COTIZACIÓN 082-26
AREA METROPOLITANA DE BUCARAMANGA
29 DE SEPTIEMBRE DE 2026

	SONICWALL ENDPOINT SECURITY MDR y Capture client MDR, Licencimiento por un año, Gestionada por el SOC de Sonicwall.		**PESOS VENTA**		
Item	**Descripción**	**Cant.**	**V. unitario**	**Valor Total**	**Tiempo de Entrega máximo**
1	SONICWALL MDR FOR ENDPOINT SECURITY MANAGED BY SONICSENTRY PER ENDPOINT 1YR **(excluida de IVA)**	72	$124.170	$8.940.223	5 DIAS
2	SONICWALL 24/7 MDR + CAPTURE CLIENT PREMIER MSSP POWERED+ TIER PER ENDPOINT 1 MO (para servidores) **(excluida de IVA)**	2	$286.342	$572.684	10 DIAS
3	Servicio de instalación y configuración (se instala , configura y parametriza en los 74 equipos.	1	$1.105.500	$1.105.500	4 dias
4	Capacitación en el manejo de la consola a uno o dos funcionarios (4 horas) y Capacitación virtual a los funcionarios /contratistas en temas de seguridad informática (2 horas)	1	$442.200	$442.200	1 DIA
5	Asistir con soporte y acompañamiento durante la vigencia de la licencia (1 año) en administración de la consola, gestión de usuario, gestión de agentes, gestión ante un ataque, soporte en general . La gestión de consola y operación la hace Sonicwall desde su SOC, y la atención local la ofrecer SYSTEL	1	$3.449.160	$3.449.160	
	SUBTOTAL			**$ 14.509.766**	
	IVA (19%)			**$ 949.403**	
	TOTAL INCLUIDO IVA			**$ 15.459.170**	

Condiciones de pago: 100% a la entrega a satisfacción de los elementos de la propuesta , maximo a los veinte dias de presentación

Validez de la oferta: 10 días

Cualquier inquietud con gusto la atenderemos.

Cordialmente,

HECTOR GIL TRIANA
GERENTE
SYSTEL INFORMATICOS SAS
Nit: 901297797-4

CRA 33 # 91-52 TORRE 2-1407 EDIFICIO MONVISO
Telefax: 6511164
coordinador.comercial@systelinformaticos.com.co
Bucaramanga - Colombia

ROYAL TECH GROUP

ROYAL TECH GROUP SAS
Carrera 22C No. 68 - 65
Barranquilla, Atlántico
Colombia 080012
NIT: 901.394.655-2

Para
ÁREA METROPOLITANA DE BUCARAMANGA
NIT: 890.210.581-8
Calle 89 Transversal Oriental Metropolitana - 69
Centro de Convenciones Neomundo, Piso 3
Bucaramanga, Santander - Colombia
(607) 689 8080

PRO-000136

ACRONIS - SOLUCIÓN DE ANTIVIRUS CON CONSOLA EN LA NUBE GESTIONADA POR EL SOC DEL FABRICANTE

Fecha: 23-09-2026
Válida hasta: 23-12-2026

#	Artículo	Cantidad	Valor Unitario	Descuento%	IVA	Valor Total
1	**Acronis Cyber Protect Cloud - Endpoint Security + Extended Detection and Response (XDR) con In-house MDR Advanced** SKU: ACRONIS-CPC-XDR-MDR Duración del Servicio: 01 Año (P1Y Annual) Unidad de medida: Licencia por equipo Workloads: Servers, VMs, Workstations, Hosting Servers Consola de administración unificada en la nube, con capacidad de administrar un número ilimitado de equipos Incluye el servicio de detección y respuesta administrada en nivel Advanced, operado por el Centro de Operaciones de Seguridad del fabricante con cobertura 24x7x365 El valor incluye la desinstalación del antivirus vigente, la instalación y configuración en sitio de las licencias, la parametrización de la consola, las capacitaciones y el soporte durante toda la vigencia, sin costo adicional para la Entidad	74	$280.108,00	0%	0%	$20.727.992,00

