Clasificación del bien o servicio	43233200 Software de seguridad y protección. 81112200 Mantenimiento y soporte de software 81111800 Servicios de Sistemas y administración de componentes de sistemas
Nombre Comercial del Bien o Servicio	**RENOVACIÓN DEL LICENCIAMIENTO, SOPORTE Y MANTENIMIENTO DE LA SOLUCIÓN BROADCOM DE PROTECCIÓN ANTI-MALWARE CON CAPACIDADES XDR Y DLP IMPLEMENTADA EN LA FISCALÍA GENERAL DE LA NACIÓN.**
Calidad	Debe cumplir con todos los requisitos establecidos en la presente ficha técnica. El oferente debe ser canal autorizado por el fabricante Broadcom y estar listado en uno de los dos niveles más altos de membresía del ecosistema de canales de dicho fabricante, para lo cual debe anexar en su propuesta el o los certificados del caso, emitido por fábrica en donde se relacionen los niveles de membresía del fabricante y se evidencie la vigencia durante la ejecución del contrato y durante el soporte y garantía. El certificado debe tener fecha de expedición menor o igual a 30 días antes del cierre del presente proceso y debe ser verificable en el portal del fabricante. El contratista debe proveer el personal con certificaciones oficiales vigentes del fabricante Broadcom para la instalación, configuración y soporte requerido de la solución anti-malware provista.
Generalidades	Se requiere contratar la renovación del licenciamiento, puesta en funcionamiento, soporte, garantía, mantenimiento, administración y demás servicios asociados de la solución Broadcom actualmente implementada en la Entidad, la cual está conformada por los siguientes componentes: • Symantec Protection Engine for NAS (Protección anti-malware para almacenamiento NAS). • Symantec Endpoint Security Complete (Protección anti-malware para endpoints). • Symantec Endpoint Security Complete (Incluye el módulo de Datacenter Security exclusivamente para los servidores con sistemas legados). (Protección anti-malware para servidores). • Symantec Data Loss Prevention Core Package (DLP) (Solución de DLP - Data Loss Prevention). • Symantec Data Loss Prevention Cloud Package (XDR) (Solución de XDR - Extended Detection and Response). • Consola(s) de administración centralizada en la nube para todas las soluciones, que permiten el almacenamiento de logs y

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada

telemetría durante la vigencia contractual y todo el tiempo de soporte y garantía.
- Soporte especializado para la atención de novedades operativas y funcionales de la solución, con la asignación de un TAM (Technical Account Manager).

La renovación del licenciamiento, administración, soporte, mantenimiento y garantía de los componentes de la solución anti-malware implementada en la Entidad tendrá vigencia hasta el 31 de julio de 2027, y deberá garantizar, como mínimo, las siguientes condiciones:

- Continuidad del servicio sin degradación en el funcionamiento de la solución anti-malware.
- Preservación integral de las políticas, reglas, sandbox, telemetría, alertas e históricos existentes.
- Soporte extendido, provisto por el fabricante, para los módulos de protección anti-malware para endpoints, para servidores, para NAS, DLP y XDR.
- Acceso a la consola SaaS actualmente utilizada, manteniendo roles, tableros de control (dashboards) y configuraciones vigentes.

Asimismo, se requiere la renovación de la protección anti-malware para almacenamiento NAS de la Entidad ubicados tanto en Bogotá como en Cali. Para ello, el contratista deberá suministrar el licenciamiento, hardware y software necesario para proteger la totalidad de Teras (TB) que conforman el almacenamiento de los dos dispositivos, sin que esto genere costos adicionales para la Entidad.

El contratista deberá suministrar toda la plataforma tecnológica e infraestructura requerida para el funcionamiento completo de la solución anti-malware Broadcom implementada en la Entidad (incluyendo hardware, software, componentes, motores de análisis, servidores, appliances, instancias o recursos en la nube), sin costos adicionales para la Entidad.

