GOBERNACIÓN DE Boyacá	**FORMATO**	**VERSIÓN: 0**
		CÓDIGO: A-AD-GC-F-018
ACEPTACIÓN DE OFERTA		**FECHA: 24/Jul/2019**

Tunja, 30 de noviembre 2023

No. PROCESO SMC	**No. DE CONTRATO**
107-2023	3548/2023

SEÑOR:
CONSULTORIA TECNICA Y SERVICIOS DE INGENIERIA SOCIEDAD POR ACCIONES SIMPLIFICADA
COTEC S.A.S
Nit 800127892 - 1
JOSE ANTONIO MATHEUS ROCHA
Dirección: Avenida Universitaria No. 41 – 50
Torre 1 Oficina 4 -Mirador
Ciudad: Tunja.

Referencia: Aceptación de oferta invitación: SMC GB 107 / 2023.

De conformidad con lo dispuesto por el artículo 94 de la Ley 1474 de 2011 y por lo reglamentado en la Subsección 5 del Decreto 1082 de 2015, me permito manifestarle que la oferta que usted ha presentado con relación a la invitación pública de la referencia ha sido aceptada de manera incondicional.

Para todos los efectos a que haya lugar, se entiende que esta carta de aceptación implica que con usted ha quedado celebrado el contrato de mínima cuantía que a partir de la fecha queda codificado de la siguiente manera:

Fecha:	30 de noviembre del 2023	
Tipo de contrato:	**PRESTACION DE SERVICIOS**	
Objeto:	**RENOVACION DEL LICENCIAMIENTO DE ANTIVIRUS ESET ENDPOINT PROTECTION ADVANCED PARA LA GOBERNACIÓN DE BOYACÁ DURANTE 3 AÑOS PARA 1165 ESTACIONES DE TRABAJO (PC) Y 35 SERVIDORES MS WINDOWS**	
Contratista	**Nombre: CONSULTORIA TECNICA Y SERVICIOS DE INGENIERIA SOCIEDAD POR ACCIONES SIMPLIFICADA** R/L JOSE ANTONIO MATHEUS ROCHA C.C. 91.202.337	
	Nit 800127892 - 1	
	Teléfono: 3107637363	Correo electrónico: **gerencia@cotec-ltda.com**
CDP	**6629 del 23 de octubre del 2023**	
Proyecto:	**N.A**	
Valor:	**VALOR TOTAL: OCHENTA Y CUATRO MILLONES NOVECIENTOS CINCUENTA MIL PESOS ($84.950.000.00) M/ CTE,** incluido impuestos y la totalidad de los costos directos e indirectos en que se incurra para la ejecución del contrato.	
Forma de Pago:	El valor establecido será cancelado de la siguiente forma: Un único pago a contra entrega del cien por ciento (100%) de la ejecución de las actividades contratadas, se haga entrega del documento que permite establecer que se haya renovado la licencia de uso de ESET ENDPOINT PROTECTION ADVANCED, verificada la instalación y configuración del software en los equipos de la Gobernación de Boyacá una vez	

	se dé recibido a satisfacción y se suscriba el acta de liquidación expedida por el supervisor del contrato y demás formatos establecido por el Sistema Integrado de Gestión de Calidad, si con la cuenta no se acompañan los documentos requeridos para el pago, será responsabilidad del CONTRATISTA y no tendrá por ello derecho al pago de intereses o compensación de ninguna naturaleza, está deberá ser radicada en la Central de Cuentas de la Gobernación de Boyacá, dando cumplimiento al Artículo 19 de la Ley 1150 de Julio 16 de 2007. *DEL DERECHO DE TURNO*
Plazo:	La ejecución del contrato será de 30 días calendarios a partir del acta de inicio. **Plazo de vigencia de la licencia**: 3 años a partir de la activación del producto
Lugar de Ejecución	Dirección de Sistemas de Información Centro de datos

Usted deberá cumplir con la ejecución del contrato de conformidad con las condiciones de la invitación publicada y con los ofrecimientos formulados en su propuesta.

