# FICHA TÉCNICA

**"ADQUISICIÓN Y RENOVACION DE LICENCIAS DE HERRAMIENTAS TECNOLOGICAS PARA LA REALIZACIÓN DE LAS ACTIVIDADES PROPIAS DE LA DIRECCIÓN DE TRANSITO Y TRANSPORTE DE FLORIDABLANCA -DTTF."**

Conforme se establece el requerimiento técnico emitido, el futuro contratista deberá ejecutar el objeto del presente proceso bajo las siguientes especificaciones técnicas:

### 1.1. FICHA TECNICA

Para el cumplimiento del objeto del contrato, el contratista se obliga con la DIRECCIÓN DE TRÁNSITO Y TRANSPORTE DE FLORIDABLANCA a prestar el siguiente servicio:

| ITEM | TIPO | DESCRIPCION | CANTIDAD |
|---|---|---|---|
| 1 | Licencia Microsoft | Licencia Office 365 Standard. 12 Meses | 15 |
| 2 | Licencia Correo Google | Licencia Correo Google Business Starter. 12 Meses | 110 |
| 3 | Licencia Correo Google | Licencia Correo Google Business Standard. 12 Meses | 1 |
| 4 | Licencia Antivirus | Licencia Antivirus ESET PROTECT ADVANCED - CLOUD. 1 año | 50 |
| 5 | Backup o almacenamiento | AWS STORAGE S3 ESTÁNDAR CAPACIDAD 5TB, CON UNA DESCARGA MENSUAL DE 1 TB INCLUIDA. 12 meses | 1 |

## CARACTERÍSTICAS

### RENOVACION LICENCIA DE ANTIVIRUS

Tecnología y Características

- La solución deberá poder realizar exploraciones en estado inactivo para poder brindar de esa forma, una protección proactiva mientras el equipo no está en uso.
- Debe tener un caché local para aumentar el rendimiento de los entornos virtuales, garantizando que el archivo sólo se explora una vez.
- El producto debe tener un control web para limitar el acceso a los sitios web por categoría, además de poderle mostrar al usuario una notificación de bloqueo.
- El bloqueo web deberá poder asignarse por un rango de tiempo, por grupo y por equipo.
- Deberá tener la capacidad de enviar una tarea para la actualización de los parches del sistema operativo.
- Dentro del módulo de firewall deberá contar con la funcionalidad de bloqueo de exploits.
- La solución de antivirus debe ejecutar un escaneo únicamente en los siguientes estados en la computadora:
    1. Protector de pantalla activo
    2. Sesión de usuario bloqueada
    3. Sesión de usuario finalizada
- La solución debe ser capaz de permitir o negar el uso de los dispositivos en base a los siguientes criterios: Fabricante o Modelo o Número de serie.
- La solución debe ser capaz de definir un listado específico de usuarios quienes pueden hacer uso de los dispositivos. Para dispositivos de almacenamiento, la solución debe permitir configurar únicamente de los siguientes permisos: Lectura/Escritura o Bloqueo o Solo de lectura o Advertir.
- Cuando se conecta o usa un dispositivo de almacenamiento, la solución de antivirus debe proporcionar las siguientes opciones: Escanear o No realizar ninguna acción o Recordar esta acción

- Sistema de prevención de intrusiones basado en el host (HIPS) La solución debe tener sistema de prevención de intrusiones basado en el host. El sistema HIPS debe tener los siguientes modos de configuración: Modo automático o Modo inteligente o Modo interactivo o Modo basado en políticas o Modo aprendizaje.
- El aprendizaje automático avanzado o “machine learning” deberá tener cuatro umbrales: Intenso, Balanceado, Cauteloso y Desactivado.
- Debe tener una tarea para aislar a un equipo de la red.
- El HIPS debe incluir una inspección a fondo del comportamiento de todos los programas en ejecución, archivos y llaves de registro
- Debe contar con filtrado para mantener libre de SPAM a los clientes de correo.
- La solución debe capaz de verificar las comunicaciones usando protocolos SSL para hallar amenazas.
- Firewall personal, la solución de antivirus debe contar con un firewall personal.
- El firewall debe tener los siguientes modos de configuración: o Modo
- automático, Modo interactivo, o Modo basado en políticas o Modo aprendizaje
- Las reglas de firewall creadas deberán ser capaces de permitir todas las siguientes acciones: o Denegar o Permitir o Preguntar.