En caso de requerirse infraestructura física (hardware, servidores, appliances, entre otros), esta deberá ser nueva, no usada, no remanufacturada, no repotenciada ni reacondicionada, no encontrarse en estado EOS (End of Sale / Fin de Venta), EOL (End of Life / Fin de Vida) ni EOM (End of Maintenance / Fin de Mantenimiento), y deberá contar con soporte, garantía y respaldo del fabricante o del canal autorizado, según corresponda.

Ubicación: La entrega, implementación y puesta en funcionamiento de la solución anti-malware Broadcom se debe realizar en la ciudad de Bogotá D.C., Avenida Calle 24 No.52-01, Edificio Gustavo de Greiff piso 1,

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada

<table>
<tr><td></td><td>Subdirección de Tecnologías de la Información y las Comunicaciones; y en la ciudad de Cali, Carrera 10 #12-10 y/o en las sedes que indique la Entidad.</td></tr>
<tr><td>Requisitos generales</td><td>Se requiere la renovación del licenciamiento, puesta en funcionamiento, soporte, garantía, mantenimiento, administración y servicios de la solución Broadcom implementada en la Entidad, la cual está compuesta por:

<table>
<tr><th>ITEM</th><th>DESCRIPCIÓN DETALLADA</th></tr>
<tr><td>1.</td><td>Symantec Protection Engine for NAS (Antimalware para la protección de dispositivos de almacenamiento NAS) para dos (2) dispositivos almacenamiento NAS.</td></tr>
<tr><td>2.</td><td>Symantec Endpoint Security Complete (Antimalware para EndPoint) para 26.000 Endpoint.</td></tr>
<tr><td>3.</td><td>Symantec Endpoint Security Complete (Antimalware para servidores) para 600 Servidores entre Linux y Windows. (Incluye el módulo de Datacenter Security exclusivamente para los servidores con sistemas legados).</td></tr>
<tr><td>4.</td><td>Symantec Data Loss Prevention Core Package (DLP) para 26.000 Endpoint.</td></tr>
<tr><td>5.</td><td>Symantec Data Loss Prevention Cloud Package (XDR) para 26.000 Endpoints y 600 servidores.</td></tr>
<tr><td>6.</td><td>Servicios de instalación, configuración, puesta en funcionamiento, administración, mantenimiento, soporte y garantía de los ítems No. 1, 2, 3, 4 y 5.</td></tr>
</table>

Con la renovación a contratar se debe garantizar:

• Extensión del soporte y garantía oficial del fabricante.
• Acceso a actualizaciones mayores y menores del producto.
• Mantenimiento de todas las integraciones actuales con el SIEM y el SOAR de la Entidad.
• Soporte a sistemas operativos legados ya cubiertos por la solución anti-malware vigente.

La instalación, configuración y puesta en funcionamiento de toda la solución anti-malware descrita anteriormente, junto con la totalidad de los agentes, deberá ser realizada en un máximo de dos (2) meses.

La renovación del licenciamiento, administración, soporte, mantenimiento y garantía de los componentes de la solución anti-malware implementada en la Entidad tendrá vigencia hasta el 31 de julio de 2027.</td></tr>
</table>

