / PATRIMONIO NETO	<= 1
INDICADOR DE CRECIMIENTO DEL EBITDA	EBITDA ULTIMO AÑO/ EBITDA AÑO ANTERIOR	> a 0,5

En caso de participar en unión temporal o consorcio, se deberá cumplir con los indicadores financieros conforme a los parámetros que se definen a continuación. La siguiente es la fórmula aplicable para los indicadores que son valores absolutos, como el capital de trabajo:

$$(i)\ Indicador\ en\ valor\ absoluto = \sum_{i=1}^{n} Indicador_i$$

Donde n es el número de integrantes del oferente plural (unión temporal, consorcio).

Para los indicadores que provienen de la división de cuentas de los estados financieros, se analizarán bajo el método de ponderación de los componentes de los indicadores:

En este método cada uno de los integrantes del oferente aporta al valor total de cada componente del indicador de acuerdo con su participación en la figura del oferente plural (unión temporal, consorcio o promesa de sociedad futura).

La siguiente es la fórmula aplicable para los indicadores que son índices en la opción 1:

$$(ii)\ Indicador = \frac{\left(\sum_{...} Componente\ 1\ del\ indicador_i \times porcentaje\ de\ participación_i\right)}{\left(\sum_{...} Componente\ 2\ del\ indicador_i \times porcentaje\ de\ participación_i\right)}$$

Donde n es el número de integrantes del oferente plural (unión temporal, consorcio).Esta opción incentiva que el integrante del proponente plural con los mejores indicadores tenga una mayor participación en dicho proponente plural.

2.6. LISTA DE REQUISITOS TÉCNICOS.

Este documento establece los requisitos técnicos mínimos que deben ser cumplidos por el Operador para garantizar la operación del Sistema de Control y Vigilancia para los CDA's en sus diferentes componentes (Sistema Central de Datos, Centro de Operaciones de Seguridad y red de comunicaciones), de la información de cada una de las transacciones en tiempo real en el momento que se realicen en cualquiera de los equipos de los CDA, así como para la generación, procesamiento y transmisión de la información requerida.

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

2.6.1 ASPECTOS TÉCNICOS GENERALES

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

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

El proceso a grandes rasgos deberá ser capaz de:

- Grabar de forma automática los momentos necesarios del recorrido del vehículo en el CDA, que son, a la entrada al recinto, a la entrada a la pista y durante todo el recorrido de la pista, así como todo el tiempo la cámara situada en la oficina de gestión del CDA.

- Detectar de forma automática las matrículas de los vehículos, extrayendo fotografías en la entrada del recinto y al inicio de pista.

- Unir todos los videos pertenecientes a un vehículo en un solo fichero y asociarle las fotografías del aparte anterior.

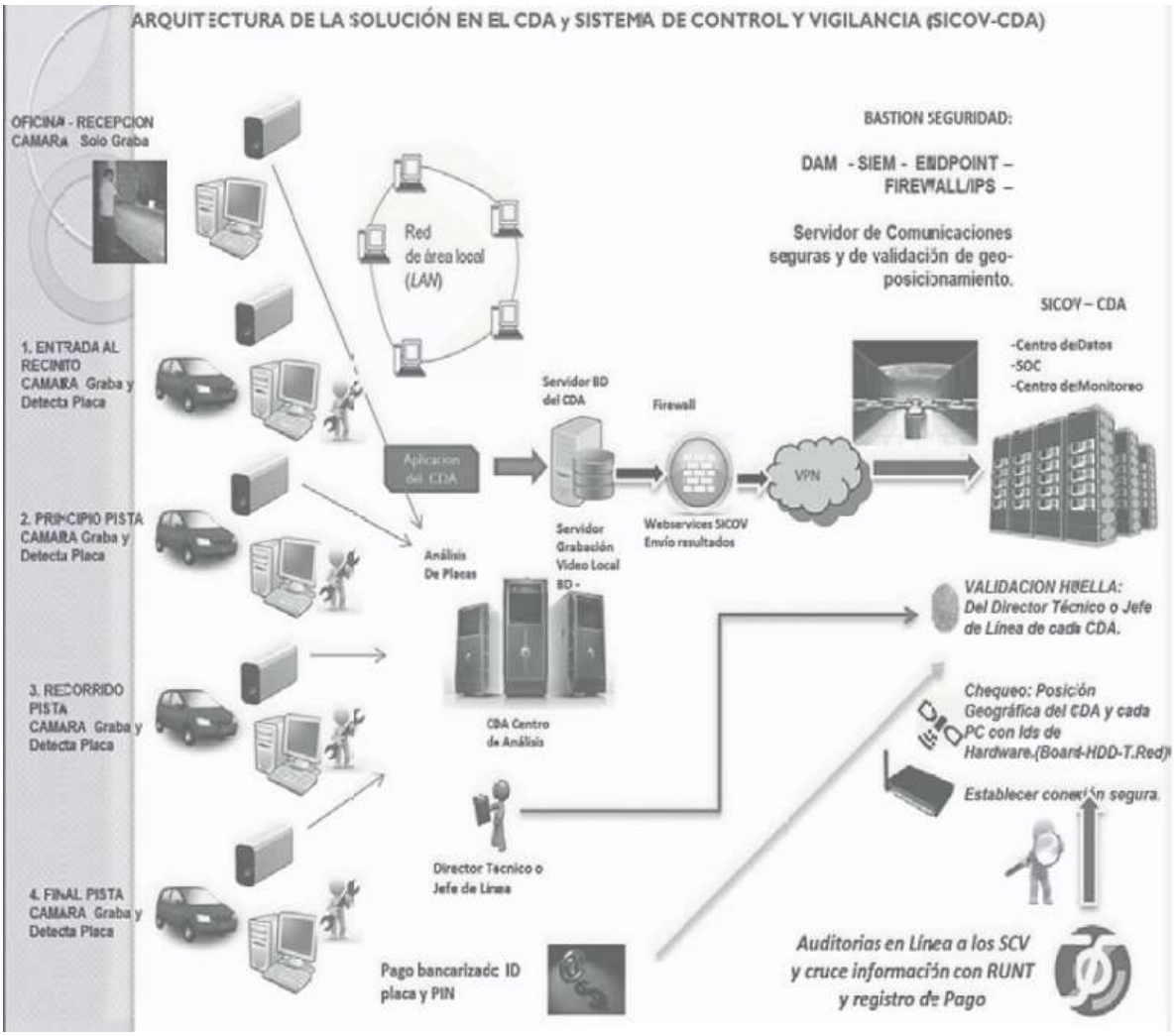
- Añadir los datos de la revisión RTMEC a la ficha del video del vehículo con los elementos técnicos que proporcione el software del CDA.

