CLAUSULAS ADICIONALES A LA MINUTA ELECTRÓNICA CONTRATO DE PRESTACIÓN DE SERVICIOS CO1.PCCNTR.9446631 - 2026	
CONTRATANTE	**ROBERTO JOSÉ RAVE RÍOS**, mayor de edad, identificado con C.C. No. 1.037.590.515 de Envigado – Antioquia, nombrado mediante Decreto No. 2024079903316 del 26 de julio de 2024 expedido por la Gobernación de Antioquia, quien en su calidad de Director, actúa en nombre y representación legal del **INSTITUTO DE CULTURA Y PATRIMONIO DE ANTIOQUIA** identificado con NIT 900.425.129-0, entidad descentralizada del orden Departamental, creada por el Decreto Ordenanzal número 0494 del 28 de febrero de 2011, modificado por los Decretos Ordenanzales número 02120 y 02132 de 2011, debidamente facultado para contratar en concordancia con las Leyes 80 de 1993 y 1150 de 2007 y sus respectivos decretos reglamentarios, y quien para efectos del presente acto se denominará el I**NTITUTO**;
CONTRATISTA	**ANDRES FERNANDO ECHEVERRY MARIN,** mayor de edad, identificada con cédula de ciudadanía No. **71.769.987** de Medellín (Antioquia), en calidad de representante legal de **INNOVART IT S.A.S** identificado con NIT. **900.662.158-1**, facultado para suscribir contratos de conformidad con el Certificado de Existencia y Representación Legal, quien para los efectos del presente contrato se denominará el **CONTRATISTA**;
hemos convenido suscribir **CONTRATO**, fundamentados en la Ley 80 de 1993, Ley 1150 de 2007, el proceso de selección bajo la modalidad de selección abreviada mediante subasta inversa electrónica **S.I 015 -2026** y la Resolución de adjudicación No. 138 de 2026, el cual se regirá por las condiciones establecidas en la Minuta Electrónica CO1.PCCNTR.9446631 - 2026 y por las siguientes **CLAUSULAS ADICIONALES** a la Minuta Electrónica diligenciada en **SECOP II**:	

1.1. PRIMERA. OBJETO: Adquisición e implementación de soluciones tecnológicas, Incluye la compra de bienes tecnológicos (hardware y software), así como el diseño y ejecución de un Plan Integral de Respaldo (inmutable) y Recuperación ante Desastres Informáticos, con mecanismos de réplica en la nube para garantizar la continuidad del servicio y la protección de la información institucional, este se enmarca dentro del proceso de modernización tecnológica del Instituto de Cultura y Patrimonio de Antioquia, orientado a fortalecer la infraestructura digital, optimizar la gestión de datos, mejorar la seguridad informática y asegurar la disponibilidad de los sistemas críticos frente a contingencias. **SEGUNDA. VALOR:** El valor total del presente contrato se estipula en **DOSCIENTOS NOVENTA Y UNO MILLONES SETECIENTOS CUARENTA Y DOS PESOS ($291.742.000,00) IVA INCLUIDO**, con cargo Certificado de Disponibilidad presupuestal No. 051 del 17 de febrero de 2026. **TERCERA. FONDOS Y APROPIACIONES PRESUPUESTALES Y CUANTIA DE LOS RECURSOS A ADMINISTRAR:** Los gastos que impliquen el cumplimiento del presente contrato para el INSTITUTO, se hacen con cargo a los siguientes fondos y apropiaciones presupuestales:

AGREGADO	SUBAGREGADO	RUBRO		PPTO OFICIAL
		CODIGO	NOMBRE	
FUNCIONAMIENTO	Maquinaria de oficina, contabilidad e informática	999999-0-1010-C99999-999992-99999299-2.1.2.01.01.003.03.02.00-999999999-21201010030302	Maquinaria de informática y sus partes, piezas y accesorios	$291,742,000
TOTAL				**$291,742,000**

CUARTA. FORMA DE PAGO: El Instituto de Cultura y Patrimonio de Antioquia pagará al contratista el valor del presente contrato mediante un pago único del 100%, sobre el servicio

contratado a partir de la firma del contrato y recibido a entera satisfacción por parte del supervisor y/o interventor del contrato, el informe completo y plan de trabajo según las necesidades según el objeto, así como la acreditación de los pagos realizados por concepto de aportes parafiscales y de seguridad social. De las cuentas de cobro o facturas que se originen en el presente contrato, al CONTRATISTA se le harán todas las deducciones establecidas por la Ley, **incluyendo Estampillas Departamentales del 4.8% y Tasa Prodeporte y Recreación del 2.5%.** La factura debe expedirse a nombre del INSTITUTO DE CULTURA Y PATRIMONIO DE ANTIOQUIA, NIT 900.425.129-0 y cumplir con todos los requisitos de facturación establecidos en el Estatuto Tributario. **QUINTA. PLAZO:** Tres (3) meses, contados a partir de la suscripción del acta de inicio. El plazo establecido no podrá superar la vigencia fiscal de 2026, de conformidad con el principio de anualidad del estatuto orgánico de presupuesto. **SEXTA OBLIGACIONES DEL INSTITUTO:** El INSTITUTO se compromete a lo siguiente:6.1. Designar un supervisor y/o interventor para que realice las funciones de control, supervisión y vigilancia del cumplimiento de las obligaciones a cargo del contratista. 6.2.Vigilar y verificar el cumplimiento por parte del contratista, de sus obligaciones con el Sistema de Seguridad Social Integral, conforme al artículo 50 de la Ley 789 de 2002 y la Ley 1150 de 2007. 6.3. Pagar oportunamente el valor del contrato de acuerdo con la forma de pago estipulada, previa presentación del recibo a satisfacción por parte del supervisor y/o interventor. 6.4. Suministrar la información necesaria relacionada con el cumplimiento de las especificaciones técnicas requeridas. 6.5.Prestar apoyo en las actividades, eventos y servicios organizados en desarrollo del objeto contractual. **SÉPTIMA. OBLIGACIONES DE EL CONTRATISTA:** El CONTRATISTA se obliga a: 7.1. Cumplir a cabalidad todas y cada una de las especificaciones técnicas descritas en el presente estudio previo. 7.2. Entregar e instalar los bienes objeto del presente proceso, en el Palacio de Cultura Rafael Uribe, ubicado en la Carrera 51 N° 52 - 03 de la ciudad de Medellín, dentro del plazo y las condiciones establecidas. 7.3. Efectuar los cambios de los elementos por reclamos de mala calidad, defectos de fabricación, defectos por mal empaque o embalaje, que en todo caso sean responsabilidad del contratista, previos los soportes y sustentación respectiva sin importar que inicialmente se haya expedido el recibo a satisfacción. 7.4. Garantizar que los equipos que sean adquiridos por la entidad sean originales de acuerdo con la marca, modelo y tipo de elemento ofertado. En todo caso se podrá exigir capacitación e instalación del elemento adquirido. 7.5. Responder por la perdida, daño o deterioro que se pueda generar