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada

	REQUERIMIENTOS ESPECÍFICOS
Requisitos específicos	**1. Protección NAS - Symantec Protection Engine for NAS.** La Entidad cuenta con almacenamiento marca HITACHI Modelo NAS Platform 4060, con las siguientes características: • Dos (2) soluciones de HNAS (1 en Bogotá y 1 en Cali), cada una consiste en un clúster físico con dos nodos activos y un elemento lógico EVS entregando servicio por cada nodo físico; para un total de 4 nodos físicos y 4 nodos virtuales (son los que brindan servicio a los usuarios). • Se estiman operaciones por segundo por nodo entre 5.200 y 10.200. • El tamaño efectivo total de la NAS de Bogotá es de 120 TB y el de la NAS de Cali es de 70 TB. El oferente debe: • Considerar el licenciamiento del protocolo ICAP para su Scan Engine sobre la plataforma de anti-malware implementada en la Entidad. • Dimensionar correctamente la cantidad de nodos de antivirus suficientes para poder cubrir las capacidades de la NAS. Con la renovación a contratar se debe garantizar como mínimo: **1.1** Renovar el licenciamiento de la solución Symantec Protection Engine for NAS para dos (2) dispositivos NAS ubicados en Bogotá y Cali, garantizando compatibilidad con la arquitectura actual. **1.2** Implementar la solución en un entorno con balanceo de carga y operación en modo clúster, asegurando alta disponibilidad y tiempo de respuesta promedio del servicio ICAP para los dispositivos NAS. En caso de requerirse servidores adicionales para balanceo, estos deberán ser suministrados por el contratista sin costo adicional para la Entidad. **2. Protección Endpoint - Symantec Endpoint Security Complete.** Con la renovación a contratar se debe garantizar como mínimo: **2.1** Renovar el Licenciamiento de la solución Symantec Endpoint Security Complete (Antimalware para EndPoint) para mínimo 26.000

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada

	EndPoint. **2.2** Brindar protección para los siguientes sistemas operativos: • Windows, para la versión XP en adelante. • Mac OS, para la versión Monterey en adelante. • Linux en sus diferentes distribuciones y versiones. **Nota:** La Entidad cuenta con equipos Windows XP, Windows 7, Windows 8, Windows 8.1, Windows 10, entre otros, que requiere mantener operativos por legado. En este caso, el contratista debe proveer e implementar mecanismos de protección soportados por el fabricante para estos equipos sin costo adicional para la entidad**.**
	3. Protección servidores - Symantec Endpoint Security Complete.
	Con la renovación a contratar se debe garantizar como mínimo: **3.1** Renovar el **l**icenciamiento de la solución Symantec Endpoint Security Complete (Antimalware para servidores) para mínimo 500 servidores (250 Licencias para LINUX y 250 Licencias Windows Server). **3.2** Brindar protección para los siguientes sistemas operativos: • Windows Server, para la versión 2008 en adelante. • Linux, para la versión Red Hat Enterprise Linux 6, en adelante. • Linux para la versión CentOS 6 en adelante. • Linux en sus diferentes distribuciones y versiones. **Nota:** La Entidad cuenta con equipos Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, Windows Server 2012 R2, Windows Server 2016, Windows Server 2019, entre otros, que requiere mantener operativos por legado. En este caso, el contratista debe proveer e implementar mecanismos de protección soportados por el fabricante para estos equipos sin costo adicional para la entidad.
	4. Protección DLP - Symantec Data Loss Prevention Core Package (DLP).
	Con la renovación a contratar se debe garantizar como mínimo: **4.1** Renovar el licenciamiento de la solución Symantec Data Loss Prevention Core Package (DLP) para mínimo 26.000 EndPoint.
	5. Protección XDR - Symantec Data Loss Prevention Cloud Package (XDR).

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada

Con la renovación a contratar se debe garantizar como mínimo:

5.1 Renovar el licenciamiento de la solución Symantec Data Loss Prevention Cloud Package (XDR) para mínimo 26.000 Endpoint y 500 servidores.

6. Consola de administración.

Con la renovación a contratar la consola de administración centralizada debe cumplir como mínimo con las siguientes características:

6.1 Operar en modalidad SaaS, on-premise o híbrida, utilizando un agente unificado para endpoints y servidores, con administración integrada de capacidades de protección avanzada, XDR y DLP.

6.2 Permitir la configuración de exclusiones, listas de bloqueo y listas de confianza personalizadas en todos sus módulos de protección (endpoints, servidores y almacenamiento NAS).

6.3 Garantizar la retención de logs de seguridad, telemetría y eventos correlacionados durante la vigencia contractual y todo el tiempo de soporte y garantía.