Como contratista del departamento deberá tener en cuenta los siguientes aspectos:

1- NORMAS APLICABLES, RESPONSABILIDAD Y AUSENCIA DE RELACIÓN LABORAL:

- La presente contratación, se regirá por las disposiciones de la Ley 80 de 1993, Ley 1150 de 2007, artículo 94 de la Ley 1474 de 2011, la Subsección 5 del Decreto 1082 de 2015 y demás normas reglamentarias y complementarias aplicables de conformidad con el Estatuto General de Contratación de la República de Colombia.
- Como contratista estará sujeto al régimen de responsabilidades civiles, disciplinarias, fiscales, sociales y penales señalados por la ley.
- Ni la celebración, ni la ejecución de este contrato genera relación laboral ni derecho a prestaciones sociales.

2- INCORPORACIÓN DE CLÁUSULAS EXCEPCIONALES AL DERECHO COMÚN: Dentro del contrato se entenderán pactadas por las partes las cláusulas de caducidad, terminación, modificaciones, interpretación unilateral, previstas en los artículos 15 al 18 de la Ley 80 de 1993, con las consecuencias legales y económicas que de ellas se deriven, cuando aplique.

3- JURAMENTO Y CESIÓN: el contratista declara bajo la gravedad de juramento que no se halla incurso en ninguna de las inhabilidades o incompatibilidades establecidas en el derecho vigente, especialmente los artículos 8, 9 y 10 de la Ley 80 de 1993.

Las obligaciones adquiridas en virtud de la presente contratación no podrán ser cedidas a título alguno mientras no medie autorización expresa y escrita por parte del Departamento.

4- ESPECIFICACIONES TECNICAS:

ITEM	ESPECIFICACION TECNICA
1	**TECNOLOGÍA Y CARACTERÍSTICAS** • La solución realiza exploraciones en estado inactivo para poder brindar de esa forma, una protección proactiva mientras el equipo no está en uso. • Posee un caché local para aumentar el rendimiento de los entornos virtuales, garantizando que el archivo sólo se explora una vez. • El producto posee 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 se puede asignar por un rango de tiempo, por grupo y por equipo.

• Tiene la capacidad de enviar una tarea para la actualización de los parches del sistema operativo.

• Dentro del módulo de firewall cuenta con la funcionalidad de bloqueo de exploits.

• La solución de antivirus ejecuta un escaneo únicamente en los siguientes estados en la computadora:

o Protector de pantalla activo

o Sesión de usuario bloqueada

o Sesión de usuario finalizada

• La solución permite o niega el uso de los dispositivos en base a los siguientes criterios:

o Fabricante

o Modelo

o Número de serie

• La solución permite definir un listado específico de usuarios quienes pueden hacer uso de los dispositivos. Para dispositivos de almacenamiento, la solución permite configurar únicamente de los siguientes permisos:

o Lectura/Escritura

o Bloqueo

o Solo de lectura

o Advertir

• Cuando se conecta o usa un dispositivo de almacenamiento, la solución de antivirus proporciona las siguientes opciones:

o Escanear

o No realizar ninguna acción

o Recordar esta acción

• Sistema de prevención de intrusiones basado en el host (HIPS)

La solución tiene un sistema de prevención de intrusiones basado en el host. El sistema HIPS debe tener los siguientes modos de configuración:

o Modo automático o Modo inteligente o Modo interactivo

o Modo basado en políticas

o Modo aprendizaje

• El aprendizaje automático avanzado o “machine learning” tiene cuatro umbrales: Intenso,

Balanceado,

Cauteloso y

Desactivado.

• Tiene una tarea para aislar a un equipo de la red.

• El HIPS incluye una inspección a fondo del comportamiento de todos los programas en ejecución, archivos y llaves de registro.

• Cuenta con filtrado para mantener libre de SPAM a los clientes de correo.

• La solución permite verificar las comunicaciones usando protocolos SSL para hallar amenazas.