**DE LA CONSOLA.**

- Deberá permitir la ejecución remota de scripts, batch files y paquetes
- personalizados a través de la consola, de terceros.
- Deberá ser una solución que pueda ser usada y sea administrable desde la consola de antivirus en sistemas operativos Windows, Linux y Mac.
- Debe permitir generar grupos de clientes dinámicos y grupos estáticos.
- El fabricante debe proporcionar al menos tres diferentes formas de realizar la instalación de la consola de administración. Instalador todo en uno Instalación por componentes Aparato virtual.
- El Appliance virtual debe soportar al menos las siguientes plataformas de virtualización: VMWare vSphere o Oracle Virtual Box, o Microsoft Hyper-V o Azure - ambiente basado en la nube
- La consola de Administración deberá estar basada en Cloud.
- Activar el acceso a la consola de antivirus con doble factor de autenticación, deber estar integrada a la misma consola de antivirus, sin ningún add-on o software adicional.
- Debe contar con des instalador de antivirus de terceros.
- Debe contar con un módulo específico para la protección contra ransomware.
- Deberá tener la capacidad para aplicar durante cierto periodo de tiempo las reglas de control de dispositivo y de control de acceso web a través de la consola de administración.
- Deberá contar con etiquetas independiente al LDAP, para identificar y buscar objetos similares.
- Obtener a través de la consola de administración de seguridad del punto final inventario de aplicaciones y de hardware de cada uno de los equipos protegidos.
- A través de la misma consola de administración de seguridad de punto final debe manejar la tecnología de Sandboxing en nube para el análisis de posibles amenazas, cifrado de los discos de almacenamiento de los puntos finales e integrarse con la solución de detección y respuesta del punto final.
- A través de la consola de administración de seguridad del punto final debe ser posible administrar dispositivos móviles iOS y Android.
- Por disponibilidad de la solución de protección de punto final, la consola de administración debe tener la capacidad para construir ambientes distribuidos donde pueda asignarse roles independientes a cada componente, así tener un componente diferente para: o Administrador de equipos móviles, o Distribuidor de actualizaciones, paquetes de instalación y reenvío de comunicación entre el punto final y el servidor, o Detector de puntos finales no administrados y a su vez debe mostrar toda la información en la consola central de administración del punto final de forma nativa.
- La solución debe tener el mecanismo para desinstalar otras soluciones antivirus presentes en el equipo final. Este mecanismo debe ser y estar: o Integrado al paquete de instalación de la solución de protección de punto final. o Disponible solamente a través de la misma consola de administración de protección al punto final. Endpoint Security for Android
- La solución de antivirus debe realizar análisis a las aplicaciones instaladas, archivos. DEX.

