COMUNICACIÓN DE ACEPTACIÓN DE OFERTA

Señores:
PC STORE IT SOLUCIONES Y SERVICIOS S.A.S. SIGLA PC STORE IT S.A.S
NIT 900.872.496-5
Rep Legal CARLOS ALBERTO COGOLLO ARISTIZABAL
CC.No 10.769.850, expedida en Montería
Referencia: PROCESO DE MÍNIMA CUANTÍA No. MC-DAL-036-2022

La suscrita **KAREN ROCIO MATOREL BELLO**, mayor de edad, vecina de esta ciudad, identificada con cédula de ciudadanía No.**45.555.311** de Cartagena En ejercicio de mis funciones y facultades constitucionales, legales y reglamentarias, y en consideración a la delegación otorgada mediante decreto No. 348 del 16 de Agosto del años 2022 a la Dirección Administrativa de Logística Código 009 grao 02, asignado a la dirección logística en materia contractual, y dando cumplimiento las normas del Decreto 1082 de 2015, y la Ley 1474 de 2011, se le informa que verificado los requisitos habilitantes y el valor de la propuesta presentada dentro del proceso de Invitación Pública No**. MC-DAL-036-2022,** se acepta expresa e incondicionalmente su oferta, la cual junto con la presente comunicación y el documento de invitación pública del proceso constituyen para todos los efectos el contrato, el que se regirá además por las siguientes estipulaciones, características y condiciones:

CONTRATANTE:	**DEPARTAMENTO DE BOLÍVAR**
CONTRATISTA	**PC STORE IT SOLUCIONES Y SERVICIOS S.A.S. SIGLA PC STORE IT S.A.S**
IDENTIFICACION	Nit No. **900.872.496-5**
REPRESENTANTE LEGAL	**CARLOS ALBERTO COGOLLO ARISTIZABAL** **CC.No** 10.769.850, expedida en Montería
OBJETO	**CONTRATAR LA RENOVACIÓN DE LICENCIA DE SOFTWARE ANTIVIRUS BITDEFENDER, CON ACTUALIZACION, SOPORTE, CAPACITACION Y ASISTENCIA TECNICA POR EL TERMINO DE UN AÑO, PARA LAS ESTACIONES DE TRABAJO Y SERVIDORES DE LA PLATAFORMA TECNOLOGICA DE LA GOBERNACION DE BOLIVAR".**
CONDICIONES TÉCNICAS - ESPECIFICACIONES TECNICAS	

ITEM	DESCRIPCION	CANT.
1	**SUMINISTRO DE LICENCIAS DE ANTIVIRUS PARA WINDOWS** • Capacidad de instalar remotamente la solución de protección de punto final en las estaciones y servidores Windows, a través de la administración compartida, login script y/o GPO de Active Directory. • Capacidad de crear perfiles de seguridad, contiene la configuración de seguridad de los dispositivos que ejecutan Microsoft Windows. • Capacidad de asignar un perfil a usuarios o a un grupo de usuarios y mantener la coherencia de la configuración de seguridad para los usuarios. • Capacidad de envío de mensajes de correo electrónico con instrucciones para instalar aplicaciones de seguridad en dispositivos del usuario • Capacidad de tener componentes de protección contra archivos peligrosos, Protección contra amenazas de correo electrónico, Protección contra amenazas de red y Protección contra amenazas web incluyen tecnologías que protegen a los usuarios contra virus, phishing y otros tipos de amenazas • Capacidad Control de funciones y Control web: Ayuda para asegurar que los dispositivos móviles se utilicen para el trabajo corporativo y no personal. • Capacidad de gestionar estaciones de trabajo y servidores de archivos protegidos por la solución antivirus. • Capacidad de detectar y eliminar de raíz ataques avanzados, realizar un análisis de la causa raíz con un gráfico de cadena de desarrollo de la amenaza y profundizar en los detalles para su posterior revisión. • Capacidad de activar Cloud para supervisar el uso de servicios en la nube en dispositivos administrados que ejecutan Windows y bloquear el acceso a servicios en la nube que se consideren no deseados. • Capacidad de definir políticas de configuraciones diferentes por grupos de estaciones • Debe proporcionar la siguiente información de las computadoras: ○ Si el antivirus está instalado. ○ Si el antivirus ha iniciado. ○ Si el antivirus está actualizado.	800 licencias