- Generar alarmas si un vehículo no cumple las características técnicas esperadas en cada uno de los aspectos a inspeccionar.

- Proporcionar estadísticas de las inspecciones de cada CDA.

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

El siguiente gráfico ilustra a alto nivel la arquitectura y los flujos del sistema:



2.6.2 REQUISITOS FUNCIONALES, TECNOLÓGICOS Y LOGÍSTICOS DE FUNCIONALIDAD DEL SISTEMA DE CONTROL Y VIGILANCIA PARA LOS CDA.

Plataforma tecnológica que soporta el proceso de inspección, vigilancia y control de la realización de la revisión técnico-mecánica por parte de los CDA, estará a cargo de los operadores homologados. Sus instalaciones y las del sistema de respaldo deberán estar ubicadas en la República de Colombia, en un sitio seguro, con controles de acceso y vigilancia, que permita procesos de auditoría sobre la información. Lo compone además de los elementos de hardware requeridos, un conjunto de programas (software) que garantizan la adecuada operación. A su vez, el SCV es el encargado del envío de la información solicitada por la Supertransporte.

Los servidores centrales del SCV deben tener la capacidad necesaria para garantizar el procesamiento de las operaciones realizadas en los CDA, con la concurrencia que el mercado demande. Estos servidores deben tener la capacidad de ser expandidos a medida que aumenten y cambien las necesidades. El SCV debe suministrar provisiones de alta disponibilidad para asegurarse que la falla en cualquier componente del sistema servidor no

cause la interrupción del sistema ni afecte su operación total. Debe ser capaz de ser reparado en cualquiera de sus componentes redundantes sin afectar la operación.

El SCV deberá tener una infraestructura tecnológica estable que garantice la disponibilidad de la información almacenada en una de las bases de datos: información de control, resultados de los eventos, información de los registros o transacciones generadas. Debe tener como mínimo: un arreglo de servidores redundantes, un sistema de red de comunicación de datos y una base de datos relacional. El servidor o servidores deberán cumplir con los requerimientos de conectividad y seguridad (se utilizan como guía los estándares IEEE 802 y 27001).

-- Registrar todas las transacciones y operaciones realizadas desde los computadores y equipos ubicados en los CDA interconectados al SCV: transacciones, videos, eventos, datos de control, así como eventos de funcionamiento del SCV.

-- Toda transacción debe ser replicada al sistema redundante de respaldo. Se debe de garantizar que el 100% de las transacciones se encuentran replicadas al momento de requerirse la entrada en operación del sistema de respaldo.

-- Registro de los resultados de las revisiones técnico mecánicas.

-- Garantizar el correcto funcionamiento de las actividades del SCV en el CDA.

-- Generar los mecanismos de seguridad de la información en línea, a través de alarmas y novedades.

La plataforma tecnológica (hardware, software, comunicaciones, bases de datos, etc.) necesaria para el control, seguimiento y auditoría por parte de la Supertransporte de las revisiones técnico mecánicas realizadas por los CDA, que deberá ser provista, instalada y puesta en operación por el Operador, requiere cumplir como mínimo con lo siguiente:

– *Centro de Procesamiento de Datos (CPD).* Infraestructura para alojar el aplicativo, con una base de datos que será una réplica de todas y cada una de las transacciones del sistema.

– *Centro de Operaciones de Seguridad (SOC).* Se compone de personas, procesos, infraestructura y tecnología dedicados a gestionar, tanto de forma reactiva como proactiva, amenazas, vulnerabilidades y en general incidentes de seguridad de la información, con el objetivo de minimizar y controlar el impacto en la organización.

– *Comunicaciones.* Infraestructura necesaria para interconectar todos los elementos del Sistema de Control y Vigilancia y los Centros de Diagnóstico Automotor.

– *Software de inspección, vigilancia y Control.* Esta aplicación estará integrada con el CPD, SOC y Comunicaciones.