• Firewall personal, la solución de antivirus posee un firewall personal. El firewall tiene los siguientes modos de configuración:

o Modo automático

o Modo interactivo

o Modo basado en políticas

o Modo aprendizaje

• Las reglas de firewall creadas permite todas las siguientes acciones:

o Denegar

o Permitir

o Preguntar

DE LA CONSOLA

Permite la ejecución remota de scripts, batch files y paquetes personalizados a través de la consola, de terceros.

Es una solución que puede ser usada y administrable desde la consola de antivirus en sistemas operativos Windows, Linux y Mac.

Permite generar grupos de clientes dinámicos y grupos estáticos.

El fabricante proporciona al menos tres diferentes formas de realizar la instalación de la consola de administración.

o Instalador todo en uno

o Instalación por componentes

o Aparato virtual

El Appliance virtual soporta al menos las siguientes plataformas de virtualización

o VMWare

o vSphere

o Oracle Virtual Box

o Microsoft Hyper-V

o Azure - ambiente basado en la nube

• La consola de Administración estar basada en Cloud.

• Permite Activar el acceso a la consola de antivirus con doble factor de autenticación, integrada a la misma consola de antivirus, sin ningún add-on o software adicional.

• Posee desinstalador de antivirus de terceros.

• Posee un módulo específico para la protección contra ransomware.

• Tiene 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.

• Cuenta con etiquetas independiente al LDAP, para identificar y buscar objetos similares.

• Se Obtiene 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 maneja la tecnología de Sandboxing en nube para el análisis de posibles amenazas, cifrado de los discos de almacenamiento de los puntos finales y se integra con la solución de detección y respuesta del punto final.

• A través de la consola de administración de seguridad del punto final es posible administrar dispositivos móviles iOS y Android.

• Por disponibilidad de la solución de protección de punto final, la consola de administración tiene la capacidad para construir ambientes distribuidos donde pueden 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 muestra toda la información en la consola central de administración del punto final de forma nativa.

	• La solución tiene el mecanismo para desinstalar otras soluciones antivirus presentes en el equipo final. Este mecanismo esta: 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.
	ESET Endpoint Security for Android • La solución de antivirus realiza análisis a las aplicaciones instaladas, archivos. DEX. • La solución de antivirus ofertada analiza memoria interna y tarjeta SD para cualquier tipo de archivo. • Es capaz de mostrar un listado de las aplicaciones instaladas, controlar el tiempo del uso de aplicaciones y el detalle de los permisos que usan los aplicativos del dispositivo móvil. • El análisis de la solución de protección de punto final explora hasta 3 anidados. • La protección del dispositivo móvil cuenta con una protección en tiempo real, además de contar con un sistema de reputación de archivos. • Permite administrar las aplicaciones que deberían estar instaladas en los dispositivos móviles. • Tiene la capacidad para detectar de forma automática aplicaciones no deseadas y no seguras para usar en el dispositivo móvil. • La solución permite enviar mensajes SMS al administrador cuando existen usuarios no autorizados manipulando el dispositivo móvil. • La solución permite proteger y seleccionar los navegadores a usar. • La solución de antivirus optimizar la batería del dispositivo y ejecuta el análisis al dispositivo únicamente cuando esté completamente cargado o conectado a la energía eléctrica. • La solución detecta nuevas tarjetas SIM instaladas en el dispositivo y las bloquea. • la solución es 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 mantiene un control de aplicaciones, las bloquea según los permisos de la aplicación o por categoría, limita la instalación de aplicaciones únicamente desde Google Play, y puede bloquear cualquier aplicación en el momento que se necesite. • La solución evitar ataques de suplantación de identidad de sitios web.
	ESET 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 incluye la detección y bloqueo de intrusiones, agrega a lista negra aquellas direcciones que han sido identificadas con este comportamiento malicioso. • La solución agrega de forma automática las exclusiones que correspondan a aplicaciones críticas del servidor. Optimiza 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
	OTROS • El fabricante posee soporte técnico en castellano. • El fabricante directamente brinda servicios de seguridad informática como por ejemplo penetration testing, vulnerability assessment o análisis de GAP. (Valor adicional al licenciamiento). • El fabricante ofrecer directamente un servicio de caza de amenazas. (Valor adicional al licenciamiento). • El fabricante posee un laboratorio de análisis y detección de malware en Latinoamérica. • Oficinas de la marca en Latinoamérica y presencia local en el país. • El fabricante tiene programas de “colaborador seguro” (Valor adicional al licenciamiento).