- La solución de antivirus ofertada deberá analizar memoria interna y tarjeta SD para cualquier tipo de archivo.
- Ser capaz de mostrar un listado de las aplicaciones instaladas, controlar el tiempo del uso de aplicaciones y tener el detalle de los permisos que usan los aplicativos del dispositivo móvil.
- El análisis de la solución de protección de punto final deberá explorar hasta 3 anidados.
- La protección del dispositivo móvil debe contar con una protección en tiempo real, además de contar con un sistema de reputación de archivos.
- Deberá poder administrar las aplicaciones que deberían estar instaladas en los dispositivos móviles.
- Debe tener la capacidad para detectar de forma automática aplicaciones no deseadas y no seguras para usar en el dispositivo móvil.
- La solución debe poder enviar mensajes SMS al administrador cuando existen usuarios no autorizados manipulando el dispositivo móvil.
- La solución será capaz de proteger y seleccionar los navegadores a usar.
- La solución de antivirus deberá ser inteligente para optimizar la batería del dispositivo y ejecutar el análisis al dispositivo únicamente cuando esté completamente cargado o conectado a la energía eléctrica.
- La solución será capaz de detectar nuevas tarjetas SIM instaladas en el dispositivo y bloquearlas.
- Es importante que la solución sea capaz de generar códigos de verificación SMS temporales al administrador para ejecutar tareas de desbloqueo de dispositivos o regresar a configuración de fábrica.
- La solución será capaz de mantener un control de aplicaciones, bloquearlas según los permisos de la aplicación o por categoría, deberá limitarse a instalar aplicaciones únicamente desde Google Play, y poder bloquear cualquier
- aplicación en el momento que se necesite.
- La solución será capaz de evitar ataques de suplantación de identidad de sitios web. Server Security
- En servidores que usan “OneDrive for Business” debe explorar los archivos almacenados en esta nube, en búsqueda de algún archivo comprometido o posible malware.
- La solución de protección en servidores debe incluir la detección y bloqueo de intrusiones, agregar a lista negra aquellas direcciones que han sido identificadas con este comportamiento malicioso.
- La solución deberá agregar de forma automática las exclusiones que correspondan a aplicaciones críticas del servidor.
- Optimizar el rendimiento de infraestructuras mixtas (hardware y virtuales) siendo capaz de eliminar la duplicidad de exploraciones en archivos, excluyendo los archivos ya explorados y limpios.
- LiveGuard
- Uso de Sandboxing en la nube para analizar el comportamiento de archivos.
- Es posible crear una exclusión por ruta, detección y su hash (SHA-1).
- Capacidad de sincronizar su licenciamiento con la nube y la consola de
- administración en sitio o en la nube.
- Detectar un archivo sospechoso ejecutado por primera vez se debe mostrar una advertencia, si el análisis se completa antes de ejecutar el archivo por primera vez, no se muestra el aviso archivo en análisis.
- Debe borrar automáticamente las muestras de los archivos/ejecutables en los servidores donde fue analizado el comportamiento.
- Capacidad para enviar correos SPAM para su análisis.
- Debe tener únicamente estos umbrales de detección: desconocido, limpio, sospechoso, altamente sospechoso y malicioso.
- Debe tener la siguiente información de un archivo enviado al Sanboxing en la nube: nombre del equipo desde donde se ingresó el archivo, el usuario que lo ingresó, la razón, hash en SHA-1, nombre del archivo ingresado, tamaño del archivo, categoría.
- Debe tener protección proactiva, es decir, que el archivo/ejecutable sea bloqueado hasta recibir el resultado del Sandbox en la nube.
- Se debe tener capacidad para integrarse con la solución de antivirus o protección del punto final, para tener mayores posibilidades de protección y aplicación de políticas.
- Enviar un archivo/ejecutable a través de una consola de administración del punto final.

- ESET Liveguard permite la configuración detallada de políticas por equipo, de modo que el administrador puede controlar lo que se envía y lo que debe ocurrir en función del resultado recibido.
- Full Disk Encryption
- La solución deberá ser capaz de cifrar los Endpoints con sistemas operativos Windows y MacOS.
- La solución deberá disponer de diversas posibilidades de recuperación de Passwords para usuarios remotos que se vean bloqueados.
- La solución deberá poder programar las tareas de cifrado sobre los Endpoints deseados con la posibilidad de pausar la ejecución para retomar luego desde el último punto.
- La solución deberá poder ser administrada desde la misma consola central junto con las otras soluciones descriptas en el TDR.
- La solución de cifrado debe permitir anular la contraseña de inicio de sesión de la estación de trabajo.

**OTROS.**

- El fabricante deberá tener soporte técnico en castellano.
- Que el fabricante directamente brinde servicios de seguridad informática como por ejemplo penetration testing, vulnerability assessment o análisis de GAP. (Valor adicional al licenciamiento).
- El fabricante deberá tener la capacidad de ofrecer directamente un servicio de caza de amenazas. (Valor adicional al licenciamiento).
- El fabricante deberá tener un laboratorio de análisis y detección de malware en Latinoamérica.
- Que tenga oficinas de la marca en Latinoamérica y presencia local en el país.
- El fabricante deberá tener programas de “colaborador seguro” (Valor adicional al licenciamiento).

(S3) es un servicio de almacenamiento de objetos que ofrece escalabilidad, disponibilidad de datos, seguridad y rendimiento líderes en el sector. S3, empresas de todos los tipos y sectores pueden almacenar y proteger cualquier volumen de datos para los más variados fines, como usarlos en lagos de datos, sitios web, aplicaciones móviles, procesos de copia de seguridad y restauración, operaciones de archivado, aplicaciones empresariales, dispositivos Iot y análisis de big data. S3 proporciona características de administración fáciles de utilizar que le permiten organizar los datos y configurar sofisticados controles de acceso con objeto de satisfacer sus requisitos empresariales, organizativos y de conformidad. S3 está diseñado para ofrecer una durabilidad del 99,999999999 % (11 nueves) y almacena datos de millones de aplicaciones para empresas de todo el mundo.