Total neto	**$20.727.992,00**
Total	**$20.727.992,00**

Valor total de la oferta: **VEINTE MILLONES SETECIENTOS VEINTISIETE MIL NOVECIENTOS NOVENTA Y DOS PESOS M/CTE ($20.727.992,00)**

OBLIGACIONES Y SERVICIOS INCLUIDOS

- El valor ofertado comprende el licenciamiento y la totalidad de los servicios asociados: instalación en sitio, configuración, puesta en funcionamiento, capacitaciones y soporte durante la vigencia del contrato, sin costos adicionales para la Entidad.
- Adquisición, configuración y puesta en funcionamiento de una solución de antivirus con consola en la nube, gestionada por el SOC del fabricante, para setenta y cuatro (74) equipos de la Entidad, con vigencia de un (1) año.
- Activación y configuración de la consola en la nube, con parametrización de los productos conforme a las políticas que defina la Entidad.
- Desinstalación, en la totalidad de los equipos de cómputo, del antivirus adquirido anteriormente por la Entidad.
- Instalación y configuración en sitio de las setenta y cuatro (74) licencias sobre los equipos que indique el supervisor del contrato, en Windows 11 Pro, Windows 10 Pro, Windows Server 2016 Standard con rol Hyper-V y Windows Server 2019 Standard con rol Hyper-V.
- Capacitación al personal de apoyo tecnológico en el uso de las consolas de administración, con una duración mínima de cuatro (4) horas, previa concertación con el supervisor.
- Capacitación en seguridad informática dirigida a funcionarios y contratistas de la Entidad, con registro de asistencia.
- Soporte técnico remoto proactivo durante toda la vigencia de la licencia, con tiempo de atención máximo de cuatro (4) horas después de la solicitud, que comprende reconfiguración y administración de la consola, conexión y actualización de agentes, y limpieza de virus.
- Acompañamiento de soporte de primer nivel durante la vigencia de la licencia: nuevas versiones liberadas en consola y agentes, actualización de bases de datos, conectividad con la consola y actualizaciones.
- Los valores cotizados incluyen todas las estampillas, tasas, impuestos y demás gravámenes aplicables en Colombia, así como todos los costos directos e indirectos que se causen.

CUMPLIMIENTO DE LAS ESPECIFICACIONES TÉCNICAS MÍNIMAS

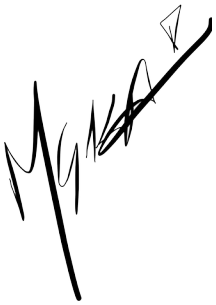
Ítem	Requerimiento de la ficha técnica	Cumplimiento de la solución ofertada
1	**Consola de administración unificada en la nube, accesible por navegador web, con capacidad de administrar un número ilimitado de equipos**	Cumple. Consola web multi-tenant, sin requerimiento de infraestructura local, con acceso seguro y doble factor de autenticación.
2	**Antimalware basado en firmas, análisis heurístico y análisis basado en comportamiento**	Cumple. Motor de protección con detección estática, heurística y comportamental.
3	**Protección contra malware avanzado, ransomware y exploits**	Cumple. Protección antimalware y antiransomware basada en inteligencia artificial, con prevención de exploits.
4	**Detección de amenazas de día cero y análisis en tiempo real**	Cumple. Detección de amenazas de día cero con análisis en tiempo real y protección multicapa.
5	**Control de dispositivos, de aplicaciones y de ejecución de archivos**	Cumple. Control de dispositivos y de puertos, control de aplicaciones y listas de aplicaciones permitidas ajustables por perfil.
6	**Protección frente a técnicas de evasión y amenazas fileless, con inspección de memoria**	Cumple. Inspección de memoria y detección de código malicioso y amenazas sin archivo.
7	**Sandboxing en la nube para análisis dinámico de archivos sospechosos, con veredicto antes o durante la ejecución**	Cumple. Análisis dinámico en entorno aislado en la nube del fabricante, con emisión de veredicto sobre el archivo.
8	**Capacidades EDR nativas: telemetría, correlación de eventos, storyline del ataque e investigación de incidentes**	Cumple. EDR nativo con registro de telemetría, correlación automatizada de eventos y construcción de la línea temporal del incidente.
9	**Threat hunting, investigación histórica e identificación de procesos, archivos y conexiones relacionadas**	Cumple. Búsqueda inteligente de indicadores de compromiso sobre la telemetría recolectada, con investigación histórica.