Esquema de Soporte y Servicios

• Se incluye la asistencia para verificación/ desinstalación de la actual instalación y configuración de la solución antivirus existente. (*)

• Soporte técnico. Los días hábiles de 8AM a 5PM. Para horarios diferentes en días no hábiles se realizará un acuerdo dependiendo de las necesidades.

o Telefónico.

o Vía e-mail.

o Mensajería instantánea

o A través de acceso remoto

o Visitas on site

• Laboratorio ESET Latinoamérica. Recolección (por acceso remoto) y envío de muestras a nuestro laboratorio para el análisis de nuevas amenazas.

• Capacitación técnica. Se realizará de manera presencial/ virtual entrenamientos en el uso de las soluciones de ESET adquiridas.

• Visitas proactivas. Se realizarán visitas presenciales o virtuales, por parte del partner asignado, para revisar los logs y la configuración de los productos de ESET implementados, proponiendo a partir de esto las mejoras respectivas.

(*) siempre que existan las credenciales y la configuración actual sea la usual.

Requisitos del sistema e información de licencia.

Para computadoras

Microsoft Windows 10, 8.1, 8, 7, Vista (*)

macOS 10.9 y posterior

Ubuntu Desktop 18.04 LTS de 64 bits y RedHat Enterprise Linux (RHEL) Desktop 7 de 64 bits

(*) solo con cobertura si Microsoft ofrece las actualizaciones necesarias para la ultima versión; en otro caso se usa la versión anterior que permita tener un grado de administracion ajustado.

Para dispositivos Android : Android 5 (Lollipop) y posterior iOS 8 y posterior

Server

Microsoft Windows Server 2019, 2016, 2012, 2008

Microsoft Windows Storage Server 2016, 2012, 2008

Microsoft Windows MultiPoint Server 2012, 2011, 2010

Microsoft Windows Small Business Server 2011, 2008

RedHat Enterprise Linux (RHEL) 7 de 64 bits

CentOS 7 de 64 bits

Ubuntu Server 16.04 LTS de 64 bits, 18.04 LTS de 64 bits

Debian 9 de 64 bits

SUSE Linux Enterprise Server (SLES) 12 de 64 bits, 15 de 64 bits

Entornos Virtuales

VMware vSphere 6.0, 6.5+, 6.7+ (vCenter Single Sign-On, vSphere Client / Web Client, vCenter Server, vCenter Inventory Service)

VMware NSX Manager 6.3+, 6.4.0, 6.4.1, 6.4.2

Introspección de invitado de VMware 6.2.4+, 6.3+, 6.4+

5- OBLIGACIONES DEL CONTRATISTA: El contratista se compromete con el Departamento a:

5.1. OBLIGACIONES GENERALES DEL CONTRATISTA:

1 Dar cumplimiento a los derechos y deberes consagrados en el artículo 5º de la Ley 80 de 1993.
2 Conocer íntegramente los manuales del Sistema Integrado de Gestión de Calidad de la Gobernación de Boyacá y aplicar los procedimientos con sus respectivos formatos en desarrollo del contrato y participar en la actualización de procedimientos del sistema según asignación.
3 Previo a la ejecución del contrato, suscribir acta de inicio con el supervisor designado y radicar el documento original en Secretaría de Contratación de la Gobernación de Boyacá dentro de los tres (3) días calendario siguientes para efectos de publicación y reporte a entes de control.
4 El contratista deberá radicar las pólizas dentro de los dos días siguientes a la firma del contrato.
5 Ejecutar y cumplir el objeto del contrato, de acuerdo con lo estipulado en los estudios y las cláusulas del contrato.
6 Elaborar y entregar, de manera oportuna y en el lugar indicado, los informes solicitados por el supervisor, en los formatos aprobados para tal fin.
7 Obrar con diligencia y cuidado necesario en los asuntos que le asigne el supervisor del contrato.
8 Seguir las indicaciones que el supervisor del contrato realice por escrito.
9 Obrar con lealtad y buena fe en cada una de las etapas contractuales, evitando dilataciones y entrabamientos.
10 Presentar los certificados de pago de aportes al sistema general de seguridad social y de parafiscales de conformidad a la normatividad vigente.
11 Mantener la reserva sobre la información que le sea suministrada para el desarrollo del objeto del contrato.
12 El CONTRATISTA debe custodiar y a la terminación del presente contrato devolver los insumos, suministros, herramientas, dotación, implementación, inventarios y/o materiales que sean puestos a su disposición para la prestación del servicio objeto de este contrato.
13 CONFIDENCIALIDAD. El CONTRATISTA debe guardar y mantener reserva de toda la información que sea de propiedad del DEPARTAMENTO DE BOYACÁ o conozca en desarrollo del contrato, en especial cuando se trate de información sujeta a reserva legal. Igualmente, el CONTRATISTA está obligado a entregar todos los documentos, correspondencia, publicaciones, útiles y demás bienes de propiedad del DEPARTAMENTO DE BOYACÁ relacionados con el objeto del presente contrato y aquellos que contengan información confidencial. En consecuencia, EL CONTRATISTA se obliga a: A. Proteger la información confidencial que el DEPARTAMENTO DE BOYACÁ comparta o suministre; B. Seguir los procedimientos establecidos en el manual de políticas de seguridad de la información el cual se encuentra en el sistema integrado de gestión; C. No dar a conocer a terceros la información confidencial, sensible, crítica, reservada o clasificada a terceros, que pueda perjudicar al DEPARTAMENTO DE BOYACÁ; D. No dar a la información confidencial un uso distinto para el cual fue compartida o suministrada, salvo previa autorización por escrito del DEPARTAMENTO DE BOYACÁ; E. Devolver y entregar toda la información archivada, utilizando la nemotecnia de las tablas de retención documental; F. Cumplir con el plan de continuidad del negocio el cual se encuentra en el sistema integrado de gestión; G. No podrá realizar la interceptación de la red de transmisión de datos en concordancia con la ley 1273 de 2009. H. Indemnización: EL CONTRATISTA se obliga a resarcir los perjuicios, por daño emergente y lucro cesante que llegare ocasionar la revelación, divulgación o utilización de la información de manera distinta al objeto del presente contrato, ya sea por mera negligencia o de forma dolosa.

5.2. OBLIGACIONES ESPECIFICAS DEL CONTRATISTA

Para efecto de la ejecución del objeto del contrato, el contratista deberá cumplir con las siguientes actividades y especificaciones:

1. Renovación de la licencia de antivirus Eset Endpoint Protection Advanced debe cubrir todas las versiones de los sistemas Operativos Microsoft instalados en los equipos de la Administración Departamental.
2. Atender con prontitud y efectividad las solicitudes, condiciones y/o recomendaciones del supervisor dentro de los términos del contrato.