durante el transporte, entrega o instalación de los equipos. 7.6. Presentar certificado de garantía de cada uno de los equipos cumpliendo con el tiempo señalado en las especificaciones técnicas. 7.7. Cumplir con las demás obligaciones establecidas en la Ley 1480 de 2011, Estatuto del Consumidor. 7.8. Facilitar la labor de supervisión y/o interventoría dando respuesta oportuna a las observaciones o requerimientos que se realicen. 7.9. Informar oportunamente al contratante cuando exista o sobrevenga alguna de las inhabilidades e incompatibilidades previstas en la Constitución y la ley. 7.10. Realizar los pagos correspondientes al sistema de seguridad social en salud y pensiones, así como a riesgos profesionales de sus empleados. 7.11. Realizar dentro de los tres (3) días siguientes a la suscripción del contrato las gestiones necesarias para el cumplimiento de los requisitos de ejecución del contrato, así como de sus modificaciones, adiciones o prorrogas y asumir los costos de éstas. 7.12. Se debe contar con personal idóneo, para realizar la configuración y puesta en marcha de los dispositivos a instalar, acorde con lo exigido en las especificaciones técnicas:

2.1 ESPECIFICACIONES TÉCNICAS

8. Paquete de actualización de Arcserve software por 1 año y su respectiva configuración y soporte posventa.

ESPECIFICACIONES TÉCNICAS REQUERIDAS[4]		
ÍTEM		**CARACTERÍSTICA MÍNIMA**
1. DESCRIPCIÓN DEL EQUIPO		
1.1	Marca	Plataforma ArcServe
1.2	Modelo de referencia	UDP y HA
1.3	Línea	UDP y HA
2. SERVICIOS		

[4] El licenciamiento fue adquirido mediante proceso de selección por el INSTITUTO DE CULTURA Y PATRIMONIO DE ANTIOQUIA en el año 2018 (ARCSERVE) la cual es nuestra plataforma de BACKUPs inteligente y de Seguridad de la información, a efectos de no realizar migración dado que esto no es conveniente para la continuidad del negocio por la cantidad de datos, y aclarando que esta no es una plataforma en la nube, es una plataforma ONSITE del INSTITUTO y en la cual se ha invertido desde del 2018 una suma considerable (Consta de Hardware y Software) y estar acorde a los lineamiento de MITIC.

- Ofrecer la opción de administración centralizada de varios sitios a través de comunicación WAN/NAT, de forma que sea posible administrar los nodos protegidos, destinos de backup y planes de protección de forma remota.
- Poseer un panel de administración web del entorno de backup con soporte para visualización del estado de todas las tareas de backup, con la opción de generar informes online y enviarlos por correo electrónico.
- Configurar un módulo de autenticación integrado a Active Directory, con la posibilidad de crear diferentes perfiles de acceso, y especificar los permisos y privilegios de cada usuario que operará la solución.
- Configurar una aplicación para descarga e instalación de actualizaciones del producto, de forma manual, programada o sin intervención del administrador.
- Configurar una interfaz de administración a través de línea de comando, para la integración con herramientas de programación y automatización de terceros.
- Realizar backups a través de tecnología de imagen (snapshot) de servidores físicos y virtuales, con soporte para los sistemas operativos mencionados en los puntos 1.2, 1.3 y 1.4, efectuando la copia completa de volúmenes, incluida información como sistemas operativos, aplicaciones, datos y configuración de estos.
- Realizar backups a nivel de archivos o directorios a partir de redes compartidas basadas en protocolos CIFS o SMB.
- Permitir la ejecución del backup de archivos abiertos, aún si son modificados durante el backup, sin necesidad de suspender la utilización de las aplicaciones por parte de los usuarios ni tener una conexión de red. La copia del archivo guardado deberá ser idéntica al archivo en el disco al inicio de la operación de backup.
- Integrar la tecnología VSS (Volume Shadowcopy Service) de Windows para realizar copias y garantizar la consistencia de cualquier aplicación que cuente con un VSS Writer en estado funcional durante la ejecución del backup.
- Integrar Exchange Online (Office 365) de forma que sea posible realizar la protección y el almacenamiento del contenido de las casillas de correo alojadas en ese servicio en el repositorio de backup local, ofreciendo posteriormente al menos las siguientes opciones de recuperación granular:
  - Mensajes
  - Elementos del calendario y compromisos
  - Tareas
  - Contactos
  - Elementos de carpetas públicas
  - Elementos archivados
  - Objetos recuperables (In-place Hold y Litigation Hold)
- Configurar tecnología de backups de imagen (snapshots) incrementales, permitiendo que, luego del primer backup completo, únicamente se copien los bloques nuevos o modificados en los volúmenes protegidos. Esos incrementos deben ser realizados por tiempo indeterminado, lo que evita tener que realizar nuevos backups completos.
- Disponer de tecnología de backups incrementales para datos en redes compartidas y en casillas de correo de Exchange Online (Office 365) permitiendo que, luego del primer backup completo, únicamente se copien los archivos/elementos nuevos o modificados. Esos incrementos deben ser realizados por tiempo indeterminado, lo que evita tener que realizar nuevos backups completos.
- Permitir la programación de backups con una frecuencia de, al menos, 15 en 15 minutos.
- Configurar la capacidad de programación avanzada, con la posibilidad de utilizar frecuencias diferentes en determinadas ventanas de horarios dentro de una misma tarea de backup, realizando backups más frecuentes durante el día y más espaciados durante la madrugada, por ejemplo.