Ítem	Requerimiento de la ficha técnica	Cumplimiento de la solución ofertada
10	**Correlación con el marco MITRE ATT&CK**	Cumple. Visualización e interpretación automatizada de la cadena de ataque con el marco MITRE ATT&CK.
11	**Aislamiento o contención de endpoints comprometidos y acciones de respuesta y remediación**	Cumple. Respuesta con un solo clic, cuarentena y aislamiento del equipo, y remediación incluida la reimagen completa.
12	**Alertas priorizadas según criticidad**	Cumple. Priorización automática de actividades sospechosas y resúmenes de incidentes generados por inteligencia artificial.
13	**Servicio MDR operado por un SOC especializado del fabricante, con cobertura 24x7x365**	Cumple. Se oferta el nivel Advanced: monitoreo y mitigación automatizada 24x7, respuesta automatizada con aislamiento, mitigación y respuesta manual en incidentes críticos, acciones completas de remediación y recuperación, threat hunting, inteligencia de amenazas e indicadores de compromiso, análisis de causa raíz con informe de incidentes, investigación bajo demanda, solicitudes ad hoc, portal de servicio y reporte mensual avanzado.
14	**Soporte de los sistemas operativos utilizados por la Entidad**	Cumple. Compatibilidad con Windows 11 de 64 bits, Windows 10 de 64 bits, Windows Server 2016 Standard y Windows Server 2019 Standard con rol Hyper-V.

ALCANCE DETALLADO POR ACTIVIDAD

1. Dossier de entrega

- Certificado de licenciamiento expedido por el fabricante y dirigido al Área Metropolitana de Bucaramanga.
- Certificado de soporte y garantía por doce (12) meses, expedido por Royal Tech Group SAS, por la instalación, la configuración y el funcionamiento de la solución.
- Fichas técnicas del sistema y de los productos que componen la solución.
- Datos de contacto para la atención postventa.
- Registro de transferencia de conocimiento al personal de apoyo tecnológico de la Entidad.
- Registro de capacitación a funcionarios y contratistas en temas de seguridad informática.
- Documento físico o digital que acredita el derecho de uso de las licencias a nombre de la Entidad.



Kevin Muñoz Guerra
Gerente de Cuentas – Sector Gobierno
Cel. 315 548 2662
kevin.munoz@royaltech.group
Barranquilla – Colombia

NOTAS Y CONDICIONES

- Los valores cotizados incluyen todas las estampillas, tasas, impuestos y demás gravámenes aplicables en Colombia (nacionales, departamentales y municipales), así como todos los costos directos e indirectos que se causen.

- La vigencia de esta propuesta es de 03 meses.
- El plazo de entrega y pago es de acuerdo a lo definido por la Entidad.
- La vigencia del licenciamiento es de un (1) año contado a partir de su activación.
- Información bancaria para pagos: Cuenta de Ahorros Bancolombia No. 08100000653.
- Las licencias se suministran como proveedor autorizado en la categoría Gold de Acronis y serán originales, nuevas, oficiales y vigentes. Se adjunta certificación de distribuidor autorizado expedida por el fabricante a nombre de la Entidad.
- Territorialidad del ICA: Bucaramanga, Santander, municipio donde se suscribe y ejecuta el contrato.
- Productos excluidos de IVA según numeral 21, Art. 476 del Estatuto Tributario.
- En cumplimiento de las pólizas expedidas para garantizar la calidad del servicio, estamos obligados a brindar soporte técnico preventivo, proactivo y reactivo a la Entidad de conformidad con los SLAs establecidos.