3. Ejecutar el objeto del contrato, cumpliendo las condiciones técnicas, económicas y financieras contenidas en la propuesta.
4. Cumplir con los procedimientos establecidos en el Sistema Integrado de Gestión.
5. Se deben aplicar la activación de la licencia en el momento de que sean instaladas en los equipos de la Gobernación de Boyacá
6. Se debe garantizar que la instalación y configuración de la consola del antivirus Eset Endpoint Protection Advanced existente en el servidor de la Gobernación de Boyacá, se mantenga debidamente operativa y ofrezca el rendimiento esperado.
7. Se debe capacitar periódicamente al personal designado por la administración sobre el manejo y configuración de la consola del antivirus con una intensidad mínima de 10 horas.
8. Se debe revisar la integridad de la Base de Datos del antivirus existente Eset Endpoint Protection Advanced.
9. Se debe garantizar que siempre se tendrá la última versión, actualizaciones y configuraciones del software contratado por la duración de la licencia adquirida.
10. Garantizar el Soporte telefónico, por correo electrónico y/o mensajería instantánea, con un horario de atención de lunes a viernes de 8:00 a.m. a 5:00 p.m., teniendo en cuenta que la atención de requerimientos se hará en un tiempo máximo de una (1) hora.
11. Soporte On site: Corresponde a la asistencia técnica y asesoría presencial de lunes a viernes, para los productos ofertados durante el tiempo de mantenimiento adquirido; el tiempo de respuesta será de máximo ocho (8) horas hábiles para prestar el servicio en la modalidad de bolsa horas, que para este caso será durante la vigencia de la licencia adquirida.
12. Soporte técnico de fábrica 7 * 24: Se debe contar con un centro de soporte y asistencia técnica a través de la página Web del fabricante, donde se disponga la consulta en español de: FAQ (preguntas frecuentes), biblioteca de virus, avisos de seguridad, contacto con soporte técnico a través de un formulario, suscripción a boletines de seguridad y soporte telefónico: help desk.
13. Revisión del estado de la consola de administración, que incluya mejoramiento en la configuración (o reinstalación) y sugerencias, mediante dos (2) visitas programadas, cada una de cuatro (4) horas en horario hábil, durante el período de mantenimiento y actualización adquirido.
14. Se debe suministrar la licencia de uso, manuales e instaladores del antivirus cuya renovación se pide suministrar en medio físico y magnético oficiales del proveedor.
15. Se debe transferir los conocimientos al personal técnico de la entidad sobre la implementación y puesta en marcha de la solución adquirida, además apoyará a la organización en la divulgación de buenas prácticas de seguridad por medio de charlas en sitio, webminarios, e información de interés vía correo electrónico.
16. El contratista deberá acompañar a la Gobernación de Boyacá en el seguimiento y verificación del correcto funcionamiento de la plataforma antivirus durante el tiempo de vigencia de la licencia, mediante una valoración mínima, cada tres meses.
17. El contratista durante el tiempo de vigencia de la licencia deberá entregar un reporte en el cual se incluyan las acciones que debe tomar la entidad para corregir las incidencias encontradas

6- CUMPLIMIENTO DE OBLIGACIONES PARAFISCALES: El contratista deberá dar estricto cumplimiento a las obligaciones de que trata el artículo 23 de la Ley 1150 de 2007 y demás normas vigentes en la materia. Lo cual se verificará por el supervisor designado al momento de suscribir el acta de iniciación y para tramitar los desembolsos pactados.

7- MULTAS Y SANCIONES: Las partes acuerdan que el Departamento de Boyacá, en caso de mora o incumplimiento parcial de las obligaciones pactadas por parte del contratista o entidad parte del convenio, el Departamento podrá imponerle multas de acuerdo al Estatuto Anticorrupción (Ley 1474 de 2011), Código de Procedimiento Administrativo y de lo Contencioso Administrativo (Ley 1437 de 2011), demás normas aplicables, y lo establecido en el procedimiento determinado por la Entidad para dar trámite a los procesos sancionatorios contractuales vigente al momento de dar inicio al procedimiento correspondiente. El pago del valor de dichas multas no exonera al contratista o entidad parte del convenio de su obligación de ejecutar las obligaciones adquiridas".

8- PENAL PECUNIARIA: En caso de incumplimiento, multas, sanciones o de declaratoria de caducidad Administrativa, cuando aplique, el DEPARTAMENTO DE BOYACÁ podrá hacer efectiva a título de pena una suma equivalente hasta por el VEINTE (20%) del valor del contrato o convenio, suma esta que ingresará al tesoro de la Entidad contratante y podrá ser tomada directamente del saldo a favor del Contratista o entidad parte del convenio, si lo hubiere. La cual se hará efectiva de acuerdo a lo establecido en el Artículo 17 de la Ley 1150 de 2007, el Articulo 86 de la Ley 1474 de 2011, Código de Procedimiento Administrativo y de lo Contencioso Administrativo (Ley 1437 de 2011), demás normas aplicables, y lo establecido en el procedimiento determinado por la Entidad para dar trámite a los procesos sancionatorios contractuales vigente al momento de dar inicio al procedimiento correspondiente".