- Minutos/horas desde la última conexión de la máquina con el servidor administrativo.
- Minutos/horas desde la última actualización de vacunas.
- Fecha y horario de la última verificación ejecutada en el equipo.
- Versión del antivirus instalado en el equipo
- Cantidad de virus encontrados (contador) en el equipo.
- Nombre del equipo.
- Fecha y horario de la última actualización de vacunas.
- Sistema operativo del equipo.
- Vulnerabilidades de aplicativos instalados en el equipo.
- Debe permitir bloquear las configuraciones del antivirus instalado en las estaciones y servidores de manera que el usuario no logre modificarlas;

- Capacidad de exportar informes para los siguientes tipos de archivos: PDF, HTML y CSV.
- Capacidad de enviar correos electrónicos para cuentas específicas en caso de algún evento.
- Capacidad de reportar vulnerabilidades de software presentes en los equipos.
- Debe proporcionar las siguientes protecciones:
  - Antivirus de archivos residente (antispyware, antitroyano, antimalware, etc.) que verifique cualquier archivo creado, accedido o modificado;
  - Antivirus de web (módulo para verificación de sitios y downloads contra virus)
  - Antivirus de correo electrónico (módulo para verificación de correos recibidos y enviados, así como sus adjuntos)
  - Autoprotección (contra ataques a los servicios/procesos del antivirus)
  - Control de dispositivos externos
  - Información de vulnerabilidades de Windows y de los aplicativos instalados
  - Las vacunas deben ser actualizadas por el fabricante y estar disponibles a los usuarios, como máximo cada hora, independientemente del nivel de las amenazas encontradas en el período (alto, medio o bajo).
  - Capacidad de detección de presencia de antivirus de otro fabricante que pueda causar incompatibilidad, bloqueando la instalación;
  - Capacidad de agregar carpetas/archivos para una zona de exclusión, con el fin de excluirlos de la verificación. Capacidad, también, de agregar objetos a la lista de exclusión de acuerdo con el resultado del antivirus.
  - Capacidad de verificar archivos por contenido, o sea, únicamente verificará el archivo si es posible de infección. El antivirus debe analizar la información de encabezado del archivo para tomar o no esa decisión a partir de la extensión del archivo;
  - Capacidad de verificar solamente archivos nuevos y modificados;
  - Capacidad de verificar objetos usando heurística;
- El antivirus de archivos, al encontrar un objeto potencialmente peligroso, debe:
  - Preguntar qué hacer, o;
  - Bloquear el acceso al objeto;
  - Borrar el objeto o intentar desinfectarlo (de acuerdo con la configuración preestablecida por el administrador);
  - Caso positivo de desinfección:
  - Restaurar el objeto para uso;
  - Caso negativo de desinfección:
  - Mover para cuarentena o borrar (de acuerdo con la configuración preestablecida por el administrador);
  - Con anterioridad a cualquier intento de desinfección o exclusión permanente, el antivirus debe realizar un respaldo del objeto.
  - Capacidad de verificar enlaces introducidos en correos electrónicos contra pishings.
  - En la verificación de tráfico web, en caso de que se encuentre código malicioso el programa debe:
    - Preguntar qué hacer, o;
    - Bloquear el acceso al objeto y mostrar un mensaje sobre el bloqueo, o;
    - Permitir acceso al objeto;
  - Posibilidad de agregar sitios de la web en una lista de exclusión, donde no serán verificados por el antivirus de web.
  - Debe tener módulo que analice cada macro de VBA ejecutado, buscando por señales de actividad maliciosa.
  - Debe tener módulo de bloqueo de Phishing, con actualizaciones incluidas en las vacunas, obtenidas por Anti-Phishing Working Group (http://www.antiphishing.org/).
  - Capacidad de distinguir diferentes subnets y brindar opción de activar o no el firewall para una subnet específica;
  - Debe tener módulo para protección contra port scans y explotación de vulnerabilidades de software. La base de datos de análisis debe actualizarse conjuntamente con las vacunas.
  - El módulo de Firewall debe contener, como mínimo, dos conjuntos de reglas:
  - Filtrado de paquetes: donde el administrador podrá elegir puertas, protocolos o direcciones de conexión que serán bloqueadas/permitidas;
  - Debe tener módulo que habilite o no el funcionamiento de los siguientes dispositivos externos, como mínimo:
    - Discos de almacenamiento locales
    - Almacenamiento extraíble
    - Impresoras
    - CD/DVD
    - Drives de disquete
    - Modems