Fecha de preparación: 30-09-2026 · Moneda COP

AMB · SOLUCIÓN DE ANTIVIRUS

Para

ÁREA METROPOLITANA DE BUCARAMANGA
NIT 890.210.581-8
Calle 89 Transversal Oriental Metropolitana - 69
Centro de Convenciones Neomundo, Piso 3
Bucaramanga, Santander · (607) 689 8080

Referencia

ACRONIS · XDR + MDR ADVANCED
74 equipos · 12 meses
Consola en la nube · SOC del fabricante

Acronis Cyber Protect Cloud

Endpoint Security + Extended Detection and Response (XDR) con In-house MDR Advanced

SKU: ACRONIS-CPC-XDR-MDR · Unidad: licencia por equipo
Duración: un (1) año (P1Y Annual)

Workloads: Servers, VMs, Workstations y Hosting Servers. Consola unificada en la nube con capacidad de administrar un número ilimitado de equipos.

Servicio de detección y respuesta administrada Advanced, operado por el SOC del fabricante con cobertura 24x7x365.

Incluye desinstalación del antivirus vigente, instalación y configuración en sitio, parametrización de la consola, capacitaciones y soporte durante toda la vigencia, sin costo adicional para la Entidad.

74 × $290.052,00 · IVA 0 %

Subtotal	**$21.463.848,00**
IVA 0 %	**$0,00**
TOTAL COP	**$21.463.848,00**

Vigencia del licenciamiento: un (1) año contado desde su activación. Los valores incluyen los costos directos e indirectos, estampillas, tasas, impuestos y demás gravámenes aplicables contemplados en el alcance.

SERVICIOS Y ENTREGABLES INCLUIDOS

• El valor ofertado comprende el licenciamiento y la totalidad de los servicios asociados: instalación en sitio, configuración, puesta en funcionamiento, capacitaciones y soporte durante la vigencia del contrato, sin costos adicionales para la Entidad.

• Adquisición, configuración y puesta en funcionamiento de una solución de antivirus con consola en la nube, gestionada por el SOC del fabricante, para setenta y cuatro (74) equipos de la Entidad, con vigencia de un (1) año.

• Activación y configuración de la consola en la nube, con parametrización de los productos conforme a las políticas que defina la Entidad.

• Desinstalación, en la totalidad de los equipos de cómputo, del antivirus adquirido anteriormente por la Entidad.

• Instalación y configuración en sitio de las setenta y cuatro (74) licencias sobre los equipos que indique el supervisor del contrato, en Windows 11 Pro, Windows 10 Pro, Windows Server 2016 Standard con rol Hyper-V y Windows Server 2019 Standard con rol Hyper-V.

• Capacitación al personal de apoyo tecnológico en el uso de las consolas de administración, con una duración mínima de cuatro (4) horas, previa concertación con el supervisor.

• Capacitación en seguridad informática dirigida a funcionarios y contratistas de la Entidad, con registro de asistencia.

• Soporte técnico remoto proactivo durante toda la vigencia de la licencia, con tiempo de atención máximo de cuatro (4) horas después de la solicitud, que comprende reconfiguración y administración de la consola, conexión y actualización de agentes, y limpieza de virus.

• Acompañamiento de soporte de primer nivel durante la vigencia de la licencia: nuevas versiones liberadas en consola y agentes, actualización de bases de datos, conectividad con la consola y actualizaciones.

• Los valores cotizados incluyen todas las estampillas, tasas, impuestos y demás gravámenes aplicables en Colombia, así como todos los costos directos e indirectos que se causen.

Dossier de entrega

• Certificado de licenciamiento expedido por el fabricante, dirigido al Área Metropolitana de Bucaramanga, y documento físico o digital que acredita el derecho de uso a nombre de la Entidad.