9- GARANTÍAS: De conformidad con lo establecido en el Artículo 7 de la ley 1150 del año 2007, el análisis de riesgos expuesto en el presente estudio previo y Articulo 2.2.1.2.3.1.1 del decreto 1082 de 2015, el oferente y el contratista se obliga a constituir, a favor del Departamento de Boyacá Garantía única que ampare lo siguiente:

Clase de Riesgos	%	Sobre el Valor	Vigencia
Cumplimiento del Contrato	20	Del contrato	La del contrato y hasta la liquidación del contrato
Calidad del servicio	20	Del contrato	La del contrato y un (1) año más
CALIDAD DE LOS BIENES SUMINISTRADOS	20	Del contrato	La del contrato y un (1) año más
Pago de Salarios, Prestaciones Sociales e Indemnizaciones.	5	Del contrato	La del contrato y tres (3) años más

Las vigencias de todos los amparos deberán ajustarse a las fechas del Acta de Iniciación del contrato. Así mismo, los valores asegurados para los amparos de pago de salarios y prestaciones sociales deberán ajustarse al valor final del contrato, según el Acta de Liquidación del mismo.

En cualquier evento en que se modifique el plazo o valor del contrato deberán modificarse las correspondientes garantías. El hecho de la constitución de estos amparos no exonera al CONTRATISTA de las responsabilidades legales en relación con los riesgos asegurados.

De conformidad con lo establecido en el Decreto 1082 de 2015, para la ejecución del contrato se requiere la aprobación de la garantía única por parte de La Dirección de Contratación del Departamento.

10- INDEMNIDAD: EL CONTRATISTA, mantendrá indemne al DEPARTAMENTO de los reclamos, demandas, acciones legales o costos que se generen por daños o lesiones causadas a personas o bienes de terceros, ocasionados por EL CONTRATISTA, subcontratistas o proveedores durante la ejecución del objeto contratado.

11- DOCUMENTOS CONTRACTUALES: Para todos los efectos son documentos que integran esta aceptación de oferta y por lo tanto hacen parte integral del mismo: a. Invitación selección mínima cuantía No. 107 de 2023. b. Certificado de Disponibilidad presupuestal. c. Propuesta presentada y sus soportes. d. Informes de evaluación. e. Los demás generados de la ejecución de los mismos (actas, informes, paz y salvo, planillas, etc.).

12- COMPROMISO ANTICORRUPCIÓN: El contratista se compromete a informar y denunciar ante la entidad contratante y/o a las autoridades correspondientes los hechos constitutivos de corrupción que tuvieren lugar dentro del ejecución del contrato o convenio, de conformidad a las reglas previstas en la ley.

13- EJECUCIÓN: Para su ejecución se requiere la aprobación de la garantía, en caso que la misma sea exigida y la expedición del Registro Presupuestal correspondiente a cargo del Departamento.

14- DESIGNACIÓN DE SUPERVISIÓN: La supervisión será desarrollada por parte de

Nombre: LUIS EDGAR MARTINEZ MUÑOZ
Cargo: Profesional Universitario
Identificación: 6.775.840
Secretaria TIC y Gobierno Abierto

En caso que el titular del cargo sea sustituido, la supervisión será asumida por su reemplazo y debe formalizarse a través del formato "**A-AD-GC-F-051 ACTA DE ENTREGA DE SUPERVISIÓN O INTERVENTORÍA".**

15- INCUMPLIMIENTO DE REQUISITOS DE EJECUCIÓN: El incumplimiento de las obligaciones que corresponden al contratista referente a los requisitos de ejecución será causal de incumplimiento del contrato, el cual será declarado por medio de acto administrativo que se expedirá dentro de las reglas del debido proceso.

WILLIAM YESID ARCHILA CARDENAS
Secretario de Contratación
Delegado para la Contratación

Revisó. **ANDREA CONSTANZA GONZALEZ FONSECA**
Directora de Procesos de Selección (E)

Proyectó: Carolina Carreño
Profesional Externo