- Disponer de un servidor de administración de los puntos de recuperación, con las siguientes características:
- Posibilidad de creación de diversos Data Stores dentro de un mismo servidor para la segmentación lógica de los backups en diferentes carpetas o volúmenes.
- Centralización de las tareas de generación de catálogos y combinación de puntos de recuperación que hayan superado el período de retención determinado en el plan de protección de datos.
- Funcionalidades de deduplicación global de datos, compresión y cifrado a nivel de Data Store.
- Configurar tecnología de deduplicación de datos nativa del software, sin necesidad de hardware específico para este fin, contemplando las siguientes características:
- Realización de la deduplicación de datos en el agente de backup o en el servidor proxy, permitiendo únicamente el tránsito de los bloques de datos únicos a través de la red.
- Deduplicación global de datos entre todos los puntos de recuperación almacenados en un mismo Data Store, de forma que cualquier bloque de datos ya almacenado anteriormente por un servidor protegido no sea enviado nuevamente por los demás agentes durante la ejecución de los backups.
- Posibilidad de determinar el tamaño de los bloques durante la deduplicación de datos.
- Configurar tecnología de replicación de puntos de recuperación nativa del software, sin necesidad de hardware específico para este fin, contemplando las siguientes características:
- Replicación de puntos de recuperación entre diferentes Data Stores y servidores de administración de puntos de recuperación.
- Posibilidad de replicación inmediata luego de la ejecución de cada backup o en intervalos programados.
- Posibilidad de control del consumo de ancho de banda para la replicación, incluidos los ajustes por día de la semana y las ventanas de horario.
- Utilización de la tecnología de deduplicación de datos durante el proceso de replicación, realizando la comparación del contenido del Data Store de origen y del de destino, y moviendo por la red únicamente los bloques que no existen en el destino.
- Replicación optimizada para redes WAN/NAT a través de tunelización HTTP.
- Posibilidad de replicación de un origen para varios destinos diferentes.
- Posibilidad de replicación y consolidación de datos de varios orígenes para un mismo destino central.
- Posibilidad de retomar la replicación desde el punto donde se vio interrumpida debido a una pérdida de comunicación entre origen y destino.
- Posibilidad de exportar el contenido de un Data Store en un medio extraíble, posibilitando el transporte físico de los datos hasta el destino para la sincronización sin conexión. Después de esta sincronización inicial, la replicación deberá enviar únicamente los bloques únicos que no existen en el Data Store de destino.
- Posibilidad de aplicar diferentes políticas de retención de datos en los Data Stores de origen y destino durante el proceso de replicación.
- Configurar funcionalidad de copia de archivos luego de la tarea de backup, contando con las siguientes características:
- Selección de archivos y carpetas a ser copiados y aplicación de filtros para localizar archivos con tipos o atributos específicos.
- Posibilidad de copia de los archivos seleccionados en un disco local, disco extraíble o red compartida.
- Posibilidad de copia de los archivos seleccionados en nubes públicas, con soporte para Amazon S3 y Windows Azure Blob Storage.
- Cifrado de los datos copiados mediante AES de 128 bits o 256 bits.

- Disponer de recurso de archivado ("archiving") que permita excluir los archivos de origen al finalizar la copia para lograr un almacenamiento de más bajo costo, de acuerdo con los criterios de antigüedad, fecha de acceso, fecha de modificación, tamaño o tipo de archivo. Luego de la exclusión, se debe mantener un archivo del mismo nombre en la ubicación original, que contenga instrucciones para la recuperación del mismo en caso de que el usuario tenga que acceder a él.
- A partir de cualquier backup realizado, ya sea completo o incremental, se debe contar con las siguientes opciones de restauración de datos:
- Restaurar cualquier archivo o carpeta del servidor en cuestión, aún si ese archivo no fue modificado en la fecha en que se realizó el backup.
- Restaurar bases de datos de Microsoft SQL Server 2005, 2008, 2008 R2, 2012, 2014 y 2016.
- Restaurar bases de datos de Microsoft Exchange Server 2007, 2010, 2013 y 2016.
- Restaurar individualmente, sin necesidad de restaurar toda la base de correo de Exchange, al menos los siguientes elementos:
  - Casillas de correo
  - Mensajes
  - Archivos adjuntos
  - Elementos del calendario y compromisos
  - Tareas
  - Contactos
  - Carpetas públicas
- Recuperar los elementos de Exchange para la casilla de correo original o para una casilla de correo alternativa, incluso en otro servidor Exchange, o exportar los mismos en un archivo .PST.
- Restaurar objetos o atributos de objetos de Microsoft Active Directory.
- Restaurar bases de datos Oracle, versiones 11g (R1/R2) y 12c, con las siguientes opciones de granularidad:
  - Base de datos completa (Tablespaces y control files)
  - Parameter File;
  - Redo Logs archivados
  - Tablespaces
  - Datafiles
  - System
  - Undo Tablespaces
  - Control Files
- Restaurar bases de datos Pervasive PSQL y MySQL
- Restaurar el sistema completo (Bare Metal Recovery), inclusive en un hardware diferente del original o en una máquina virtual, permitiendo recuperar un servidor completo en caso de desastres, sin necesidad de reinstalar de forma manual el sistema operativo.
- Ofrecer funcionalidad de "standby virtual" para recuperación de desastres a través de tareas automáticas de conversión de los backups realizados en máquinas virtuales VMware o Hyper-V, copiándolas y registrándolas automáticamente en el hipervisor de destino, ya sea que esté en el sitio local o en un sitio remoto.
- Ofrecer funcionalidad de "máquina virtual instantánea" para la creación de máquinas virtuales directamente desde cualquier punto de recuperación almacenado en disco de forma inmediata, permitiendo iniciar un servidor rápidamente en caso de desastres sin que sea necesario copiar previamente los datos en el hipervisor de destino.
- Deberá permitir recuperar cualquier aplicación a nivel de objetos, en cualquier sistema operativo compatible, utilizando las propias herramientas de administración de las aplicaciones existentes.