- Dispositivos de cinta
- Dispositivos multifuncionales
- Lectores de smart card
- Wi-Fi
- Adaptadores de red externos
- Dispositivos MP3 o smartphones
- Dispositivos Bluetooth

- Capacidad de limitar el acceso a sitios de internet por categoría, por contenido (video, audio, etc)
- Debe proporcionar protección residente para archivos (antispyware, antitrojano, antimalware, etc.) que verifique cualquier archivo creado, accedido o modificado;
- Debe contar con soportes a notificaciones.
- Las vacunas deben ser actualizadas por el fabricante y estar disponibles a los usuarios, como máximo cada hora, independientemente del nivel de las amenazas encontradas en el período (alto, medio o bajo).
- Capacidad de volver a la base de datos de la vacuna anterior.
- Capacidad de barrer la cuarentena automáticamente después de cada actualización de vacunas.
- Capacidad de agregar carpetas/archivos para una zona de exclusión, con el fin de excluirlos de la verificación. Capacidad, también, de agregar objetos a la lista de exclusión de acuerdo con el resultado del antivirus, (ej.:"Win32.Trojan.banker") para que cualquier objeto detectado con el resultado elegido sea ignorado;
- El antivirus de archivos, al encontrar un objeto potencialmente peligroso, debe:
  - Preguntar qué hacer, o;
  - Bloquear el acceso al objeto;
    - Borrar el objeto o intentar desinfectarlo (de acuerdo con la configuración preestablecida por el administrador);
    - Caso positivo de desinfección:
      - Restaurar el objeto para uso;
    - Caso negativo de desinfección:
      - Mover para cuarentena o borrar (de acuerdo con la configuración preestablecida por el administrador);
- Anteriormente a cualquier intento de desinfección o exclusión permanente, el antivirus debe realizar un respaldo del objeto;
- Capacidad de verificar archivos de formato de correo electrónico;
- Posibilidad de trabajar con el producto por la línea de comando, con como mínimo opciones para actualizar las vacunas, iniciar un barrido, para el antivirus e iniciar el antivirus por la línea de comando;

Servidores Windows –

- Compatibilidad:
  - Microsoft Windows Server 2019 o superior x86/x64
  - Microsoft Windows Server 2016 x86/x64
  - Microsoft Windows Small Business Server 2011 Essentials/Standard x64
  - Microsoft Windows Server 2008 Standard/Enterprise/Datacenter SP1 x86/x64
  - Microsoft Windows Server 2008 Core Standard/Enterprise/Datacenter SP1 x86/x64
  - Microsoft Windows Server 2008 R2 Standard/Enterprise/Datacenter SP1
  - Microsoft Windows Server 2008 R2 Core Standard/Enterprise/Datacenter SP1
  - Microsoft Windows Server 2012 Foundation/Essentials/Standard x64
  - Microsoft Windows Server 2012 R2 Standard x64
  - Microsoft Windows Hyper-V Server 2008 R2 SP1
  - Microsoft Windows Hyper-V Server 2012
  - Microsoft Terminal basado en Windows Server 2008
  - Microsoft Terminal basado en Windows Server 2008 R2
- Características:
  - Debe proporcionar las siguientes protecciones:
    - Antivirus de archivos residente (antispyware, antitroyano, antimalware, etc.) que verifique cualquier archivo creado, accedido o modificado;
    - Autoprotección contra ataques a los servicios/procesos del antivirus
    - Control de vulnerabilidades de Windows y de los aplicativos instalados
  - Las vacunas deben ser actualizadas por el fabricante, como máximo, cada hora.
  - El módulo de Firewall debe contener, como mínimo, dos conjuntos de reglas:
    - Filtrado de paquetes: donde el administrador podrá elegir puertas, protocolos o direcciones de