– *Mesa de Ayuda (Help Desk).* Es un conjunto de recursos tecnológicos y humanos, para prestar servicios con la posibilidad de gestionar y solucionar todas las posibles incidencias de manera integral, junto con la atención de requerimientos relacionados a las Tecnologías de la

Información y la Comunicación (TIC). El personal o recurso humano encargado de Mesa de Ayuda (MDA) debe proporcionar respuestas y soluciones a los usuarios finales, clientes o beneficiarios (destinatarios del servicio), y también puede otorgar asesoramiento en relación con una organización o institución, productos y servicios.

2.6.2.1 CENTRO DE PROCESAMIENTO DE DATOS (CPD)

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

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

Requisitos Generales:

-- Disponibilidad y monitorización “24x7x365” un centro de datos diseñado apropiadamente proporcionará disponibilidad, accesibilidad y confianza 24 horas al día, 7 días a la semana, 365 días al año.

-- Fiabilidad: Los centros de datos deben tener redes y equipos altamente robustos y comprobados.

-- Seguridad, redundancia y diversificación: Almacenaje exterior de datos, tomas de alimentación eléctrica totalmente independientes y de servicios de telecomunicaciones para la misma configuración, equilibrio de cargas, sistemas de alimentación ininterrumpida o SAI, control de acceso, etc.

-- Control ambiental / prevención de incendios: El control de ambiente trata de la calidad de aire, temperatura, humedad, inundación, electricidad, control de fuego, y por supuesto, acceso físico.

-- Acceso a internet y conectividad a redes de área extensa WAN para conectividad a Internet: Los centros de datos deben ser capaces de hacer frente a las mejoras y avances en los equipos, estándares y anchos de banda requeridos, pero sin dejar de ser manejables y fiables.

-- El centro de procesamiento de datos podrá estar ubicado en el territorio nacional o extranjero, los costos de traslado y viáticos diferentes a la ciudad de Bogotá serán asumidos por el aspirante a proveedor para su verificación en la visita de evaluación.

2.6.2.1.1 SEGURIDAD FÍSICA Y AMBIENTAL

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

1. Desastres naturales, incendios accidentales, tormentas e inundaciones.

2. Amenazas ocasionadas por el hombre.

3. Disturbios, sabotajes internos y externos deliberados.

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

2.6.2.1.2 Control de Acceso

Las áreas restringidas como los CPD necesitan una buena gestión de los accesos a la sala. Los sistemas de control de accesos son sistemas creados para la gestión e integración informática de las necesidades de una empresa relacionadas con el control de accesos de sus empleados o de personas ajenas en sus edificios y delegaciones, existen varias opciones de terminales según el nivel de seguridad necesario (banda magnética, proximidad, teclado/pin y biométrico). Sistemas Biométricos. El centro de operaciones de seguridad deberá contar con un control de acceso biométrico a través de huella dactilar, o de reconocimiento facial, o de verificación de patrones oculares. Se validará que cumplan con los estándares actuales para el acceso biométrico utilizado seleccionado.

2.6.2.1.3 Protección electrónica

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

2.6.2.1.3.1 CCTV (Circuito Cerrado de Televisión)

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

2.6.2.1.4 Condiciones Ambientales

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

2.6.2.1.4.1 Sistema contra Incendios

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

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

-- El local CPD no debe situarse encima, debajo o adyacente a áreas donde se procesen, fabriquen o almacenen materiales inflamables, explosivos, gases tóxicos o sustancias radioactivas.

-- Las paredes deben hacerse de materiales incombustibles y extenderse desde el suelo al techo.

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

-- No debe estar permitido fumar en el área de proceso.

-- Deben emplearse muebles incombustibles, y cestos metálicos para papeles. Deben evitarse los materiales plásticos e inflamables.

-- El piso y el techo en el recinto del centro de cómputo y de almacenamiento de los medios magnéticos deben ser impermeables.

-- Seguridad del Equipamiento. Es necesario proteger los equipos de cómputo instalándolos en áreas en las cuales el acceso a los mismos sólo sea para personal autorizado. Además, es necesario que estas áreas cuenten con los mecanismos de ventilación y detección de incendios adecuados. Para protegerlos se debe tener en cuenta que:

– La temperatura no debe sobrepasar los 18o C y el límite de humedad no debe superar el 65% para evitar el deterioro.

– Los centros de cómputos deben estar provistos de equipo para la extinción de incendios en relación al grado de riesgo y la clase de fuego que sea posible en ese ámbito.

– Deben instalarse extintores manuales (portátiles) y/o automáticos (rociadores).

– Recomendaciones. El personal designado para usar extinguidores de fuego debe ser entrenado en su uso.

– Si hay sistemas de detección de fuego que activan el sistema de extinción, todo el personal de esa área debe estar entrenado para no interferir con este proceso automático.

– Implementar paredes protectoras de fuego alrededor de las áreas que se desea proteger del incendio que podría originarse en las áreas adyacentes.

– Proteger el sistema contra daños causados por el humo. Este, en particular la clase que es principalmente espeso, negro y de materiales especiales, puede ser muy dañino y requiere una lenta y costosa operación de limpieza.

– Mantener procedimientos planeados para recibir y almacenar abastecimientos de papel.