Con el bloqueo de objetos de S3, se puede aplicar fechas de retención a los objetos para evitar su eliminación, así como satisfacer los requisitos de conformidad. A diferencia de las bibliotecas de cintas, con S3 Glacier la restauración de objetos archivados puede tardar desde tan solo un minuto en el caso de las recuperaciones rápidas a entre 3 y 5 horas en el caso de las recuperaciones estándar.

S3 Estándar
S3 Estándar ofrece almacenamiento de objetos de alta durabilidad, disponibilidad y rendimiento para datos a los que se obtiene acceso con frecuencia. Dada su baja latencia y alto nivel de procesamiento, el tipo S3 Estándar es apropiado para una amplia variedad de casos de uso, como aplicaciones en la nube, sitios web dinámicos, distribución de contenido, aplicaciones para dispositivos móviles, y el análisis de big data.

**DISEÑO DE LA SOLUCIÓN**

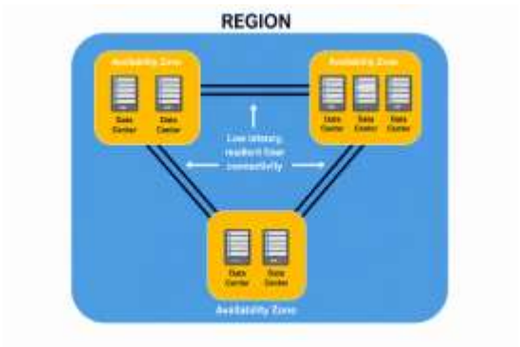
La solución se compone del servicio llamado S3 ESTÁNDAR.




El acceso a este repositorio se realizará por medio de:

- Acceso a la consola AWS
- Acceso por medio de API
- Acceso por medio del uso de un cliente compatible con S3 como WINSCP.

Disponibilidad




Todos los objetos se almacenan automáticamente en varios dispositivos distribuidos en un mínimo de tres zonas de disponibilidad independientes, cada uno separado por kilómetros en una región de AWS por lo que S3 entrega una durabilidad del servicio del 99.999999999% y una disponibilidad del 99,99%.

Se incluye bloqueo por eliminación y manejo de versiones para bloquear la posibilidad de pérdida de información por error humano.

El proponente deberá asegurar que el servicio de almacenamiento se realizará a un máximo de 10 equipos autorizados por la entidad, para automatizar el proceso.

**SEGURIDAD**

Almacene sus datos en S3 y protegerlos del acceso no autorizado con funciones de cifrado y herramientas de administración de acceso. S3 es el único servicio de almacenamiento de objetos que le permite bloquear el acceso público a todos sus objetos en el depósito o en el nivel de cuenta con S3 Block Public Access. S3 mantiene programas de cumplimiento, como PCI-DSS, HIPAA / HITECH, FedRAMP, Directiva de protección de datos de la UE y FISMA, para ayudarlo a cumplir con los requisitos reglamentarios. AWS también admite numerosas capacidades de auditoría para monitorear las solicitudes de acceso a sus recursos de S3.

**NOTA No. 1:** No se aceptan propuestas parciales, teniendo en cuenta el servicio requerido por la DTTF.

**NOTA No. 2:** El proponente debe asumir todos los costos directos e indirectos, los costos fijos, incluidos impuestos referentes a la actividad, retenciones de ley e imprevistos y utilidades.

**NOTA No. 3:** Se podrá realizar una prueba técnica para validar el cumplimiento de cada uno de los requisitos técnicos funcionales y no funcionales de la ficha técnica. Si no cumple con algún de los requisitos se podrá rechazar la oferta.

## 1.2. OBLIGACIONES DE LAS PARTES

### 1.2.1. COMPROMISOS COMUNES:

**1)** Colaborar recíprocamente para el normal desarrollo del contrato
**2)** Concurrir a la liquidación final del contrato una vez terminado su objeto.
**3)** Cumplir integra y oportunamente los compromisos específicos.