• Certificado de soporte y garantía por doce (12) meses por la instalación, configuración y funcionamiento de la solución.

• Fichas técnicas del sistema y de los productos que componen la solución; información de operación y mantenimiento.

• Datos de contacto para la atención postventa.

• Registros de transferencia de conocimiento al personal de apoyo tecnológico y de capacitación a funcionarios y contratistas en seguridad informática.

ESPECIFICACIONES TÉCNICAS DE LA SOLUCIÓN

Característica	Alcance ofertado
1. Consola en la nube	Consola web multi-tenant, sin infraestructura local; administración ilimitada de equipos, acceso seguro y doble factor de autenticación.
2. Antimalware	Detección basada en firmas, análisis estático, heurístico y comportamental.
3. Protección avanzada	Protección antimalware y antiransomware basada en inteligencia artificial, con prevención de exploits.
4. Amenazas de día cero	Análisis en tiempo real y protección multicapa.
5. Control	Control de dispositivos y puertos, aplicaciones, ejecución de archivos y listas de aplicaciones permitidas ajustables por perfil.
6. Evasión y fileless	Inspección de memoria y detección de código malicioso y amenazas sin archivo.
7. Sandboxing	Análisis dinámico en entorno aislado en la nube del fabricante, con veredicto antes o durante la ejecución.
8. EDR nativo	Telemetría, correlación automatizada de eventos, storyline e investigación de incidentes.
9. Threat hunting	Búsqueda de indicadores de compromiso en la telemetría, investigación histórica e identificación de procesos, archivos y conexiones.
10. MITRE ATT&CK	Visualización e interpretación automatizada de la cadena de ataque con el marco MITRE ATT&CK.
11. Respuesta y remediación	Cuarentena, aislamiento del equipo y respuesta con un clic; remediación incluida la reimagen completa.
12. Alertas	Priorización de actividades sospechosas según criticidad y resúmenes de incidentes generados por inteligencia artificial.
13. MDR Advanced · SOC 24x7x365	Monitoreo y mitigación automatizada; aislamiento, mitigación y respuesta manual en incidentes críticos; remediación y recuperación completas; threat hunting, inteligencia de amenazas e indicadores de compromiso; análisis de causa raíz e informe de incidentes; investigación bajo demanda, solicitudes ad hoc, portal de servicio y reporte mensual avanzado.
14. Compatibilidad	Windows 11 y Windows 10 de 64 bits; Windows Server 2016 Standard y Windows Server 2019 Standard con rol Hyper-V.

ANEXO · REQUERIMIENTOS DE LA ENTIDAD

Ficha técnica y obligaciones del proceso: se conserva el alcance requerido para la adquisición, configuración y puesta en funcionamiento de la solución.

1. Alcance

1. El alcance del objeto del contrato consiste en la adquisición de licencias antivirus con EDR, para atender las diferentes dependencias de la entidad conforme a las especificaciones técnicas mínimas y condiciones descritas a continuación:

NECESIDAD Solución de antivirus, con consola en la nube, Gestionada por el SOC del fabricante Cantidad de licencias requeridas: 74 Vigencia de la licencia: UN (01) AÑO

CARACTERÍSTICAS DEL ANTIVIRUS

• La solución debe disponer una consola de administración unificada que se administre en la nube (Consola WEB) con capacidad de administrar un número ilimitado de equipos.

• Antimalware basado en firmas.

• Análisis heurístico.

• Análisis basado en comportamiento.

• Protección contra malware avanzado.

• Protección contra ransomware.

• Protección contra exploits.

• Detección de amenazas de día cero.

• Análisis en tiempo real.

• Protección multicapa.

• Control de dispositivos.

• Control de aplicaciones.

• Control de ejecución de archivos.

• Protección frente a técnicas de evasión.

• Sandboxing en la nube para análisis dinámico de archivos sospechosos, con capacidad de ejecución controlada y generación de veredicto antes o durante la ejecución en el endpoint.