6.4 Ofrecer tableros de control por rol, con visibilidad de:

- Detecciones,
- Vulnerabilidades,
- Nivel de riesgo corporativo,
- Estado y versiones del agente,
- Enriquecimiento y correlación bajo el marco MITRE ATT&CK para eventos e incidentes.

6.5 Realizar monitoreo y alertamiento continuo de eventos de seguridad que puedan afectar endpoints, servidores y dispositivos de almacenamiento NAS.

6.6 Contar con reportes bajo demanda y programables, con exportación y alertas en formatos CSV y/o PDF (según el componente), incluyendo como mínimo:

- Top de incidentes,
- Resúmenes ejecutivos,
- Actividades de auditoría.
- Disponibilidad de las herramientas de la solución.

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada

6.7 Permitir la integración con el SIEM institucional para el envío de logs y con el SOAR institucional para la ejecución de tareas automatizadas.

6.8 Aplicar controles de protección al agente que impidan su desinstalación, modificación o eliminación no autorizada, así como la terminación de sus procesos activos.

6.9 Protegerse contra la desinstalación o desactivación no autorizada por parte de usuarios finales.

6.10 Garantizar la operación completa del servicio en los equipos de la Entidad que se encuentren fuera de la red LAN institucional, conectados únicamente a Internet.

6.11 Permitir la implementación, despliegue y gestión centralizada de reglas o políticas de protección.

6.12 Permitir la detección, inventario y visibilidad de los endpoints y servidores institucionales protegidos.

6.13 Permitir la definición y contención de archivos potencialmente maliciosos en:

- Endpoints,
- Servidores,
- Dispositivos de almacenamiento NAS.

6.14 Permitir la identificación de ataques a los que puedan estar expuestos los endpoints, servidores y dispositivos de almacenamiento NAS de la Entidad.

6.15 Proporcionar acceso en tiempo real a componentes de inteligencia artificial, motores analíticos o bases de datos del fabricante para la detección y clasificación de amenazas.

6.16 Permitir la integración con la herramienta de observabilidad institucional para el envío de logs.

7. Actualización en Línea.

Con la renovación a contratar, El contratista o fabricante debe garantizar como mínimo:

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada

7.1 Realizar la actualización en línea del software, firmas y componentes (hardware, firmware) de protección para los endpoint, los servidores, dispositivos de almacenamiento NAS, módulos XDR y DLP durante la vigencia contractual y todo el tiempo de soporte y garantía ofrecida, lo anterior sin costo para la Entidad.

7.2 Realizar la actualización de versiones de software y firmware (disponibles y estables) para las versiones instaladas, así como el acompañamiento en la estabilización de la solución, para lo cual deberá presentar un plan de actualización (ventanas, pruebas y procedimiento de reversión) a realizar en una ventana de mantenimiento a convenir con el supervisor del contrato. Lo anterior deberá contar con el conocimiento y visto bueno del comité de control de cambios de la Entidad.

7.3 Realizar la resolución de conflictos o fallas que sean generados por la solución en los endpoints, servidores y dispositivos de almacenamiento NAS, asegurando la continuidad operativa y el adecuado funcionamiento de la plataforma teniendo en cuenta los tiempos establecidos en el ítem 12.9.

8. Requerimientos de Administración

Con la renovación del servicio de administración a contratar, el contratista debe garantizar como mínimo:

8.1 Permitir definir los perfiles de administrador y perfiles de usuarios de consulta.

8.2 Generar alertas para mínimo los siguientes eventos:

- Malware detectado en los endpoint.
- Malware detectado en los servidores.
- Malware detectado en los sistemas de almacenamiento tipo NAS.
- Pérdida o fuga de información detectada en los endpoint.
- Clasificación de amenazas y ejecución de acciones de respuesta ante las amenazas.