			conexión que serán bloqueadas/permitidas; ▪ Filtrado por aplicativo: donde el administrador podrá elegir cuál aplicativo, grupo de aplicativo, fabricante de aplicativo, versión de aplicativo o nombre de aplicativo tendrá acceso a la red, con la posibilidad de elegir qué puertas y protocolos podrán ser utilizados. ▪ Capacidad de configurar niveles de verificación diferentes para cada carpeta, grupo de carpetas o archivos del servidor. ▪ Capacidad de bloquear acceso al servidor de máquinas infectadas y cuando una máquina intenta grabar un archivo infectado en el servidor. ▪ Capacidad de crear una lista de máquinas que nunca serán bloqueadas, aunque sean infectadas. ▪ Capacidad de detección de presencia de antivirus de otro fabricante que pueda causar incompatibilidad, bloqueando la instalación; ▪ Capacidad de pausar automáticamente barridos agendados en caso de que otros aplicativos necesiten más recursos de memoria o procesamiento; ▪ Capacidad de verificar archivos por contenido, o sea, únicamente verificará el archivo si es pasible de infección. El antivirus debe analizar la información de encabezado del archivo para tomar o no esa decisión a partir de la extensión del archivo; ▪ Capacidad de verificar objetos usando heurística; ▪ Capacidad de pausar automáticamente la verificación cuando se inicie un aplicativo; ▪ El antivirus de archivos, al encontrar un objeto potencialmente peligroso, debe: ▪ Preguntar qué hacer, o; ▪ Bloquear el acceso al objeto; ▪ Borrar el objeto o intentar desinfectarlo (de acuerdo con la configuración preestablecida por el administrador); ▪ Caso positivo de desinfección: 1. Restaurar el objeto para uso; ▪ Caso negativo de desinfección: 1. Mover para cuarentena o borrar (de acuerdo con la configuración preestablecida por el administrador); ▪ Anteriormente a cualquier intento de desinfección o exclusión permanente, el antivirus debe realizar un respaldo del objeto. Tiempo validez de las licencias (12 meses)	
		2	**CAPACITACIÓN DE SOFTWARE DE ANTIVIRUS** Se requiere que el contratista realice capacitación del antivirus a suministrar (tanto para las 800 licencias de sistema operativo Windows. La capacitación se debe realizar en las oficinas de la Dirección TIC de la gobernación, y será dirigida al personal técnico de sistemas. za capacitación debe abarcar las siguientes temáticas: • Introducción al antivirus a suministrar • Mecanismo de instalación, configuración y parametrización segura de antivirus • Identificación de ataques y vulnerabilidades • Administración de ambientes • Protección contra amenazas basada en Aprendizaje automático (Machine Learning – ML) • Protección de datos • Capacidad de instalar la solución de seguridad en smartphones y tablets Android, IOS • Creación de perfiles • Configuración de seguridad y protección para correos electrónicos • Capacidad Control de funciones y Control web • Activación de Cloud • Políticas y configuraciones	1
		3	**SOPORTE Y ASISTENCIA TÉCNICA DE SOFTWARE DE ANTIVIRUS POR UN (1) AÑO** Se requiere que el contratista ofrezca el servicio de soporte y asistencia técnica del software antivirus a suministrar El servicio de soporte y asistencia técnica debe contar con las siguientes características:	1 año	