### 1.2.2. OBLIGACIONES DEL CONTRATISTA:

**OBLIGACIONES GENERALES:**

1. Cumplir cabalmente con el objeto del contrato.
2. Entregar en la Secretaría General y Jurídica los documentos de ejecución del contrato, de conformidad con los procedimientos y formatos de la Entidad.
3. Obrar con diligencia y el cuidado necesario en los asuntos que le asigne el supervisor del contrato.
4. Presentar oportunamente las respectivas facturas o cuentas de cobro.
5. Presentar los certificados de estar al día en el pago de los aportes al sistema de seguridad social integral, así como los propios del SENA, ICBF, y cajas de compensación familiar, cuando corresponda.
6. Obrar con lealtad y buena fe en las distintas etapas contractuales, evitando dilaciones y en trabamientos que puedan presentarse.
7. Todas las demás que se señalen en la Ley para este tipo de contratos o las establecidas en la invitación pública y en la oferta presentada por EL CONTRATISTA y las que se deriven de su naturaleza.
8. Obligaciones en materia de anticorrupción y transparencia
9. Acoger el principio de Transparencia que constituya una apuesta por la lucha contra la corrupción, a partir de la publicación de todas las actuaciones que se surtan durante toda la etapa contractual, así como la difusión de los incumplimientos (multas, declaratorias de incumplimiento, caducidad del contrato, imposición de cláusula penal) que se lleguen a derivar en desarrollo del contrato suscrito con la Entidad.
10. Conocer, y acatar las políticas y lineamientos de los Sistemas de Gestión adoptados por la Entidad, desde el proceso de selección, hasta la ejecución del contrato y su liquidación en caso de resultar adjudicatario**.**
11. No ofrecer, prometer, entregar, solicitar, y/o aceptar sobornos, dádivas, recompensas o gratificaciones, en cualquiera de sus etapas**.**
12. Utilizar el personal idóneo, íntegro y técnicamente capacitado para la ejecución del objeto contractual, en caso de que se evidencie y/o presente alguna conducta presuntamente delictiva y/o irregular, deberá ser retirado de manera inmediata, y presentar un informe detallado de los hechos acaecidos al Supervisor del contrato, máximo al día hábil siguiente.
13. Cumplir con todas las demás obligaciones legales respecto a seguridad industrial y salud ocupacional, ambientales y de anticorrupción que surjan con ocasión de la suscripción y ejecución del contrato.

## OBLIGACIONES EN MATERIA DE ANTICORRUPCIÓN Y TRANSPARENCIA

1. Acoger el principio de Transparencia que constituya una apuesta por la lucha contra la corrupción, a partir de la publicación de todas las actuaciones que se surtan durante toda la etapa contractual, así como la difusión de los incumplimientos (multas, declaratorias de incumplimiento, caducidad del contrato, imposición de cláusula penal) que se lleguen a derivar en desarrollo del contrato suscrito con la Entidad.
2. Conocer, y acatar las políticas y lineamientos de los Sistemas de Gestión adoptados por la Entidad, desde el proceso de selección, hasta la ejecución del contrato y su liquidación en caso de resultar adjudicatario.
3. No ofrecer, prometer, entregar, solicitar, y/o aceptar sobornos, dádivas, recompensas o gratificaciones, en cualquiera de sus etapas.
4. Utilizar el personal idóneo, íntegro y técnicamente capacitado para la ejecución del objeto contractual, en caso de que se evidencie y/o presente alguna conducta presuntamente delictiva y/o irregular, deberá ser retirado de manera inmediata, y presentar un informe detallado de los hechos acaecidos al Supervisor del contrato, máximo al día hábil siguiente.
5. Cumplir con todas las demás obligaciones legales respecto a seguridad industrial y salud ocupacional, ambientales y de anticorrupción que surjan con ocasión de la suscripción y ejecución del contrato.