8.3 Análisis y registro de eventos de seguridad, recursos del sistema, estadísticas de eventos y tráfico en la plataforma del contratista. El contratista gestionará el registro de requerimientos para la plataforma en la herramienta de mesa de ayuda de la Entidad.

8.4 Permitir el envío de logs a la herramienta de SIEM de la Entidad.

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada

8.5 Permitir la ejecución de tareas automatizadas enviadas por la herramienta SOAR de la Entidad.

8.6 Permitir el envío de logs a la herramienta de observabilidad de la Entidad.

8.7 Permitir la conexión con el directorio activo de la Entidad.

8.8 Realizar copias de respaldo diarias de los logs generados por la plataforma en el almacenamiento provisto en la solución, con retención por toda la vigencia contractual incluyendo el tiempo de soporte y garantía.

8.9 Realizar pruebas de restauración de las copias de respaldo de los logs generados por la plataforma.

8.10 Entregar semanalmente un (1) boletín de concienciación para los funcionarios de la Entidad con información actual relacionada con temas de cibercultura, seguridad digital, ciberseguridad, seguridad de la información de acuerdo con el contexto de la solución contratada.

8.11 Entregar un informe mensual con mínimo los siguientes indicadores:

- Equipos detectados en la consola de administración.
- Eventos detectados en los equipos monitoreados.
- Acciones tomadas por los componentes de la solución.
- Número de actualizaciones desplegadas.
- Recomendaciones.
- Disponibilidad de las herramientas de la solución.

9. Instalación y puesta en funcionamiento.

Con la renovación a contratar, el contratista deberá garantizar el correcto funcionamiento de la solución para lo cual se requiere como mínimo:

9.1 Realizar la instalación, configuración y puesta en funcionamiento de la solución con personal certificado por el fabricante.

9.2 Entregar la documentación técnica correspondiente al proceso de la instalación, configuración y despliegue de la solución.

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada

9.3 Presentar un plan de instalación que deberá ejecutarse en una ventana de mantenimiento acordada con el supervisor del contrato.

9.4 Presentar el reporte detallado de instalación una vez culminado el proceso.

9.5 Realizar el despliegue a nivel nacional de la última versión liberada por el fabricante de la solución, con el licenciamiento provisto para los equipos requeridos sin costo adicional para la Entidad.

9.6 Realizar la desinstalación total de las soluciones anti-malware distintas a la actualmente implementada de la Entidad y garantizar el correcto funcionamiento de la solución, para lo cual en caso de ser necesario deberá suministrar la infraestructura necesaria (hardware, software, licencias, entre otros) sin costo adicional para la Entidad.

9.7 Realizar la instalación de los componentes de la solución anti-malware, de la solución DLP y de la solución XDR adquiridos, de manera remota o presencial en la sede que se requiera sin costo adicional para la Entidad. Esta puede llevarse a cabo mediante el mecanismo o herramienta que el contratista considere más adecuado, dentro del tiempo establecido, sin afectar el funcionamiento o el servicio de la Entidad, y sin generar costo adicional para la entidad.

9.8 En caso de requerirse, el contratista deberá identificar mediante marquillas la parte frontal de los equipos instalados, de manera que sean claramente visibles para su gestión en el centro de datos de la Entidad.

10. Implementación.

Con la renovación a contratar, el contratista debe garantizar como mínimo:

10.1 Realizar el despliegue de la solución a nivel nacional de forma centralizada y que los equipos reporten a una o varias consolas en modalidad SAAS, on-premise o híbrida.