• Integrar mecanismos de detección estática, heurística y comportamental, permitiendo identificar amenazas independientemente de que exista o no una firma conocida.

• Contar con mecanismos avanzados de inspección de memoria capaces de detectar código malicioso, ataques de día cero y amenazas fileless que intenten evadir los mecanismos tradicionales de detección basados en archivos o firmas

• Disponer de una consola de administración centralizada, basada en nube, accesible mediante navegador web, desde la cual sea posible administrar políticas, agentes, eventos, alertas, incidentes, dispositivos y reportes.

• Proporcionar información sobre el estado de seguridad del endpoint y permitir identificar condiciones que puedan facilitar la ejecución o persistencia de amenazas.

EDR con capacidades de correlación de eventos, storyline, threat hunting, investigación de incidentes y mapeo de técnicas de ataque.

• Incorporar capacidades EDR nativas.

• Registrar telemetría de los endpoints.

• Correlacionar eventos relacionados con un mismo incidente.

- Construir una línea temporal o storyline del ataque.
- Permitir investigación de incidentes.
- Identificar procesos, archivos, conexiones y actividades relacionadas.
- Permitir búsqueda de amenazas sobre la telemetría recolectada.
- Permitir threat hunting.
- Permitir investigación histórica.
- Permitir identificar técnicas y tácticas utilizadas por el atacante.
- Permitir correlación con MITRE ATT&CK.
- Permitir aislamiento o contención de endpoints comprometidos.
- Permitir acciones de respuesta y remediación.
- Generar alertas priorizadas según criticidad.

Incluir un servicio de detección y respuesta administrada (MDR), operado por un Centro de Operaciones de Seguridad (SOC) especializado, con cobertura 24x7x365, que contemple:

- Monitoreo 24x7x365.
- Análisis continuo de alertas.
- Threat hunting.
- Investigación de incidentes.
- Triage de alertas.
- Correlación de eventos.
- Análisis de comportamiento.
- Identificación de falsos positivos.
- Priorización de incidentes.
- Recomendaciones de contención.
- Respuesta ante incidentes.
- Remediación.
- Escalamiento de incidentes críticos.
- Notificación al personal autorizado.
- Seguimiento hasta cierre del incidente.
- Reportes periódicos.
- Informe de incidentes.
- Evidencia técnica para investigación forense.
- Gestión de políticas de seguridad.
- Ajuste de reglas/políticas basado en las amenazas detectadas.

La solución deberá soportar las versiones de Windows actualmente utilizadas por la organización, incluyendo versiones de escritorio y servidor soportadas por el fabricante.

- Estaciones de trabajo
- Windows 11 64 bits.
- Windows 10 64 bits.
- Servidores
- Win Server 2016 Standard (Hyper - V)

• Win Server 2019 Standard (Hyper - V)

CONDICIONES DE ENTREGA

o Activación, configuración de la consola en la nube.

o Configuración y parametrización de los Productos.

o Capacitación al personal de apoyo tecnológico en el uso de las consolas de administración, mínimo 4 horas previa concertación con el supervisor.

o Instalación y configuración en sitio de las licencias adquiridas en los equipos de cómputo de la entidad en Sistemas Operativos Win 11 Pro, 10 Pro, Win Server 2016 Standard (Hyper - V), Win Server 2019 Standard (Hyper - V).

o Soporte técnico remoto proactivo durante la vigencia de la licencia (compréndase el soporte en reconfiguración de consola, soporte en la administración de la consola, conexión y actualización de los agentes, limpieza de virus), máximo en 4 horas después de la solicitud de soporte.