- Permitir el montaje de puntos de recuperación como unidades de disco, de forma que sea posible acceder a su contenido inmediatamente a partir del repositorio de backup, sin necesidad de transferir datos.
- La integración con subsistemas de almacenamiento debe estar disponible, al menos, para los siguientes tipos de backup:
- Backup de servidores Windows a través de agentes.
- Backup de servidores virtuales en plataforma VMware, sin agentes.
- Backup de servidores virtuales en plataforma Hyper-V, sin agentes.
- Soporte para entornos virtualizados en la plataforma VMWare vSphere, debiendo:
- Brindar soporte para VMWare ESX/ESXi, vCenter Server y vCenter Server Appliance versiones 5.0, 5.1, 5.5, 6.0, 6.5.
- Permitir recuperar la máquina virtual completa en el host/datastore original o en un host/datastore alternativo, sin requerir la instalación de agentes dentro de las máquinas virtuales y con la opción de renombrar la máquina virtual durante la recuperación y alterar el tipo de disco empleado (Thick/Thin).
- Restaurar de forma granular, sin requerir la instalación de agentes dentro de las máquinas virtuales y a través de una única tarea de backup de snapshot, lo siguiente:
  - Archivos y directorios pertenecientes a Guest VM Windows y Linux.
  - Archivos y bases de datos de Microsoft Exchange pertenecientes a Guest VM Windows.
  - Elementos y objetos de Microsoft Exchange (mensajes, archivos adjuntos, compromisos, tareas, contactos y carpetas públicas) pertenecientes a Guest VM Windows.
  - Archivos y bases de datos de Microsoft SQL Server pertenecientes a Guest VM Windows.
  - Archivos, bases de datos y elementos de Microsoft SharePoint pertenecientes a Guest VM Windows.
  - Archivos y bases de datos de Pervasive PSQL pertenecientes a Guest VM Windows.
  - Archivos y bases de datos de Oracle pertenecientes a Guest VM Windows.
  - Archivos y bases de datos de MySQL pertenecientes a Guest VM Windows o Linux.
- En el caso de la restauración granular, no hay necesidad de restaurar una Guest VM entera.
- Permitir redireccionar la restauración de una Guest VM hacia una carpeta alternativa, otro datastore, host o red.
- Las tareas de backup y restauración deberán ser realizadas a través de la interfaz gráfica y sin necesidad de scripts.
- Integración con tecnología CBT (Changed Block Tracking) de VMware para identificar y copiar únicamente los bloques en uso de los discos virtuales (archivos. vmdk).
- Soporte para entornos virtualizados en la plataforma Microsoft Hyper-V, debiendo:
- Brindar soporte para Microsoft Hyper-V Server versiones 2008 R2, 2012, 2012 R2, 2016, 2019 y 2022.
- Brindar soporte para Hyper-V de Microsoft Windows Server, versiones 2008 R2, 2012 y 2012 R2, 2016, 2019 y 2022.
- Brindar soporte para clusters Hyper-V, incluyendo Cluster Shared Volumes (CSV), basados en Windows Server 2012, 2012 R2, 2016, 2019 y 2022
- Permitir recuperar la máquina virtual completa en el host/directorio original o en un host/directorio alternativo, sin requerir la instalación de agentes dentro de las máquinas virtuales y con la opción de renombrar la máquina virtual durante la recuperación y alterar el tipo de disco empleado (Fixed/Dynamic).
- Restaurar de forma granular, sin requerir agentes instalados dentro de las máquinas virtuales y a través de una única tarea de backup de snapshot, lo siguiente:
  - Archivos y directorios pertenecientes a Guest VM Windows y Linux.
  - Archivos y bases de datos de Microsoft Exchange pertenecientes a Guest VM Windows.
  - Elementos y objetos de Microsoft Exchange (mensajes, archivos adjuntos, compromisos, tareas, contactos y carpetas públicas) pertenecientes a Guest VM Windows.

Palacio de la Cultura Rafael Uribe Uribe. Carrera 51 #52-03 Medellín-Colombia
F:+57(4)2518461 / T:+57 (4) 3209780 / contacto@culturantioquia.gov.co / www.culturantioquia.gov.co
Nit 900.425.129-0 / Redes: @Culturantioquia

- Archivos y bases de datos de Microsoft SQL Server pertenecientes a Guest VM Windows.
- Archivos, bases de datos y elementos de Microsoft SharePoint pertenecientes a Guest VM Windows.
- Archivos y bases de datos de Pervasive PSQL pertenecientes a Guest VM Windows.
- Archivos y bases de datos de Oracle pertenecientes a Guest VM Windows.
- Archivos y bases de datos de MySQL pertenecientes a Guest VM Windows o Linux.
- En el caso de la restauración granular, no hay necesidad de restaurar una Guest VM entera.
- Permitir redireccionar la restauración de una Guest VM hacia una carpeta alternativa, otro host o red.
- Las tareas de backup y restauración deberán ser realizadas a través de la interfaz gráfica y sin necesidad de scripts.
- Disponer de tecnología CBT (Changed Block Tracking) propia para identificar y copiar únicamente los bloques en uso de los discos virtuales de VM de Microsoft Hyper-V (archivos .vhd/.vhdx).
- Permitir expandir y navegar el contenido de los backups realizados directamente por Windows Explorer, sin necesidad de operar la consola de administración de la solución para hacer una restauración de archivos y carpetas.
- Configurar el módulo nativo de cifrado, permitiendo elegir entre AES de 128 bits o de 256 bits.
- Permitir el envío automático de alertas por correo electrónico, al menos para los siguientes eventos:
- Falla de un procedimiento de backup o restauración.
- Éxito de un procedimiento de backup o restauración.
- Espacio disponible en el destino de los backups inferior a un valor predeterminado.
- Nuevas actualizaciones disponibles para su instalación.
- Uso de memoria, CPU, E/S de red o disco que supera los valores predeterminados.
- Permitir la automatización de diferentes tareas, como backup, copia de archivos, replicación de puntos de recuperación y standby virtual, dentro de un mismo plan de protección de datos, permitiendo crear diferentes estrategias de acuerdo con los objetivos de punto de recuperación y objetivos de tiempo de recuperación de cada servidor protegido.
- Disponer de funcionalidad para la realización de pruebas automatizadas de integridad de los backups, para eliminar la necesidad de restaurar los datos de forma manual periódicamente con el objetivo de validar la confiabilidad de los backups. Se deben ofrecer, al menos, los siguientes tipos de pruebas:
- Prueba de integridad y consistencia del sistema de archivos, a través de la verificación basada en la herramienta chkdsk.exe o un mecanismo similar.
- Prueba amplia de la imagen, a través de la inicialización de la misma como una máquina virtual en un entorno VMware o Hyper-V previamente especificado para esa finalidad. La creación de estas máquinas virtuales debe realizarse directamente desde cualquier punto de recuperación almacenado en disco de forma inmediata, sin que sea necesario copiar previamente los datos en el hipervisor de destino u ocupar cualquier espacio adicional en los discos del hipervisor.
- Se debe permitir la especificación de scripts personalizados para que se ejecuten durante las pruebas, de forma que sea posible ajustar los criterios de aprobación o falla de acuerdo con características específicas del entorno.
- Deberá permitir regular de forma dinámica y con parámetros la exigencia sobre los sistemas protegidos, de forma tal que se puedan definir límites de utilización del rendimiento en discos y/o en la red, para disminuir el impacto en la infraestructura de producción, durante las actividades de backup.
- Permitir dentro del software la definición de los SLA de recuperación (RTO, Recovery Time Objective – Objetivo de Tiempo de Recuperación) para los nodos o grupos de nodos protegidos.