10.1.1 En caso de que el contratista requiera de hardware, licencias o componentes adicionales para garantizar el correcto funcionamiento de la solución provista, debe suministrar tanto el hardware, las licencias y los componentes necesarios para la instalación y uso de las licencias requeridas, de manera que se garantice el funcionamiento de la

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada

	solución, plataforma de administración, control, monitoreo, equipos de usuario y en general de la plataforma e infraestructura de uso de la Entidad. Esto sin costo adicional para la Entidad. **10.2** Suministrar un esquema de alta disponibilidad que garantice la continuidad del servicio sin interrupciones ante fallas de hardware, software o conectividad. **10.3** Realizar el despliegue e implementación de los componentes de la solución a nivel nacional en un tiempo no mayor a dos (2) meses para la totalidad de la solución ofertada. **10.4** Realizar la desinstalación de las soluciones anti-malware distintas a la actualmente implementada de la Entidad en un tiempo no mayor a un (1) mes, sin costo adicional para la Entidad. **10.5** Realizar la configuración de los servidores provistos por el contratista para la correcta operación de la solución. **10.6** Realizar la configuración de los componentes antimalware en la(s) plataforma(s) de administración provista(s) por el oferente, ya sea en modalidad SaaS, on-premise o híbrida, para realizar los escaneos correspondientes. Las plataformas deberán garantizar la funcionalidad requerida, independientemente de si se trata de una o varias consolas, siempre que se asegure una gestión centralizada, eficiente e integrada. **10.7** Coordinar las actividades de la implementación, soporte, garantía y acompañamiento requerido en las Características Mínimas Técnicas exigidas. **10.8** Realizar la implementación o migración de reglas, directivas, indicadores de compromiso IOC´s o políticas de protección existentes en la solución actual. **10.9** Cubrir todos los costos de implementación y funcionamiento durante el término del contrato, del soporte y de la garantía sin costo adicional para la Entidad. **10.10** Suministrar el almacenamiento para ambientes virtuales de la solución y el registro de logs por la vigencia del contrato, del soporte y de la garantía. **10.11** Las licencias se deben entregar mediante correo electrónico al correo licencias.tics@fiscalia.gov.co, con copia al supervisor del

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada

contrato; donde esté el nombre de la empresa que las suministra y el número del contrato. Estas deben ser a nombre de la FISCALÍA GENERAL DE LA NACIÓN para su uso.

11. Mantenimiento.

Con la renovación del servicio de mantenimiento de los componentes de la solución a contratar, el contratista debe garantizar como mínimo:

11.1 Realizar cuatro (4) mantenimientos preventivos al año, uno (1) en el primer trimestre, uno (1) en el segundo trimestre, uno (1) en el tercer trimestre, uno (1) en el cuarto trimestre y los mantenimientos correctivos que sean necesarios para garantizar el correcto funcionamiento de la solución.

11.2 Realizar los mantenimientos correctivos cuando se presenten incidentes de funcionamiento de la solución anti-malware implementada en la Entidad que afecten disponibilidad, rendimiento, integridad de políticas, actualización de firmas o funcionamiento del agente.

11.3 Presentar con cada visita técnica al supervisor del contrato, un informe detallado que incluya como mínimo:

- Diagnóstico del problema.
- Recomendación y/o acción a ejecutar, cada vez que se presenten fallas en la solución contratada en el presente proceso.

11.4 Registrar las novedades de servicio presentadas para cada equipo en formato de hoja de vida de los bienes (entregado por la Entidad) y generar un informe técnico al supervisor del contrato, cada vez que sea solicitado, debidamente firmado por el funcionario y por el técnico, donde se registren datos del equipo, el estado en que se encontró, el estado de funcionamiento después del cambio o instalación de los componentes, mantenimiento (instalación del repuesto), soporte y las observaciones a que haya lugar.

11.5 El contratista o fabricante deberá definir y ejecutar los mantenimientos correctivos que lleguen a requerirse.

11.6 Presentar al supervisor la garantía de hardware y software ofrecido directamente con el fabricante.

12. Soporte.

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada

Con la renovación del servicio de soporte de los componentes de la solución a contratar, el contratista debe garantizar como mínimo:

12.1 Prestar directamente o a través del fabricante, el servicio de soporte de todos los componentes que conforman la solución anti-malware objeto del contrato, garantizando su adecuada operación, disponibilidad y continuidad del servicio.