2.6.2.1.4.3 Sistema de Aire Acondicionado

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

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

2.6.2.1.4.3 Inundaciones

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

– Techo impermeable para evitar el paso de agua desde un nivel superior.

– Puertas acondicionadas para contener el agua que bajase por las escaleras.

2.6.2.1.4.4 Terremotos

El Centro de Procesamiento de Datos (CPD) y el Centro de Operaciones de Seguridad deberán estar en una edificación antisísmica, conforme al estándar actual requerido. Se verificará su autenticidad.

2.6.2.1.5 Sistema de Alimentación Ininterrumpida (SAI)

EL CPD deberá contar con un sistema de corriente regulada en línea y de contingencia que garantice la operatividad en ausencia del sistema de suministro de energía principal del edificio por un tiempo mínimo de 4 horas continuas. Los equipos de sistema de alimentación ininterrumpida deberán ser protección nivel 9 (ON-LINE de DOBLE CONVERSIÓN). Se verificará en la visita. Ver documento: “ANEXO REQUISITOS TÉCNICOS INFRAESTRUCTURA TECNOLÓGICA Y DE COMUNICACIONES”

2.6.2.1.6 Red Eléctrica

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

2.6.2.1.7 Ubicación

El CPD deberá estar ubicado en territorio nacional.

2.6.2.1.8 Consideraciones generales

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

2.6.2.1.9 SEGURIDAD LÓGICA

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

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

Así, la Seguridad Física, sólo es una parte del amplio espectro que se debe cubrir para no vivir con una sensación ficticia de seguridad. El activo más importante que se posee es la información, y por lo tanto deben existir técnicas, más allá de la seguridad física, que la aseguren. Estas técnicas las brinda la Seguridad Lógica.

Existe un viejo dicho en la seguridad informática que dicta que “todo lo que no está permitido debe estar prohibido” y esto es lo que debe asegurar la Seguridad Lógica.

Los objetivos que se plantean son:

-- Restringir el acceso a los programas y archivos.

-- Asegurar que los operadores puedan trabajar sin una supervisión minuciosa y no puedan modificar los programas ni los archivos que no correspondan.

-- Asegurar que se estén utilizados los datos, archivos y programas correctos en y por el procedimiento correcto.

-- Que la información transmitida sea recibida sólo por el destinatario al cual ha sido enviada y no a otro.

-- Que la información recibida sea la misma que ha sido transmitida.

-- Que existan sistemas alternativos secundarios de transmisión entre diferentes puntos.

-- Que se disponga de pasos alternativos de emergencia para la transmisión de información.

2.6.2.1.9.1 Controles de Acceso

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

2.6.2.1.9.1.1 Identificación y Autenticación

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

2.6.2.1.9.2 Roles

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

2.6.2.1.9.3 Limitaciones a los servicios

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

2.6.2.1.10 Modalidad de Acceso

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

2.6.2.1.11 Ubicación y Horario

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

2.6.2.1.12 Administración

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

2.6.2.1.13 Administración del Personal y Usuarios – Organización del personal

Este proceso debe llevar los siguientes cuatro pasos:

1. Definición de puestos. Debe contemplarse la máxima separación de funciones posibles y el otorgamiento del mínimo permiso de acceso requerido por cada puesto para la ejecución de las tareas asignadas.

2. Determinación de la sensibilidad del puesto.

3. Elección de la persona para cada puesto.

4. Entrenamiento inicial y continuo del empleado.

2.6.2.1.13.1 Actualizaciones de sistemas y aplicaciones

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

2.6.2.2 CENTRO DE OPERACIONES Y SEGURIDAD (SOC)

2.6.2.2.1 SEGURIDAD FÍSICA Y AMBIENTAL

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

1. Desastres naturales, incendios accidentales.

2. Amenazas ocasionadas por el hombre.

3. Sabotajes internos y externos deliberados.

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

2.6.2.2.2 Control de Acceso

2.6.2.2.2.1 Sistemas Biométricos

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

2.6.2.2.2.2 Protección electrónica

2.6.2.2.2.2.1 CCTV (Circuito Cerrado de Televisión)

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

2.6.2.2.2.3 Condiciones Ambientales

2.6.2.2.2.3.1 Sistema contra Incendios

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

– El SOC debe contar con elementos de detección y extinción de fuego, en relación al grado de riesgo y la clase de fuego que sea posible en ese ámbito.

– No debe estar permitido fumar en el área.

– El SOC debe contar con un esquema de evacuación, y su personal debidamente capacitado ante desastres.

– Seguridad del Equipamiento. Es necesario proteger los equipos de cómputo instalándolos en áreas en las cuales el acceso a los mismos sólo sea para personal autorizado. Además, es necesario que estas áreas cuenten con los mecanismos de ventilación y detección de incendios adecuados. Para protegerlos se debe tener en cuenta que:

- La temperatura no debe sobrepasar los 23oC.

- Deben instalarse extintores manuales (portátiles) y/o automáticos (rociadores).

– Recomendaciones. El personal designado para usar extinguidores de fuego debe ser entrenado en su uso.

- Si hay sistemas de detección de fuego que activan el sistema de extinción, todo el personal de esa área debe estar entrenado para no interferir con este proceso automático.