## OBLIGACIONES ESPECÍFICAS

Para desarrollar el objeto del contrato y dar cumplimiento al mismo, el contratista se compromete a:

1. Cumplir a cabalidad con el objeto del contrato conforme a las normas legales que rigen la contratación estatal, las especificaciones técnicas y la propuesta presentada, la cual para todos los efectos forma parte integral del contrato.
2. Entregar a nombre de la Dirección de Tránsito los documentos y catálogos en el que conste la renovación de las licencias y la suscripción del servicio de soporte y actualización por el término de 12 meses, dentro de los cinco (05) días hábiles siguientes a la fecha de suscripción del acta de inicio.
3. Entregar un cronograma con las actividades a realizar de acuerdo con lo definido en el anexo técnico, el cual debe ser entregado después del segundo día hábil de suscrito el acta de inicio.
4. Cumplir con el objeto del contrato y atender los requerimientos que en desarrollo de este efectúe la entidad, de conformidad con lo previsto en el Anexo Técnico, los estudios previos, y demás documentos que forman parte integral del contrato.
5. Garantizar el oportuno cumplimiento y la calidad de los servicios y productos contratados, durante el tiempo de vigencia de las licencias renovadas y adquiridas con las que cuenta la entidad.
6. Atender y responder los requerimientos del supervisor del contrato, en un término máximo un (1) día hábil, contados a partir del recibo de la correspondiente solicitud escrita, durante la ejecución del contrato.
7. Informar oportunamente al supervisor del contrato sobre las dificultades que se presenten en la ejecución del mismo, así como ofrecer alternativas que permitan garantizar la buena ejecución del contrato.
8. Presentar los informes requeridos por el supervisor del contrato para el seguimiento de las obligaciones contractuales.
9. Una vez finalice el objeto del contrato, el contratista deberá entregar al supervisor del mismo, un informe consolidado de las actividades realizadas durante su ejecución.
10. Pagar de su propia cuenta los tributos a que esté obligado en virtud del contrato.
11. Adoptar las medidas correspondientes y velar para que se cumplan los requisitos y términos contractuales de acuerdo con lo establecido para tal efecto en la Ley 80 de 1993, la Ley 1150 de 2007, el Decreto 1082 de 2015 y sus respectivos decretos reglamentarios y normas concordantes.

12. Informar de inmediato y por escrito al Supervisor del Contrato la ocurrencia de situaciones de fuerza mayor o caso fortuito que puedan afectar la ejecución del contrato, incluyendo las recomendaciones que procedan según el caso.
13. Realizar la instalación y configuración de las diferentes herramientas adquiridas por la entidad, en conjunto con los funcionarios del área de Gestión Tic y Soporte de la DTTF.
14. El contratista debe estar en capacidad de brindar soporte de manera virtual y presencial, durante el tiempo de ejecución del contrato y posterior durante el tiempo activo de los servicios.
15. Cumplir con las obligaciones frente al pago de salarios, prestaciones sociales, sistema de seguridad social integral, parafiscales (Cajas de Compensación Familiar, SENA e ICBF) de conformidad con el artículo 50 de la Ley 789 del 27 de diciembre de 2002, en concordancia con la Ley 828 del 10 de julio de 2003 y demás normas aplicables, en este sentido, anexo a la factura de cobro mensual deberá allegar la Certificación expedida por el revisor Fiscal o representante legal, según corresponda, con la cual acredite el pago de sus obligaciones frente al Sistema de Seguridad Social Integral.
16. Las demás solicitadas por el supervisor del contrato y/o la oficina gestora.

### 1.2.3. OBLIGACIONES DE LA DTTF:

a) Ejercer el respectivo control en el cumplimiento del objeto del contrato.
b) Realizar el pago del contrato según la forma establecida para ello.
c) Poner a disposición del contratista la información necesaria que se requiera para el desarrollo de las actividades a ejecutar.
d) Aprobar el mecanismo de cobertura del riesgo cuando haya lugar.
e) Supervisar la ejecución técnica y financiera del presente contrato, para lo cual delegara un supervisor.
f) Los demás establecidas en el artículo 4º de la Ley 80 de 1993

### 1.3. PLAZO DE EJECUCIÓN DELCONTRATO

El plazo de ejecución del contrato será de **UN (01) MES** contado a partir de la suscripción del acta de inicio, previo cumplimiento de los requisitos legales.

**EDWIN FABIAN FONTECHA ANGULO**
Director Operativo
DTTF

Proyecto Aspectos Técnicos: **CESAR ERNESTO SAENZ ARANDA –** Ing. CPS Dirección Operativa