12.2 Disponer, hasta el 31 de julio de 2027, de un recurso de soporte en sitio en la sede Bunker de Bogotá, en modalidad 5x8, para la gestión y respuesta ante incidentes, y garantizar adicionalmente la disponibilidad del servicio en esquema 7x24x365 mediante personal certificado por el fabricante y los mecanismos de soporte y escalamiento necesarios, dicho recurso deberá cumplir con los siguientes requerimientos:

- Tecnólogo o Ingeniero (electrónico, sistemas, mecatrónica, electromecánico o afines).
- Experiencia mínima de dos (2) años en administración de plataformas anti-malware.
- Certificación vigente del fabricante en la solución de anti-malware y XDR ofrecida.

NOTA: Las certificaciones y hoja de vida del recurso deben ser entregadas al supervisor del contrato una vez suscrito el contrato.

12.3 En caso de requerir soporte en las diferentes sedes a nivel nacional, este se realizará de forma remota en coordinación con el personal de Mesa de Servicios de la Entidad.

12.4 Realizar las visitas en sitio para la atención, diagnóstico y solución de fallas cuando así se requiera, utilizando personal calificado y certificado por el fabricante, sin generar costos adicionales para la Entidad.

12.5 Atender, gestionar y resolver los incidentes que afecten el funcionamiento de la solución antimalware implementada en la Entidad, incluyendo fallas técnicas, daños, degradaciones de desempeño y cualquier anomalía operativa.

12.6 Realizar los cambios, configuraciones y ajustes que sean solicitados por la Entidad. Lo anterior deberá contar con el conocimiento y visto bueno del comité de control de cambios de la Entidad.

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada

12.7 Atender en sitio los incidentes de seguridad digital y ciberseguridad relacionados con ataques de malware que afecten los componentes de la solución.

12.8 Suministrar, reemplazar o proveer sin costo adicional para la Entidad los repuestos o componentes que se requieran para asegurar la operación normal de la solución.

12.9 El contratista o fabricante deben prestar el soporte y mantenimientos correctivos de ser requeridos cumpliendo como mínimo con los siguientes tiempos:

- Tiempo Máximo de Respuesta a Solicitudes: Se debe dar atención a las solicitudes en las ciudades donde se instalará la solución en máximo treinta (30) minutos, de manera presencial o remota.
- Tiempo Máximo de Diagnóstico: Se debe dar diagnóstico a las solicitudes efectuadas en un tiempo no mayor a cuatro (4) horas posteriores al reporte.
- Tiempo Máximo de Solución: Se debe presentar un plan de solución al supervisor del contrato y establecer un tiempo de solución no mayor a veinticuatro (24) horas, en caso de requerirse mayor tiempo, deberá ser documentado y justificado mediante reporte o informe ante el supervisor del contrato. Para la ejecución de la solución deberá cumplir con los procedimientos establecidos por la Entidad.

12.10 Presentar con cada visita técnica al supervisor del contrato un informe detallado que incluya como mínimo:

- Diagnóstico del problema.
- Recomendaciones y acciones ejecutadas o a ejecutar.

12.11 El contratista o fabricante deberán registrar todos los casos de soporte, realizar el seguimiento necesario y mantener actualizados los estados de los casos abiertos o escalados por la Entidad.

12.12 Registrar el análisis de eventos de seguridad de la información en la herramienta de gestión de casos de Mesa de Servicios de la Entidad.

12.13 Suministrar soporte especializado, priorización en la atención y revisiones periódicas orientadas al buen funcionamiento de la solución.

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada

12.14 Asignar un Technical Account Manager (TAM), quien será responsable del acompañamiento técnico, la gestión proactiva y el seguimiento integral de la operación.

12.15 El fabricante deberá realizar dos (2) revisiones presenciales anuales de buenas prácticas y configuraciones de la solución, entregando al supervisor un informe con recomendaciones y plan de mejoras.