	• Jornadas de asistencia técnica de revisión preventiva cada tres (3) meses. • Soporte técnico por problemas técnicos. • Habilitación de Help Desk sobre las demandas más comunes de los usuarios, el cual debe contener un centro de ayuda (documento) donde los usuarios encuentran asistencia sobre las funcionalidades y módulos del antivirus a suministrar. • Posibilidad de ofrecer el servicio de soporte y asistencia técnica habilitado con múltiples canales. • Atención las expectativas del personal de la dirección TIC con respecto a la experiencia. Tiempo validez de soporte y asistencia técnica (12 meses).
VALOR	El valor del contrato es hasta por la suma de **OCHENTA Y SIETE MILLONES QUINIENTOS SETENTA MIL PESOS M/CTE LEGAL COLOMBIANA ($87.570.000)** Incluido IVA, y demás tasas, contribuciones e impuestos a que haya lugar para la legalización y ejecución del contrato, amparados bajo el Certificado de Disponibilidad Presupuestal No. 1637 del 29/11/2022, cuya Unidad ejecutora es la Dirección Logística, del presupuesto de la presente vigencia fiscal 2022.
FORMA DE PAGO	El Departamento, cancelará el valor del contrato en un solo pago del 100%, de acuerdo con los servicios efectivamente realizados, previa presentación de la factura respectiva, acompañada de la certificación del supervisor en donde consta el cumplimiento de los suministros facturados. Además, deberá entregar certificación original del cumplimiento en los pagos de los aportes a los sistemas de salud, riesgos profesionales, pensiones. Se verificará que el Contratista se encuentre al día con los aportes al Sistema Integral de Seguridad Social en Salud, Pensión y Riesgos Laborales, así como los propios del Sena, ICBF y Cajas de Compensación Familiar, siempre y cuando no se encuentre exento de este pago, según lo establecido en el artículo 25 de la Ley 1607 de 2012, de acuerdo con las obligaciones que por este concepto deba cumplir. Si se encuentra exento del pago en los términos de la precitada ley, deberá manifestarlo en forma expresa Todos los pagos estarán sujetos al Programa Anual Mensualizado de Caja - PAC y al cumplimiento de los procedimientos presupuestales. El pago lo realizará la tesorería, con abono en cuenta al Contratista adjudicado, previo cumplimiento de los requisitos descritos anteriormente. El Departamento no se responsabilizará por la demora en el pago al CONTRATISTA, cuando ella fuere provocada por encontrarse incompleta la documentación que sirva de soporte para el trámite de las facturas y no se ajuste a cualquiera de las condiciones establecidas en el presente contrato. El Contratista debe indicar el número de cuenta activa y el nombre del titular de la misma en donde el DEPARTAMENTO consignará los respectivos pagos, asimismo indicar en la facturación que presente, el régimen tributario que lo regula. Se deberá realizar el pago de los impuestos departamentales, para la presentación de las cuentas de cobro del contrato así: ESTAMPILLA PRODESARROLLO: 2 % sobre el valor del contrato ESTAMPILLA PROCULTURA: 2 % sobre el valor del contrato ESTAMPILLA UNIVERSIDAD DE CARTAGENA: 1% sobre el valor del contrato ESTAMPILLA CONTRIBUCION 1% sobre el valor del contrato ESTAMPILLA PROANCIANATO: 3% sobre el valor del contrato **Se aclara que es responsabilidad de cada interesado en participar, verificar los anteriores impuestos, y la existencia de**

	otros, en la Secretaría de Hacienda de la entidad, con el propósito de tenerlo en cuenta dentro de su propuesta económica.
PLAZO DE EJECUCIÓN	El plazo de ejecución del contrato, atendiendo la naturaleza del servicio, será hasta el 31 de diciembre de 2022 o hasta agotarse el presupuesto asignado para esta contratación, lo primero que ocurra. Contados a partir del cumplimiento de los requisitos de perfeccionamiento y ejecución del mismo, esto es, suscripción del contrato por la partes en la Plataforma Secop II y expedición del registro presupuestal y aprobación de la garantía única de cumplimiento
OBLIGACIONES GENERALES DEL CONTRATISTA:	a) Especificaciones requeridas, el alcance de su objeto, y con las normas de calidad de este tipo de servicio. b) Ejecutar el objeto del contrato por su cuenta y riesgo, asumiendo todas las implicaciones que se requieran para el buen desarrollo del mismo. c) Mantener fijos los precios ofrecidos durante la ejecución del contrato. d) Cumplir con los compromisos adquiridos con la presentación de la oferta. e) Acatar las órdenes del supervisor, darle relevancia a la puntualidad y oportunidad. f) Sufragar los gastos que se ocasionen por razón de perfeccionamiento, legalización y ejecución del presente Contrato, entre estos, pago de impuestos, entrega de los bienes objeto del contrato, etc. g) Obrar con lealtad y buena fe en la ejecución del contrato. h) Guardar la reserva que se requiera de la información que maneje en virtud del contrato. i) El proponente deberá acreditar que se encuentra al día en el pago de aportes parafiscales relativos al sistema de seguridad social integral (certificados o documentos que acrediten encontrarse al día con el pago de aportes a salud, pensiones y riesgos laborales). Así como los propios del SENA, ICBF y LAS CAJAS DE COMPENSACIÓN FAMILIAR, cuando corresponda, Certificado de Existencia y Representación Legal de la Cámara de Comercio, NIT, Documentos del Representante Legal: fotocopia Cedula de Ciudadanía, Certificados Disciplinarios y Fiscales expedidos por la Procuraduría General de la Nación y la Contraloría General de la República, respectivamente. j) Las demás inherentes y conexas que se desprendan del objeto contractual.
OBLIGACIONES ESPECÍFICAS DEL CONTRATISTA	• Entregar bienes y/o servicios que se encuentran relacionados en el estudio previo de acuerdo a las características exigidas y ofertadas. • Garantizar que los elementos entregados cumplan con los estándares de cantidad y calidad dados para cada producto. • Brindar garantía y soporte de 1 año. • Cumplir con el objeto contratado. • Asumir los costos de transporte y medios para cumplir con la entrega. • Presentar junto con la factura o cuenta de cobro los soportes exigidos.