CONDICIONES TÉCNICAS Y COMERCIALES ESTABLECIDAS PARA ENTREGAR, INSTALAR, Y PONER EN

FUNCIONAMIENTO LA RENOVACIÓN ADQUIRIDA.

a) Aspectos técnicos previos a la Instalación: Una vez cumplidos los requisitos de perfeccionamiento y ejecución del contrato, entre el contratista y el supervisor designado, definirán el cronograma para instalar las licencias y realizar las revisiones respectivas, junto con la entrega del documento físico o digital, donde conste el derecho de uso de las licencias para el Area Metropolitana de Bucaramanga. Adicionalmente el proveedor debe incluir la siguiente información: Ficha técnica, operación y mantenimiento.

b) Condiciones de instalación, implementación y puesta en funcionamiento: Cumplidos los requisitos previamente señalados, se formalizará por parte del supervisor del contrato, la recepción e ingreso al almacén de los licenciamientos adquiridos a través del soporte documental, toda vez que, al ser un software en la nube se configura la consola. Una vez instaladas, probadas y concluidas las pruebas de funcionamiento, el contratista procederá a realizar la transferencia de conocimiento en la operación de los productos adquiridos e instalados a los funcionarios de la entidad que el Supervisor establezca, de los cuales se dejará un registro de asistencia.

c) Condiciones post-venta: La oferta debe incluir la información de cumplimiento referente a las condiciones y especificaciones técnicas mínimas en la fase de post-venta, tales como: mantenimientos, asistencias ante fallos por garantía (tiempos de respuesta), configuración de la herramienta, asistencia técnica, y el dossier de entrega de las licencias que hacen parte de la solución adquirida.

d) Dossier de entrega: El contratista suministrará con el acta de entrega los siguientes documentos que constituyen el dossier de entrega:

1) Certificado de Licenciamiento expedido por el fabricante dirigido al Área Metropolitana de Bucaramanga.

2) Certificado de soporte y garantía por doce (12) meses, expedida por el contratista por la instalación, configuración y funcionamiento.

3) Fichas técnicas del sistema/producto.

4) Datos de contacto para atención postventa.

5) Registro de transferencia de conocimiento a personal de Apoyo tecnológico de la Entidad.

6) Registro de capacitación a funcionarios y contratistas del Área Metropolitana de Bucaramanga en temas de seguridad informática

2.1.2 OBLIGACIONES GENERALES DEL CONTRATISTA

En desarrollo de la contratación a realizar de adquisición de suministro de bienes, se deben cumplir con las siguientes obligaciones:

1. Adelantar todas las gestiones necesarias para la ejecución del contrato en condiciones de oportunidad, eficiencia y calidad, bajo las condiciones económicas, técnicas y financieras estipuladas en las cláusulas correspondientes y de acuerdo a las especificaciones exigidas por el AMB en los estudios previos y los pliegos, las cuales hacen parte vinculante del contrato.

2. Disponer oportunamente de todo lo necesario, para que el objeto del contrato se cumpla a cabalidad.

3. Pagar de manera oportuna los salarios, prestaciones sociales e indemnizaciones de todo el personal que ocupe en la ejecución del contrato estableciendo que NO se podrá subcontratar ningún servicio necesario para el cumplimiento del objeto contratado, quedando claro que no existe ningún tipo de vínculo laboral del personal que utilice el contratista con el Área Metropolitana de Bucaramanga.

4. Cumplir con lo establecido para el efecto en el artículo 50 de la ley 789 de 2002, y la ley 828 de 2003. El incumplimiento de esta obligación será causal de multas, y caducidad del contrato de conformidad con las normas vigentes.

5. Acreditar de acuerdo con lo establecido en el inciso segundo del artículo 41 de la Ley 80 de 1993, adicionado mediante el artículo 23 de la ley 1150 de 2007, que se encuentra al día en el pago de aportes parafiscales relativos al Sistema Nacional de Aprendizaje - SENA, Instituto Colombiano de Bienestar Familiar - ICBF y las cajas de compensación familiar, cuando corresponda.

6. Responder por los impuestos que cauce la legalización del contrato

7. Mantener indemne a la entidad frente a reclamaciones judiciales y extrajudiciales por los daños y perjuicios que se deriven de los actos, omisiones o hechos ocasionados por las personas que sean subcontratistas o dependan del adjudicatario.