Palacio de la Cultura Rafael Uribe Uribe. Carrera 51 #52-03 Medellín-Colombia
F:+57(4)2518461 / T:+57 (4) 3209780 / contacto@culturantioquia.gov.co / www.culturantioquia.gov.co
Nit 900.425.129-0 / Redes: @Culturantioquia

- La solución deberá disponer de informes integrados en su consola web, al menos con las siguientes opciones:
- Informe de tendencias del tamaño de los backups.
- Informe de distribución de los datos en los medios.
- Informes del estado de los backups.
- Informe de RPO (Recovery Point Objective – Objetivo de Punto de Recuperación).
- Informe de RTO (Recovery Time Objective – Objetivo de Tiempo de Recuperación).
- Informe de estado de las tareas, que incluye tiempo de ejecución, total de datos procesados y total ocupado en el disco.
- El esquema de la base de datos de la solución debe poseer documentación pública, de forma que sea posible elaborar informes personalizados directamente desde la base de datos o integrar soluciones de monitoreo de terceros.
- Soporte/garantía: los productos adquiridos deberán contemplar soporte/asistencia las 24 horas del día, los 7 días de la semana (24x7), por teléfono (central de 0800) a través de Internet/Web, por un período de garantía de hasta 36 (treinta y seis) meses.
- Configurar agentes remotos para sistemas Windows, Mac OS X, Linux y UNIX, con soporte para las siguientes versiones:
- Windows Server 2003, Windows Server 2008, Windows Server 2008 R2, Windows Server 2012, Windows 2012 R2, Windows Server 2016, Windows Server 2019, Windows Server 2022 Windows XP, Windows Vista, Windows 7, Windows 8, Windows 8.1 y Windows 10.
- Debian, Suse Linux Enterprise Server, Red Hat Enterprise Linux, CentOS y Oracle Enterprise Linux.
- Solaris SPARC y x64 versiones 8, 9, 10 y 11.
- IBM AIX (máquina física y LPAR) v5.2, v5.3, v6.1 y v7.1.
- HP-UX 11.23 y 11.31.
- Mac OS X 10.6.X, 10.7.X, 10.8.X y 10.9.X.
- Permitir la ejecución del backup de archivos abiertos en Windows, aún si son modificados durante el backup, sin necesidad de suspender la utilización de las aplicaciones por parte de los usuarios ni tener una conexión de red. La copia del archivo guardado deberá ser idéntica al archivo en el disco al inicio de la operación de backup.
- Ofrecer protección continua de datos para servidores de archivos a través de la tecnología de replicación de datos por bloque, integrada a la solución de backup.
- Configurar un agente remoto para Microsoft Exchange, debiendo:
- Ser compatible con Exchange 2003, 2007, 2010, 2013 y 2016.
- Restaurar casillas de correo individuales y mensajes específicos a través de una única tarea de backup de Information Store.
- Permitir redirigir la restauración a otro servidor de Exchange, así como a otra bandeja de entrada, en caso de que se restauran mensajes individuales.
- Configurar un agente remoto para Microsoft SharePoint, debiendo:
- Ser compatible con SharePoint Server y SharePoint Services.
- Restaurar documentos individuales, sitios, sitios secundarios, listas, elementos de listas y calendarios a través de una única tarea de backup, sin necesidad de restaurar toda la aplicación.
- Configurar un agente remoto para Active Directory, debiendo:
- Restaurar objetos y atributos específicos a través de una única tarea de backup, sin necesidad de realizar una restauración completa de los modos autoritativos y no autoritativos de Windows. La restauración de los objetos y atributos no debe exigir que se reinicie el servidor Domain Controller.
- Configurar un agente remoto para Microsoft SQL Server, debiendo:

- Envío automático a la cinta del backup más reciente disponible en el disco, complementando el mismo caso, ya sea incremental o un backup deduplicado.
- Posibilidad de restaurar archivos y carpetas directamente desde la cinta, sin necesidad de recuperar la imagen completa del servidor.
- Posibilidad de restaurar la imagen completa de un determinado servidor de cinta en una ubicación en el disco, permitiendo la recuperación de este luego de un desastre.
- Soporte/garantía: los productos adquiridos deberán contemplar soporte/asistencia las 24 horas del día, los 7 días de la semana (24x7), por teléfono (central de 0800) a través de Internet/Web, por un período de garantía de hasta 36 (treinta y seis) meses.
- Configuración de características del módulo de replicación de archivos
- Compatibilidad del software de replicación con plataformas Windows Server 2003 y 2008, 2008 R2, 2012, 2012 R2, 2016, 2019 y 2022, de 32 y 64 bits.
- Compatibilidad del software de replicación con plataformas Red Hat Enterprise Linux 4.x a 7.x, CentOS 4.x a 7.x, SUSE Linux Enterprise Server 9 a 11 SP1 y Oracle Enterprise Linux 5.7-5.9 y 5.11, de 32 y 64 bits.
- Compatibilidad del software de replicación con las plataformas Unix relacionadas que se mencionan debajo:
- IBM AIX 5.3, 6.1 y 7.1.
- Sun Solaris 10, 11, 11.1 SPARC.
- Disponibilidad de una interfaz gráfica, que ofrezca acceso rápido a la información de soporte técnico, manuales online y asistentes.
- Tener una consola de visualización de las operaciones de replicación en modo gráfico, que permita administrar en tiempo real de los datos en tránsito y el estado de los servidores y aplicaciones.
- Permitir la administración también a través de líneas de comando.
- Ofrecer la posibilidad de simular una replicación sin necesidad de mover datos, permitiendo monitorear el porcentaje de alteración del entorno y otros datos relevantes para el cálculo del ancho de banda necesario.
- Poseer una interfaz web donde se proporciona información rápida sobre los escenarios de replicación, así como informes sobre las operaciones realizadas.
- Permitir la replicación de datos a través de redes locales (LAN) o remotas (WAN).
- Poseer la capacidad de dividir la replicación en varios flujos simultáneos, para optimizar la utilización de enlaces de comunicación que tengan alta latencia y oscilación.
- Permitir limitar el ancho de banda utilizado para la replicación, estipulando valores máximos de consumo por rangos de horario y día de la semana.
- Ofrecer soporte para la replicación de archivos y datos en sistemas operativos Microsoft Windows Server, Linux (Red Hat y Suse) o Unix (IBM AIX y Oracle Solaris).
- Permitir la replicación en las modalidades online (en tiempo real), programada o periódica.
- Permitir la sincronización entre servidores mediante los siguientes métodos:
- Sincronización de archivos, moviendo archivos enteros.
- Sincronización de volúmenes, moviendo todos los datos de los volúmenes de un servidor cuando se realiza una replicación del sistema completo.
- Sincronización de bloques, moviendo solamente los bloques modificados, lo cual es más adecuado para la replicación de bases de datos.
- Sincronización sin conexión, que permite realizar la copia a través de medios extraíbles sin tráfico en la red.
- Ofrecer soporte para la replicación de datos de instancias EC2 en la nube de Amazon.
- Realizar la replicación sin depender de almacenamientos externos y sin necesidad de usar hardware idéntico en los servidores de origen y de destino, siendo capaz de replicar datos de servidores físicos a físicos, físicos a virtuales, virtuales a virtuales y virtuales a físicos.
- Efectuar el cifrado de los datos en tránsito.