<table>
<tr><td></td><td>

- Mantener fijo el precio ofrecido en la propuesta durante la ejecución del contrato.
- Reportar de manera inmediata cualquier novedad o anomalía al supervisor del contrato.
- Cuando el supervisor del contrato lo solicite, en cualquier tiempo y durante la ejecución del contrato, allegar las certificaciones expedidas por el revisor fiscal o representante legal, según el caso, de acuerdo con lo ordenado en el artículo 50 de la Ley 789 de 2002 y demás normas concordantes. además, se debe aportar del revisor fiscal la copia de la cedula y tarjeta profesional.
- Presentar dentro de la propuesta del oferente las acciones a realizar para cumplir con los Requisitos de Calidad descritos en el numeral 3.1 DESCRIPCIÓN TÉCNICA DEL SERVICIO, del presente proceso de selección.
- Certificado soporte y apoyo técnico.

</td></tr>
<tr><td>OBLIGACIONES DEL DEPARTAMENTO DE BOLÍVAR:</td><td>

1. Adelantar los trámites y cumplir con los requisitos para la ejecución del contrato.
2. Realizar la Supervisión del contrato.
3. Realizar los pagos con el que se obliga en calidad de contratante.
4. Suscribir la correspondiente acta de liquidación a la terminación del contrato de conformidad con las normas vigentes.
5. Las demás relacionadas con el objeto y naturaleza del presente contrato y garantice el cabal y oportuno cumplimiento del contrato, de acuerdo con las normas vigentes y concordantes**.**

</td></tr>
<tr><td>GARANTIA UNICA</td><td>

Para el presente caso, según el Decreto reglamentario No 1082 de 2015, "Artículo 87. Garantías. La entidad estatal es libre de exigir o no garantías en el proceso de selección de mínima cuantía y en la adquisición en grandes superficies. Por lo tanto se considera necesario solicitar las siguientes garantías necesarias teniendo en cuenta las exigencias en que se prestará el servicio y los riesgos antes analizados.

<table>
<tr><th>Amparo</th><th>Vigencia</th><th>Valor Asegurado</th></tr>
<tr><td>Cumplimiento general del contrato y el pago de las multas y la cláusula penal pecuniaria que se le impongan</td><td>Por el término de ejecución del contrato y cuatro (04) meses más.</td><td>Diez por ciento(10%) del Valor del contrato.</td></tr>
<tr><td>Pago de salarios,prestaciones socialeslegales e indemnizaciones laborales del personal que el contratista haya de utilizar en el territorio nacional para la ejecucióndel contrato</td><td>Con una vigencia igual al término de duración del contrato y tres (3) años más.</td><td>Cinco por ciento (5%) del Valor del contrato</td></tr>
<tr><td>Calidad del servicio por los perjuicios derivados dela deficiente calidad del servicio prestado.</td><td>Con una vigencia igual al plazo del mismo, el término señalado por el ofertante en su propuesta en relación con la garantía de calidad y cuatro (4) meses más</td><td>20% del valor totaldel contrato</td></tr>
</table>