2.6.2.2.2.3.2 Sistema de Aire Acondicionado

Se debe proveer un sistema de ventilación y aire acondicionado, que se dedique al SOC en forma exclusiva. Teniendo en cuenta que los aparatos de aire acondicionado son causa

potencial de inundaciones, en caso de utilizar sistemas de enfriamiento por agua se verificará que estén instaladas redes de protección en todo el sistema de cañería al interior y al exterior.

2.6.2.2.2.3.3 Terremotos:

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

2.6.2.2.2.4 Sistema de Alimentación Ininterrumpida (SAI)

El SOC deberá contar con un sistema de corriente regulada en línea y de contingencia que garantice la operatividad en ausencia del sistema de suministro de energía principal por un tiempo mínimo de 4 horas continuas. Se verificará en la visita.

2.6.2.2.3 SEGURIDAD LÓGICA

2.6.2.2.3.1 Controles de Acceso

2.6.2.2.3.1.1 Identificación y Autenticación

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

2.6.2.2.3.2 Roles

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

2.6.2.2.3.3 Modalidad de Acceso

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

2.6.2.2.3.4 Ubicación y horario

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

2.6.2.2.3.5 Administración

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

2.6.2.2.3.6 Actualizaciones de sistemas y aplicaciones

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

2.6.2.2.4 SOFTWARE DE SEGURIDAD MONITOREO

Se debe tener un sistema y/o Software que genere alarmas, las cuales deben llegar al Sistema de Control y Vigilancia y a su vez al CICTT - Centro Inteligente de Control de Tránsito y Transporte (cuando entre en operación), el cual tenga como mínimo los siguientes parámetros:

2.6.2.2.4.1 De los equipos

– Desconexión de cámara.

– Falta de señal de la cámara.

– De cambio de ubicación en el geoposicionamiento de los equipos instalados en el CDA.

– De intento de manipulación de los equipos ubicados en el CDA.

– De ausencia de fluido eléctrico en el CDA.

– De disco lleno.

– Debe permitir a través de un dispositivo de comunicaciones remoto y/o con un agente de software instalado en el servidor propiedad del CDA, realizar un registro inicial de los Números de Identificación (ID) de la tarjeta madre, Disco duro y Tarjeta de red física, para su posterior verificación, cada vez que establezcan conexión con él.

Estas alarmas se verificarán en la visita al CDA y en el SOC de los Sistemas de control de vigilancia y serán requisito para homologarse.

2.6.2.2.4.2 Del Software de gestión

– Si él envió de los resultados del FUR no coinciden con la hora y fecha de la grabación del video.

– Si el CDA no quemó el pin del operador de recaudo a través de la interface suministrada por el homologado.

– Si los datos del RUNT (FUR) no coinciden con los entregados por el CDA al homologado, (se garantiza con una carta de compromisos posteriores a la homologación).

– Si la prueba es por reinspección y se quiere cambiar otro dato diferente al rechazado en la primera revisión.

Estas alarmas se verificarán en la visita al CDA y en el SOC de los Sistemas de control de vigilancia y serán requisito para homologarse.

2.6.2.2.4.3 De seguridad de la información

El Sistema debe contar con una solución SIEM, que permita el análisis en tiempo real de las alertas de seguridad generadas por el hardware y el software involucrado. Estas se verificarán en la visita al SOC de los Sistemas de control de vigilancia y serán requisito para homologarse. La herramienta deberá estar clasificada en el último cuadrante de Gartner, en el cuadro de Líderes o Competidores.

2.6.2.2.5 GESTIÓN DE ALMACENAMIENTO DE LA INFORMACIÓN (seguridad 27001)

El Sistema de almacenamiento debe contemplar las siguientes consideraciones:

-- Sistema de fuentes de poder n+1.

-- El sistema de almacenamiento debe contemplar arreglos de discos Arreglo de discos en raid 5 con Spare disks, mínimo 1 disco en Spare.

-- Doble sistema de conexión con servidor, en iScsi o F.O.

-- Se debe considerar un sistema de respaldo de información, con procesos de restauración de la información y sus protecciones correspondientes. Se debe garantizar un respaldo de la información, donde deberá tener una redundancia de la base de datos. Se realizarán pruebas de restauración de datos.

-- Debe contemplar interface de administración web, vía Ethernet.

-- Debe configurarse alarmas sobre eventos de control de espacio en disco, así como monitoreo de los eventos generados por posibles fallas o alarmas del hardware o configuraciones.

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

- Que la documentación del sistema estar protegida contra el acceso no autorizado.

- Que se tienen políticas, procedimientos y controles formales de intercambio de información.

- Se debe mostrar que se cuenta con registro de usuarios, contraseñas y privilegios por cada usuario.

- Se debe demostrar que los equipos cuentan con las respectivas licencias del software utilizado, incluyendo sistema operativo.

- Se debe mostrar que se cuenta con procedimientos para el manejo.

- Y almacenamiento de la información con el fin de proteger la integridad de dicha información.

- Se debe demostrar que se cuenta con políticas y procedimiento de análisis del riesgo, disponibilidad e integridad de la información.

- Deberán demostrar a través de documento técnico cómo se realizará la retención de video por un año como mínimo (se garantiza además con una carta de compromisos posteriores a la homologación).

2.6.2.2.6 SEGURIDAD EN REDES Y COMUNICACIONES – firewall y elementos activos seguridad 27001

La seguridad en los elementos activos de redes y comunicaciones involucrados en el CPD y el SOC deben cumplir con los siguientes requerimientos:

– Servicios de inspección profunda de paquetes, Anti-Virus, Anti-Spyware, Intrusión Preventión.