12.16 Garantizar soporte técnico presencial cuando sea requerido por la Entidad, asegurando la continuidad y disponibilidad del servicio, sin generar costos adicionales.

12.17 Prestar asistencia técnica vía telefónica o por medio de acceso remoto o en sitio a solicitud de la Entidad.

13. Garantía.

Con la renovación de la garantía de los componentes de la solución a contratar, el contratista debe garantizar como mínimo:

13.1 Incluir cambio de partes, repuestos o equipos necesarios para el normal funcionamiento de la solución, sin costo adicional para la Entidad.

13.2 Suministrar los componentes de hardware, software o licencias adicionales para asegurar el correcto funcionamiento de la solución, e integrarlos durante la instalación, configuración y puesta en funcionamiento de la solución, sin costo adicional para la Entidad.

13.3 En caso de requerirse el reemplazo de partes o el suministro de repuestos, estos deberán ser nuevos y ser provistos directamente por el contratista o por el fabricante, sin costo adicional para la Entidad.

13.4 En caso de que una falla impida la operación normal de la solución y su corrección exceda las cuarenta y ocho (48) horas, el Contratista deberá suministrar temporalmente los elementos, partes o equipos necesarios para garantizar la continuidad operativa de la solución contratada. La implementación de dichos elementos deberá contar con el conocimiento y visto bueno del Comité de Control de Cambios de la Entidad.

14. Otros Requerimientos.

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada

Con la renovación a contratar, el contratista debe garantizar como mínimo:

14.1 La solución soporte los protocolos de direccionamiento IPv4 e IPv6, conforme a los estándares aplicables del fabricante.

14.2 La solución maneje protocolos de comunicación seguros incluyendo SSL, TLS y otros mecanismos criptográficos equivalentes o superiores que garanticen la integridad y confidencialidad de la información intercambiada.

14.3 Suministrar e implementar la última versión estable liberada por el fabricante al momento de la instalación, configuración y puesta en funcionamiento de la solución, incluyendo todas las actualizaciones necesarias para su operación óptima.

14.4 Definir y suministrar el canal de comunicación al supervisor del contrato durante la ejecución y durante la vigencia de la solución.

14.5 Entregar a la Entidad la documentación completa de la implementación de la solución, que como mínimo deberá incluir:

- Cantidad total de dispositivos detectados.
- Características de instalación y configuración aplicada.
- Arquitectura de la solución implementada.

14.6 Entregar al supervisor el manual de implementación, documentación técnica oficial del fabricante, configuración final aplicada a la solución y los lineamientos de operación y administración de la solución.

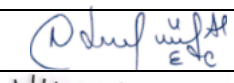
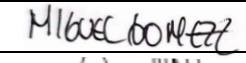
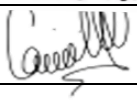
14.7 Entregar al supervisor del contrato los logs generados y almacenados durante toda la vigencia contractual, en formatos CSV, PDF, y cuando aplique, JSON, conforme lo requiera la Entidad.

14.8 Garantizar la prestación del servicio contratado en las sedes que determine la Entidad. Para tal efecto, el Contratista deberá asumir, sin costo adicional para la Entidad, el traslado, la reinstalación, la configuración y la puesta en operación de todos los componentes de la solución en la sede que esta disponga.

14.9 A solicitud de la Entidad, el Contratista deberá realizar la desinstalación total de las soluciones antimalware implementadas en la

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada

	Entidad, en un plazo máximo de un (1) mes contado a partir de la recepción del requerimiento, sin que ello genere costo adicional alguno para la Entidad.
Empaque y rotulado	N/A
Presentación y Unidad de Medida	Licencias por número de unidades.

Elaboró	Nelson Javier Castelblanco	02/07/2026	
	Miguel Ángel Gómez Cuan	02/07/2026	
Aprobó	Giselle Viviana Muñeton Lara	02/07/2026	

Este documento es copia del original que reposa en la Intranet. Su impresión o descarga se considera una Copia No Controlada