</td></tr>
<tr><td>OTRAS ESTIPULACIONES</td><td>

PENAL PECUNIARIA: En caso de incumplimiento total por parte del **CONTRATISTA, EL Departamento** cobrará como indemnización una suma equivalente al diez por ciento (10%) del valor total del contrato a título de pena, sin que por ello quede afectado el derecho de la Entidad a cobrar integralmente el valor de lo debido que no haya quedado satisfecho con el diez por ciento (10%) anterior, y de todos los perjuicios que pudieran ocasionarse como consecuencia del incumplimiento. En caso de incumplimiento parcial la pena se rebajará proporcionalmente en relación con la tasación del

</td></tr>
</table>

	incumplimiento. **EL DEPARTAMENTO** podrá descontar y tomar directamente el valor que resultare a cargo del **CONTRATISTA** por este concepto, de cualquier suma que se le adeude al **CONTRATISTA,** en razón del contrato. Si lo anterior no fuera posible, la Entidad cobrará la pena pecuniaria por vía de la Jurisdicción Coactiva conforme a la Ley. Lo anterior sin perjuicio del derecho que conservará el Departamento de aceptar el cumplimiento tardío de la obligación, simultáneamente con el cobro de la cláusula penal, cuando ello sea el caso. **MULTAS:** En caso de incumplimiento parcial de las obligaciones contractuales por parte del **CONTRATISTA,** y como acto independiente de la cláusula penal pecuniaria, si a ello hubiere lugar, **El Departamento** impondrá multas diarias equivalentes al uno por ciento (1%) del valor total del contrato, sin que el total de las mismas exceda el diez por ciento (10%) del valor total del mismo. Las multas se aplicarán de conformidad con las Leyes 1150 de 2007, 1474 de 2011, el Decreto 1082 de 2015. **INDEMNIDAD:** Quien sea seleccionado como contratista, mantendrá indemne a la Entidad Estatal de cualquier daño o perjuicio originado en reclamaciones de terceros y que se deriven de sus actuaciones o de las de sus subcontratistas o dependientes. En todo caso, en el evento en que se presente reclamación, la entidad así lo hará saber al contratista a efecto de que tomen las medidas en salvaguarda de la indemnidad señalada, pudiendo en todo caso descontar de manera directa de las sumas adeudadas, los conceptos y valores para conservar la indemnidad del Departamento.
SUPERVISOR	Dentro de las funciones principales del funcionario de vigilancia y coordinación están las de: 1) Realizar vigilancia, control y seguimiento a las actividades contenidas en el objeto del Contrato. 2) Revisar y Avalar los informes. 3) Revisar y aprobar las cuentas que presente el contratista de acuerdo con lo estipulado en la futura Carta de aceptación y en la invitación pública. 4) Proyectar y firmar el acta de inicio, y liquidación final del contrato y 5) Las demás acciones que correspondan al ejercicio propio de las funciones de encomendadas. Datos del Supervisor: RUDY JOEL NIETO Cargo : DIRECTOR TIC

Que, con la publicación de esta comunicación en el SECOP el oferente **PC STORE IT SOLUCIONES Y SERVICIOS S.A.S. SIGLA PC STORE IT S.A.S.** identificado con NIT: 900.872.496-5, representada legalmente por **CARLOS ALBERTO COGOLLO ARISTIZABAL**, identificad con la cedula de ciudadanía número 10.769.850, expedida en Montería, se entiende notificado de la Aceptación de su oferta.

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 **CONTRATAR LA RENOVACIÓN DE LICENCIA DE SOFTWARE ANTIVIRUS BITDEFENDER, CON ACTUALIZACION, SOPORTE, CAPACITACION Y ASISTENCIA TECNICA POR EL TERMINO DE UN AÑO, PARA LAS ESTACIONES DE TRABAJO Y SERVIDORES DE LA PLATAFORMA TECNOLOGICA DE LA GOBERNACION DE BOLIVAR,** el cual, a partir de la fecha, queda numerado de la siguiente manera: **MC-DAL-036-2022.**

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.
Dado en Turbaco- Bolívar, a los 29 días del mes de Diciembre de 2022.

KAREN MATOREL BELLO
DIRECTORA LOGISTICA

JOSÉ LUIS VERGARA MARTÍNEZ
Profesional Universitario
Dirección Administrativa Logística
Departamento de Bolívar
proyecto