– Filtrado de Contenido, Rastreo por HTTP URL, HTTPS IP, palabra clave y contenido, bloqueo de ActiveX, Java Applet, y cookies.

– Gestión de ancho de banda.

– IPS (sistema de prevención de intrusos).

2.6.2.2.7 ENCRIPTACIÓN DE LA INFORMACIÓN

La solución debe permitir las conexiones seguras VPN entre el SOC y cada uno de los CDA a monitorear. Debe cumplir con las siguientes características:

- Debe permitir cifrado/autenticación/grupo DH DES, 3DES, AES (128, 142, 256 bits), MD5, SHA-1/grupo DH 1, 2, 5, 14.

- Presentar opciones de conectividad que ofrezcan acceso remoto seguro de alta velocidad.

- Debe comprobar la fiabilidad de los usuarios remotos y los dispositivos terminales.

- Usar protocolos SSL VPN e IPSec VPN.

- Permitir prestaciones VPN Dead Peer Detection, DHCP a través de VPN, IPSec NAT Transversal, pasarela VPN redundante, y VPN basada en enrutamiento.

- Debe permitir Plataformas Global VPN Client soportadas como mínimo Microsoft® Windows 2000, Windows XP, Vista 32 bits/64 bits, Windows 7 32/64 bits.

- Debe permitir el intercambio de claves IKE, clave manual, Certificados (X.509), L2TP sobre IPSec.

- Debe permitir Plataformas SSL VPN Microsoft Windows 2000/ XP/ Vista 32 bits/64 bits/Windows 7, Mac OSX 10.4+, Linux FC3+/ Ubuntu 7+/ OpenSUSE.

- Debe permitir Plataforma Mobile Connect soportada iOS 4.2 y superior garantizar la integridad del acceso VPN desde dispositivos remotos, incluidos los basados en iOS.

- Permitir la reconexión WAN y VPN.

- Realizar clean VPN para cifrar y descontaminar el tráfico.

2.6.2.2.8 NORMATIVIDAD EN SEGURIDAD LOPD Y LSSICE

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

2.6.2.2.9 AUDITORÍAS DE SEGURIDAD INFORMÁTICA

El homologado deberá permitir como mínimo una auditoría en Seguridad informática al año, en la cual se validará el sostenimiento del cumplimiento de los requisitos como homologado. Los costos de esta auditoría estarán a cargo del homologado, estos quedaran definidos en los compromisos posteriores.

2.6.2.2.10 Otros Requisitos

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

– Descripción General del Sistema, Descripción General de Subsistemas, Diagrama de red, arquitectura de servidores, arquitectura general de la aplicación, arquitectura de seguridad física en sitios remotos y geo-posicionamiento satelital, esquema de seguridad de la información, esquema de intercambio transaccional para el recaudo, esquema de alta disponibilidad y continuidad de negocio, esquema de ANS. En el caso en que el representante legal de la compañía no sea ingeniero de sistemas o electrónico o afines deberá contar con una carta de aval de un ingeniero de sistemas o electrónico o afines.

El aspirante debe anexar el esquema de soporte para atención de los ANS (ACUERDO DE NIVELES DE SERVICIO) de la solución completa.

El aspirante a homologación podrá tener subcontratado el servicio de centro de operaciones de seguridad SOC. En este caso deberá presentar el contrato firmado con el proveedor que le preste el servicio de SOC mínimo por veinticuatro (24) meses y, las hojas de vida del equipo de seguridad podrán ser funcionarios del proveedor de SOC y cumpliendo con la totalidad de requisitos administrativos exigidos para el equipo de trabajo, no podrá subcontratar a otro aspirante a homologarse u homologado. Se aclara que el único responsable ante la Superintendencia por los ANS (ACUERDO DE NIVELES DE SERVICIO) es el homologado y no el SOC contratado.

– En caso de ser desarrollo propio, se debe adjuntar copia del certificado de registro de soporte lógico de la Dirección Nacional de Derechos de Autor. En el caso de que el aspirante utilice una licencia de software dé una solución fabricada por otra compañía, el aspirante deberá adjuntar copia de la respectiva licencia.

– El aspirante a homologación podrá tener subcontratado el servicio de Centro de Procesamiento de Datos (CPD). No podrá subcontratar a otro aspirante a homologarse. Se aclara que el único responsable ante la Superintendencia por los ANS (ACUERDO DE NIVELES DE SERVICIO) es el homologado y no el CPD contratado.

– El proveedor deberá suministrar Hardware, software, comunicaciones y servicios de integración y gestión de proyecto. A continuación se detallan los elementos Hardware y Software necesarios:

2.6.2.2.11 Compromisos Posteriores

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

- Los aspirantes a proveedores deberán presentar un documento de compromiso posterior, que la disponibilidad del servicio (ANS o SLA) con los CDA deberá ser al iniciar la operación como mínimo del 95% y al año de entrada en operación deberá ser del 97% con base en el horario de atención de los CDA.

- Establecer un canal dedicado con el sistema RUNT. Este canal entrará en vigencia, una vez el RUNT le entregue los protocolos que debe cumplir el homologado para dicha comunicación.