- Permitir el envío automático de eventos e información relevante sobre los escenarios de replicación mediante correo electrónico.
- Ser capaz de proteger el propio servicio de control sin necesidad de licencias adicionales, garantizando que se pueda acceder al mismo para administrar los escenarios de replicación, incluso en caso de fallas en uno de los servidores.
- Disponer de tecnología que permita probar el funcionamiento del entorno de réplica, iniciando y poniendo a disposición la aplicación sin afectar el entorno de producción y sin necesidad de efectuar una nueva sincronización después de las pruebas, retomando la replicación desde el punto donde la misma fue suspendida.
- Generar puntos de recuperación de forma automática o programada, manteniendo un registro de los últimos cambios efectuados en el servidor de réplica de forma que sea posible revertirlos si es necesario, ofreciendo una protección continua de la información (CDP).

La actualización del paquete de ArcServe debe habilitar 5 procesadores (sockets), y debe incluir en caso de ser necesario la reinstalación y configuración de la última versión del software y mantenimiento (BACKUPS) por 1 año.

9. **Renovación respaldo del repositorio ARCSERVE a la nube en almacenamiento del tipo inmutable y recuperación de todos los servidores del instituto en servidor externo a las instalaciones físicas del instituto.**

ESPECIFICACIONES TÉCNICAS REQUERIDAS		
ÍTEM		**CARACTERÍSTICA MÍNIMA**
1. DESCRIPCIÓN		
1.1	Marca	**ESPECIFICAR**
1.2	Línea	**ESPECIFICAR**
2. GARANTÍA		
2.1	Tipo de almacenamiento	inmutable
2.2	Tiempo	Mínimo Un (1) año
2.3	Almacenamiento mínimo en Nube	48 TB

Renovación del sistema de respaldo del repositorio de ARCSERVE a la nube en un almacenamiento inmutable debe tener las siguientes características:

- Tipo de Tecnología: Inmutable. Tecnología de almacenamiento de datos que permite escribir datos a un dispositivo de almacenamiento una sola vez y evita que se cambie.
- Debe tener una capa adicional de protección: que protege activos valiosos como propiedad intelectual y secretos comerciales de acceso no autorizado e infracciones potenciales de datos.
- Cumplimiento de regulación en modo Enterprise y Compliance.
- Protección activa de archivos.

- Protección de carpetas y archivos.
- Compatible con sistemas de archivos BTRFS y tecnología Copy-on-write de btrfs.
- Cheque de información por CRC32 checksum.
- Archivos de bloqueo de forma automática o manual. (Auto Lock).
- Al bloquear un archivo se debe poder establecer un período de retención, especificando cuánto tiempo debe permanecer bloqueado el archivo y qué tipo de estado encerrarlo para protegerlo contra modificaciones o eliminaciones.
- El Auto Lock Timer para calcular el tiempo de bloqueo basado en la actualización más reciente del archivo.
- Establecimiento de períodos de retención
- Los directorios de directorios y padres que contienen el archivo no pueden ser eliminados.
- Reloj tamper-per-Proof para el sistema inmutable.
- Integración con varios protocolos de archivos, tales como SMB, NFS, AFP, FTP, y WebDAV
- La recuperación de la información deberá ser inmediata en caso de ser necesario. No se deberá contar con tiempos superiores a pocos segundos.
- El tiempo de retención mínimo de la información deberá ser de al menos 36 meses
- La característica de la retención para las copias inmutables deberá ser de al menos 3 años para garantizar temas de compliance.
- Aunque el servicio sea prestado por 1 año, el instituto podrá solicitar copias de seguridad del repositorio de hasta 36 meses de antigüedad.
- El proveedor deberá garantizar una segunda copia en un lugar alterno separado del primero como mínimo unos 500 kilómetros.

El sistema de Backup externo deberá contar con una tecnología donde los datos viajen encriptados a través de un sistema IPsec que sea 100% compatible con el UTM con el que cuenta el Instituto. El sistema se deberá hacer a través de una conexión segura tipo Lan To Lan o similar con las siguientes características:

- Encriptación de extremo a extremo a nivel de túnel y a nivel de transporte
- Uso de cifrado tipo AES, Blowfish, Triple DES, ChaCha y DES-CBC.
- Uso de paquetes IKE e Ipsec
- Soporte de aceleración Criptográfica
- Encripción en modo túnel y en modo transporte

El sistema de recuperación de desastres de los servidores del instituto deberá ejecutarse como mínimo en un servidor con las siguientes características:

ESPECIFICACIONES TECNICAS REQUERIDAS		
ITEM		CARACTERISTICA MINIMA
1. DESCRIPCION DEL EQUIPO		
1.1	Marca	**ESPECIFICAR**
1.2	Modelo de referencia	**ESPECIFICAR**
1.3	Tipo de Chasis	Rack máximo de 2U (Dos Unidades de Rack)
2. PROCESAMIENTO		

2.1	Cantidad	Dos (2) procesadores
2.2	Procesador	Intel Xeon Gold
2.3	TDP	125 W
2.4	Tipo	Intel Xeon Gold 6152 o superior
2.5	Velocidad de procesamiento	2.1 GHz o superior
2.6	Catidad de Nucleos	20 o superior
2.7	Memoria CACHÉ	22 MB o superior
	3. MEMORIA	
3.1	Cantidad	Ochos (8) módulos
3.2	Ram incorporada	512 GB (Crecimiento a 1024 GB)
3.3	Tipo	DDR4 Registered ó superior
3.4	Velocidad	2666 MHZ ó superior
3.5	Ranuras de Memoria	24 DIMMs para memoria o superior
	4. ALMACENAMIENTO	
4.1	Cantidad	Ocho (8) unidades
4.2	Capacidad de almacenamiento	Dos (2) unidades de 480 GB SSD Seis (6) Unidades 1920 GB SSD
4.3	Velocidad	SSD
4.4	Tipo de disco y controladora de arreglo	SATA
	Factor de Forma	Small Form Factor SFF
4.5	Crecimiento Interno	Mínimo 8 discos SFF
4.6	Detección de fallas	Por software
4.7	RAID	RAID 0/1/1+0/5/5+0/6/6+0 Las unidades de 480 GB deben estar en RAID 1 Las unidades de 1920 GB debden estar en RAID 5 ó 6
4.8	Interface	Soporte para SAS
	5. CONECTIVIDAD	
5.1	Cantidad tarjetas de red	Dos (2) unidad