8. Responder por toda clase de demandas, reclamos o procesos que instaure el personal o los subcontratistas.

9. Salvaguardar la información confidencial que se obtenga o conozca en desarrollo de la ejecución del contrato, salvo requerimiento expreso de autoridad competente. Toda la información o documentos que se produzcan en desarrollo del contrato a firmar serán de uso exclusivo del AMB, obligándose a no utilizarlos para fines distintos a los previstos, ni a divulgar la información que se le suministre.

10. Cumplir a cabalidad con el objeto del contrato, ejecutando las actividades contratadas de acuerdo con los documentos que soportan el presente objeto contractual.

11. Cumplir con las normas y especificaciones técnicas.

12. Suministrar tanto en calidad, cantidad como en tiempo, todo el personal, equipo, herramientas, y demás elementos necesarios para la ejecución de las actividades previstas en el objeto.

13. Acatar las órdenes e instrucciones del supervisor del contrato.

14. Atender en forma permanente a la supervisión dirección de la ejecución del objeto contractual.

15. Atender las consultas requerimientos y recomendaciones que se presenten durante la ejecución del objeto contractual, emitidas por el supervisor.

16. Elaborar y presentar, las actas mensuales e informes de ejecución requeridos

17. Informar al AMB de cualquier situación que pudiera generar la suspensión y/o paralización del contrato.

18. Mantener actualizadas las garantías del contrato, de acuerdo con las modificaciones o adiciones contractuales que se llegasen a suscribir

19. Otorgar al AMB los beneficios a que tenga derecho.

20. Las demás inherentes al contrato para su ejecución en debida forma, así como las contenidas en la invitación pública y que no hayan sido incluidas en el presente documento

2.1.3 OBLIGACIONES ESPECÍFICAS DEL CONTRATISTA:

1. Entregar e instalar en sitio las licencias de acuerdo con las condiciones y especificaciones técnicas establecidas.

2. Cumplir con cada uno de los elementos descritos en las cantidades, calidad y en los lugares, fecha y hora que le indique el supervisor.

3. Cumplir a cabalidad con las condiciones técnicas requeridas en el presente proceso.

4. Responder ante la entidad y ante terceros por la divulgación indebida o el manejo inadecuado de la información entregada por la AMB para el desarrollo de las actividades contratadas.

5. Contar con el personal certificado para la entrega, instalación y puesta en funcionamiento de las licencias adquiridas.

6. Allegar certificado que acredite que es distribuidor autorizado de la marca ofertada para la venta de licencias antivirus.

7. En caso de ser distribuidor autorizado, extender a la entidad todos los beneficios que reciban del fabricante relacionados con el software.

8. Garantizar la protección de datos e información entregada por la entidad, de conformidad con las disposiciones legales vigentes.

9. Brindar Capacitación al personal de apoyo tecnológico en el uso de las consolas de administración mínimo 4 horas, previa concertación con el supervisor.

10.Brindar soporte técnico remoto proactivo durante la vigencia de la licencia (compréndase el soporte en reconfiguración de consola, soporte en la administración de la consola, conexión y actualización de los agentes, limpieza de virus) máximo en 4 horas después de requerido.

11.Desinstalar de los equipos de cómputo la totalidad de los antivirus adquiridos anteriormente por la entidad.

12.Instalar en sitio, el total de las licencias en los equipos de cómputo indicados por el supervisor del contrato. Cualquier costo derivado de un consumo generado después de la fecha de terminación del contrato, no será asumido por el AMB.

13.Entregar los soportes (Certificado de Licenciamiento expedido por el fabricante dirigido al Área Metropolitana de Bucaramanga) que acrediten el licenciamiento del fabricante adquirido dentro del presente proceso contractual.

14.El contratista durante el tiempo de la vigencia de la licencia (1 año), dé acompañamiento de soporte primer nivel (Nuevas versiones liberadas en consola y agentes, actualización bases de datos, conectividad con la consola y actualizaciones).

15.Las licencias suministradas son para uso en entidad de gobierno.



Representante legal