- Establecer las siguientes integraciones requeridas con el sistema RUNT:

-- Solicitud de número de certificado RTMEC.

-- Solicitud de Cargue de certificado RTMEC.

La Superintendencia de Puertos y Transporte se encargará de gestionar las autorizaciones con el RUNT para establecer los procesos de conexión.

- 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 Diagnóstico Automotor.

-- Acceso al Sistema de Captura de Video del Centro de Control.

-- Envío de alarmas.

-- Acceso a través de un usuario de consulta a la herramienta de control y monitoreo.

2.6.2.2.12 VISITAS DE VERIFICACIÓN

Se realizarán 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 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 auditoría 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 en la base de datos 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 que el sistema posea herramientas de pruebas de seguridad. Se deberá demostrar que están instaladas las herramientas de pruebas de seguridad de aplicación dinámica y estática;

f) Verificación que el sistema integrado muestre un mapa de ubicaciones de Centros y máquinas. Se deberá mostrar la ubicación de por lo menos un centro de diagnóstico automotor en la cual se muestre el estado de su conexión;

g) Verificación que graba de forma automática los momentos necesarios del recorrido del vehículo en el CDA, que son, a la entrada al recinto, a la entrada a la pista y durante todo el recorrido de la pista, así como la cámara situada en la oficina de gestión del CDA;

h) Verificación que el sistema detecta de forma automática las matrículas de los vehículos, extrayendo fotografías en la entrada del recinto y al inicio de pista;

i) Verificación que une o relaciona todos los videos pertenecientes a un vehículo en un solo fichero y asociarle las fotografías del aparte anterior;

j) Verificación que el sistema añade los resultados de la RTME (el FUR) al fichero del vehículo con los elementos técnicos que proporcione el software del CDA, según el estándar definido por el homologado que contrate el CDA;

k) Verificación que el sistema genera alarmas si un vehículo no cumple las características técnicas esperadas en cada uno de los aspectos a inspeccionar;

l) Verificación que el sistema proporciona estadísticas de las inspecciones de cada CDA.

2.6.2.2.13 PROCESOS DE VERIFICACIÓN

La plataforma de aplicaciones o de software integrada con otras tecnologías deberá realizar y verificar los siguientes procesos.

2.6.2.2.13.1 Proceso de verificación de la presencia del vehículo en las instalaciones del CDA a través de la captura del video registro fílmico.

a) Verificación del vehículo donde se cubra el 100% de la inspección técnico mecánica y de emisiones contaminantes efectuada y se permita la visualización de la placa para su plena identificación.

– Se deberá demostrar que una aplicación integrada con todo el sistema deberá realizar la identificación del vehículo a través de tecnología basada con video analítica con reconocimiento automático de placas, para lo cual deberá tener las cámaras necesarias para garantizar el monitoreo de los vehículos y sus placas desde que ingresan a pista hasta que finalizan la Revisión Técnico Mecánica y de Emisiones Contaminantes. Se realizará la validación de que el sistema de video analítica funcione automáticamente sin intervención manual en la detección y registro de placas, en vehículos de servicio público, servicio particular y motocicletas. Las especificaciones técnicas de las cámaras de video con video analítica son definidas en el documento "ANEXO REQUISITOS TÉCNICOS INFRAESTRUCTURA TECNOLÓGICA Y DE COMUNICACIONES";

b) Verificación del ingreso y salida del vehículo donde se permita la visualización de la placa para su plena identificación.

– Se deberá demostrar que una aplicación integrada con todo el sistema deberá realizar la identificación del vehículo a través de tecnología basada con video analítica con reconocimiento automático de placas sin intervención manual en cada una de las pruebas, para lo cual deberá tener las cámaras necesarias para garantizar el monitoreo de los vehículos y sus placas desde que ingresan a pista hasta que finalizan la revisión técnico mecánica y de emisiones contaminantes. Se realizará la validación de que el sistema de video analítica funcione automáticamente sin intervención manual en la detección y registro de placas, en vehículos de servicio público, servicio particular y motocicletas. Las especificaciones técnicas de las cámaras de video con video analítica son definidas en el documento "ANEXO REQUISITOS TÉCNICOS INFRAESTRUCTURA TECNOLÓGICA Y DE COMUNICACIONES".

Verificación de los registros de video el cual debe ser compatible con el sistema de intercambio de información de la Superintendencia. Como hoy no se ha definido la fecha de ingreso del sistema de la Superintendencia, el software del homologado debe ser capaz de entregar el video en mínimo los siguientes formatos: MPEG (1, 2 y 4), AVI, WINDOWS MEDIA, MXF, HD, DV, DVCPRO25;

c) Verificar la auditoría transaccional y de base de datos en este proceso.

Se revisarán los logs de eventos y los logs de bases de datos que se encuentren asegurados y gestionados.