5.2	Puertos	Tarjeta 1: Cuatro (4) puertos de red GigabitEthernet Tarjeta 2: Dos (2) puertos de red SFP+ @ 10 Gbps Opcional:
	6. UNIDAD OPTICA	
6.1	Unidad óptica	SATA DVD RW 9.5mm (Opcional)
	7. PUERTOS Y SLOT	
7.1	Slots para conexión de tarjetas	Minimo 3 slots PCI Express
7.2	Puertos USB 3.0	Mínimo cinco (5) puertos
	8. ENERGIA	
8.1	Fuente de poder	Mínimo 800 W (Se debe garantizar la capacidad máxima del servidor en óptimo funcionamiento)
8.2	Categoría	Platinum
	9. REDUNDANCIA	
9.1	Redundancia de Fuentes de poder	Sí, mínimo dos (2) fuentes de poder hot plug redundantes
9.2	Redundancia de Ventiladores	Sí, mínimo siete ventiladores hot plug redundantes
	10. ADMINISTRACION REMOTA Y SEGURIDAD	
10.1	Administración Remota	Sí, administración de infraestructura remota tipo Onboard Administrator con aprovisionamiento inteligente (integrado).
10.2	Seguridad	Verificación de Firmware al arranque Verificación de Firmware periodica Recuperación segura de Firmware UEFI
	11. ACCESORIOS	
11.1	Rieles y soporte de desplazamiento para Rack	Sí, mínimo un (1) Kit
	12. INSTALACION, CONFIGURACION Y PUESTA A PUNTO	

12.1	Instalación	Instalación y aseguramiento del servidor en rack, con el riel de fácil instalación. Instalación de los demás elementos de hardware adicionales del servidor (fuentes, memorias, procesadores, disipadores, unidades ópticas, discos duros, entre otros). Conectar a las redes eléctricas reguladas y redes de datos necesarias. Debe incluir la configuración del direccionamiento de acuerdo con la solicitud que presente el instituto
12.2	Configuración de hardware	Configuración del hardware del servidor que garantice el correcto funcionamiento de los accesorios y de sus partes redundantes. Configuración de los discos duros para garantizar el arreglo RAID correspondiente definido por el Instituto de acuerdo con el número de Discos.
12.3	Instalación y Configuración de las máquinas virtuales y de los sistemas operativos.	Preparación del hardware, instalación, configuración y puesta a punto del sistema operativo Windows Server u otro de los que sea usados en las máquinas virtuales. Se debe verificar el correcto licenciamiento para el número de procesadores y núcleos del servidor, así mismo como garantizar la firma digital de los dispositivos en modo kernel y el correcto funcionamiento del Sistema Operativo con los procesadores y hardware.
12.5	Configuración de Servicios	La configuración del servidor podría incluir (sin limitarse a algunos en particular) los siguientes servicios, los cuales durante esta etapa podrán ser requeridos por el Instituto: - Instgalación y configuración del Sistema Operativo Windows Server 2016 Standar - Servicios de dominio de Active Directory - Configuración de perfiles y politicas de usuarios - Servidor DHCP - Servidor DNS - Servicios de archivo (incluido Administrador de recursos del servidor de archivos) - Virtualización con Hyper-V - Configuración direccionamiento, switches, máquinas virtuales y demás elementos relacionados con Hyper-V - Servicios de impresión y documentos - Servidor web (incluido un subconjunto de ASP.NET) - Servidor Windows Server Update - Servidor Active Directory Rights Management - Enrutamiento y acceso remoto y los siguientes subroles: - Agente de conexión a Servicios de Escritorio remoto - Administración de licencias - Virtualización

Palacio de la Cultura Rafael Uribe Uribe. Carrera 51 #52-03 Medellín-Colombia
F:+57(4)2518461 / T:+57 (4) 3209780 / contacto@culturantioquia.gov.co / www.culturantioquia.gov.co
Nit 900.425.129-0 / Redes: @Culturantioquia

12.6	Puesta a punto	Realizar las pruebas que determinen el correcto desempeño de los dispositivos, del sistema operativos instalado, de la interacción con los equipos de red, y en general garantizar y configurar el acceso de los diferentes usuarios del Instituto de acuerdo a los perfiles definidos por la entidad.
13. GARANTIA Y SOPORTE DE PROVEEDOR		
13.1	Tiempo	Un (1) año
13.2	Cobertura	En partes, mano de obra al equipo completo, accesorios y periféricos relacionados en estas especificaciones. Los repuestos deberán ser originales, nuevos y embalados en su respectivo empaque. Igualmente, el servicio debe incluir diagnóstico, soporte remoto y actualizaciones, además de reparación de hardware en el sitio, si se requiere para resolver un problema, durante el tiempo de la garantía.
13.3	Período de cobertura	24x7x4: Disponibilidad del servicio 24 horas al día, 7 días por semana, incluyendo los festivos. Desde el reporte de la falla hasta la atención por parte del fabricante con ingeniero en sitio o remoto.

10. Software para diseño suscripción por 1 año. Cantidad (4)

ESPECIFICACIONES TÉCNICAS REQUERIDAS		
ÍTEM		**CARACTERÍSTICA MÍNIMA**
1. DESCRIPCIÓN DEL EQUIPO		
1.1	Marca	**ESPECIFICAR**
1.3	LÍNEA	**GOBIERNO**
13. GARANTÍA		
13.1	Cobertura	Mano de obra.
13.2	Tiempo	Un (1) año
13.3	Funcionalidades	Software para manejo y edición video, necesario para las actividades de Comunicaciones y fonoteca. Software de edición de vídeo orientado a la edición de vídeos profesionales.