2.6.2.2.13.2 Proceso de verificación de realización de las pruebas y expedición del certificado.

a) "Verificación de los resultados finales de la revisión que emitió cada uno de los equipos en el proceso de inspección, sin que en este proceso intervenga el Centro de Diagnóstico". El software de la RTMyEC del CDA deberá entregar de forma automática al terminar la prueba

los datos del FUR al sistema de control y Vigilancia sin que en este proceso haya intervención humana, según el estándar definido por el homologado que contrate el CDA;

b) Verificación del Director técnico y/o Jefe de Línea encargado de la realización de cada una de las pruebas realizadas al vehículo durante el proceso de inspección. Se validarán los operarios de pista a través del video y al director técnico a través de la lectura biométrica como validación del FUR, confrontándola con la base de datos del homologado. También se hará un enrolamiento inicial de todos los operarios que intervengan en el proceso. Se realizará la verificación de validación de identidad del Director Técnico y/o Jefe de Línea encargado y se deberá demostrar que una aplicación integrada con todo el sistema, realice la validación con el procedimiento alternativo temporal de validación de identidad definido;

c) Verificación de los registros de video, el cual debe ser compatible con los registros de captura, donde se tenga la función analítica para detección de placa. La aplicación de video-analítica, debe estar en operación con todas las cámaras que intervengan en el proceso de pista;

d) Verificación de coordenadas del sitio donde se realizan las inspecciones;

e) Verificación de los equipos requeridos para el funcionamiento y operación autorizados por la entidad competente se encuentren dentro de las instalaciones del CDA. El sistema de Control y Vigilancia validará el ID de la tarjeta principal, disco duro y la tarjeta de red física del servidor y/o PC del CDA que contiene la base de datos del FUR. Registro y Revisión de equipos de RTM. (censo vs. Resolución) El homologado realizará el enrolamiento de cada equipo PC de cada prueba y el servidor. MAC y ID del PC. Con respecto a los PC en cada prueba solo se considera conveniente que se controle únicamente el equipo o servidor que contenga la Base de Datos de la RTM del CDA;

f) Se debe realizar el levantamiento y registro de los seriales físicos de los equipos de inspección, guardarlos en la base de datos, para facilitar que los entes de control y acreditación realicen las debidas verificaciones;

g) Verificación de comunicaciones a través de redes privadas establecidas por el sistema de control con los Centros de Diagnóstico Automotor;

h) Verificar el registro y envío de los resultados de cada una de las pruebas efectuadas al vehículo por parte del Centro de Diagnóstico Automotor al Sistema de Control y Vigilancia, garantizando que se encuentren la totalidad de los campos establecidos en el Formato Uniforme de Resultados de Revisión Técnico Mecánica y de las Emisiones Contaminantes;

i) Verificar la auditoría transaccional y de base de datos en este proceso.

Se revisarán los logs de eventos y los logs de bases de datos que se encuentren asegurados y gestionados.

2.6.2.2.13.3 Proceso de Registro de Pago

a) Verificación del actor del sector financiero esté vigilado por la Superintendencia Financiera de Colombia;

b) Verificación que el aliado de recaudo provea cobertura Nacional. En las zonas donde están ubicados los CDA;

c) Verificación que el aliado de recaudo cuente con base de datos de todos los pagos realizados y su discriminación según el estado que se encuentre de los servicios prestados por los CDA;

d) Verificar la auditoría transaccional y de base de datos presente en este proceso;

e) El actor de recaudo debe ofrecer diversidad de medios de pago para facilitarle al usuario final (ciudadano) el pago del servicio de la RTMyEC. Estos medios de pago pueden ser, sin limitarse a ellos, datáfonos, quioscos, botones de pago en internet, tarjetas de crédito y débito, consignación bancaria.

2.6.2.2.13.4 Proceso de Cruce de Información e interconexión

a) Superintendencia de Puertos y Transporte con el actor del Sistema de recaudo;

b) Superintendencia de Puertos y Transporte con el RUNT;

c) Verificación de canales de Comunicaciones Dedicados y Sistemas Óptimos conforme a la cantidad de conexiones y el número de sitios a homologar. 3Mbps por CDA;

d) Verificar que el Sistema de Control y Vigilancia realice el cruce de información generado por cada uno de los entes involucrados (actor de recaudo, el RUNT y la Superintendencia de Puertos y Transporte);

e) Verificar la auditoría transaccional y de base de datos presente en este proceso.

Nota: Los costos asociados a la interconexión entre el RUNT y la Supertransporte no estarán a cargo de los homologados.

2.6.3 CONCLUSIONES Y RECOMENDACIONES

-- La UPTC recomienda a la Superintendencia de Puertos y Transporte, que el Sistema de Control y Vigilancia (SICOV) comience a operar a partir de que existan como mínimo dos (2) proveedores que hayan completado todos los requisitos y hayan superado el proceso de evaluación y verificación de los mismos. Y que además se demuestre que los dos proveedores tengan contratación real y no solo cumplimiento de requisitos en documentos.

-- Para entrar a operar el Sistema de Control y Vigilancia contará con cuatro (4) meses, contados a partir de que esté el segundo proveedor evaluado y verificado.

-- Queda a discrecionalidad de la Superintendencia de Puertos y Transporte.

-- La Superintendencia de Puertos y Transporte exige a los proveedores del Sistema de Control y Vigilancia (SICOV), que en cuanto al aliado u operador de recaudo, miembro del sector financiero, es preciso que los proveedores faciliten a los organismos de apoyo CDA, la integración técnica, operativa y comercial de los nuevos miembros del sector financiero presentados por los CDA, para realizar la función de recaudo. Estos nuevos miembros del sector financiero presentados por los CDA, deberán cumplir a cabalidad con el 100% de los requisitos y criterios exigidos en el presente anexo técnico.