		Debe contar con una interfaz personalizable, por defecto organizada en espacios de trabajo que coincidan con las etapas de la edición: ensamblaje, edición, color, efectos, audio y títulos. Que permite el trabajo con múltiples secuencias (líneas de tiempo), que además puedan ser jerarquizadas, unas dentro de otras. A parte de medios, las líneas de tiempo que admitan una serie de elementos especiales como capas de ajuste (mismo concepto que en Photoshop), títulos, composiciones de After Effects y gráficos esenciales. Debe incorporar una librería de efectos, que sea extensible mediante la instalación de plugins. Las propiedades de los efectos se pueden animar mediante un sistema de fotogramas clave y posibilitar la creación de máscaras en la zona donde se desee aplicar el efecto, siendo útil en la generación de viñetas, correcciones de color, etc. En cuanto a especificaciones técnicas, la máxima resolución que se admite es 16k X 10k 32 y 64 bits o superior por canal, tanto en RGB como YUV o superior que permita potenciar tanto las previsualizaciones como el renderizado.

11. Software de diseño para proyectos de infraestructura - Including Specialized Toolsets Ad Commercial New Single. Suscripción por 1 año. Cantidad (2)

ESPECIFICACIONES TÉCNICAS REQUERIDAS		
ÍTEM		**CARACTERÍSTICA MÍNIMA**
1. DESCRIPCIÓN		
1.1	Marca	**Software de diseño para proyectos de infraestructura - Including Specialized Toolsets Ad Commercial New Single.**
1.3	Línea	**Gobierno**
2. GARANTÍA		
13.1	Cobertura	Mano de obra.
13.2	Tiempo	Un (1) año
	Funcionalidades	Software para diseño, en el que se pueda realizar todo tipo de proyectos técnicos, útil para ingenieros, arquitectos, etc. Pudiendo crear y visualizar

		diseños de todo tipo en 2d, planos, objetos, cortes de objetos, etc. y con herramientas avanzadas. Al igual que otros programas de Diseño Asistido por Ordenador (DAO), este debe gestionar una base de datos con entidades geométricas (puntos, líneas, arcos, etc.) con la que se puede operar a través de una pantalla gráfica en la que se muestren éstas, el llamado editor de dibujo. La interacción del usuario se debe de realizar a través de comandos, de edición o dibujo, desde la línea de órdenes. Como todos los programas de DAO, este debe procesar imágenes de tipo vectorial, debe admitir incorporar archivos de tipo fotográfico o mapa de bits, donde se puedan dibujar figuras básicas o primitivas (líneas, arcos, rectángulos, textos, etc.), y mediante herramientas de edición se creen gráficos más complejos. El programa debe permite organizar los objetos por medio de capas o estratos, ordenando el dibujo en partes independientes con diferente color y grafismo. El dibujo de objetos seriados debe gestionarse mediante el uso de bloques, posibilitando la definición y modificación única de múltiples objetos repetidos. El programa debe estar orientado a la producción de planos, empleando para ello los recursos tradicionales de grafismo en el dibujo, como color, grosor de líneas y texturas tramadas. Debe utilizar el concepto de espacio modelo y espacio papel para separar las fases de diseño y dibujo mínimo en 2D, de las específicas para obtener planos trazados en papel a su correspondiente escala y la posibilidad de manejar también los formatos para integrar compatibilidad con otros softwares de dibujo. Suscripción a 1 año - Single-user (Standalone) Este software debe ser compatible con Windows 10/11 Profesional Y MAC a 64-bits en español o superior.

12. Renovación de Licencia de Antivirus Symantec por 1 año. Endpoint Security Enterprise, Hybrid - Cloud Subscription License with Support 100. Cantidad (100)

Es importante precisar que se está solicitando esta marca de Antivirus, primero porque software se tiene implementado en la institución desde el 2014, con el cual hemos tenido muy buen desempeño y eficacia en su rol como medida de defensa adicional a nuestro firewall físico, por otro lado, implementar otro antivirus acarrea reconfiguración del servidor y reinstalación en

todas las maquinas, por lo que se tendría un sobre costo por la mano de obra en todo el proceso de implementación, con la renovación se optimiza el recurso.

13. Renovación de Licencia de FIREWALL, 3 años para los dos equipos en HA

ESPECIFICACIONES TECNICAS REQUERIDAS		
ITEM		CARACTERISTICA MINIMA
1. DESCRIPCION DEL EQUIPO		
1.1	Marca	Especificar
1.2	Modelo de referencia	Especificar
1.3	Tipo de Chasis	Rack máximo de 1U (Una Unidades de Rack)
2. HARDWARE		
2.1	Puertos acelerados por hardware	16
2.2	Puerto de administración de alta disponibilidad	1
2.4	Puertos acelerados por hardware SFP	8
2.5	Puertos acelerados por hardware SFP+	4
2.6	Puerto de Consola	Si – Especificar
2.7	Puerto USB	Si – Especificar
2.8	Módulo de plataforma confiable	Si
2.10	Firmware firmado por el fabricante	Si
2.11	Chipset	Si – Especificar
3. DESEMPEÑO		
3.1	Desempeño de IPS	5,3 Gbps
3.2	Desempeño de firewall de próxima generación	3,1 Gbps

Palacio de la Cultura Rafael Uribe Uribe. Carrera 51 #52-03 Medellín-Colombia
F:+57(4)2518461 / T:+57 (4) 3209780 / contacto@culturantioquia.gov.co / www.culturantioquia.gov.co
Nit 900.425.129-0 / Redes: @Culturantioquia

3.3	Desempeño de protección contra amenazas	2,8 Gbps
3.4	Tipo	DDR4 Registered ó superior
3.5	Capacidad de procesamiento Firewall	39/39/38 Gbps
3.6	Latencia máxima de firewall	3,17 us
3.7	Millones de paquetes por segundo Firewall	42
3.8	Sesiones concurrentes de TCP	3M
3.9	Sesiones nuevas por segundo	140K
3.10	Máximas políticas de Firewall	10K
3.11	Desempeño de VPN IPSec	35 Gbps
3.12	Cliente a VPN Gateway	16K
3.13	Desempeño VPN - SSL	1,5 Gbps
3.14	Usuarios concurrentes de VPN SSL-VPN	500
3.15	Desempeño de inspección SSL	3 Gbps
3.16	Inspección de sesiones concurrentes de ips HTTPS	315k
3.17	Desempeño de control de aplicaciones	6,7 Gbps

3.18	Desempeño CAPWAP	35 Gbps
3.19	Dominios Virtuales	10
3.20	Switches soportados	48
3.21	Access Points Soportados	128
3.22	Tokens	5000
3.23	Configuración de Alta Disponibilidad	Activo - Pasivo / Activo - Activo
3.24	Crecimiento	384 GB o superior
	4. SUSCRIPCIÓN Y LICENCIAMIENTO	
4.1	Cantidad	1
4.2	Tiempo	36 meses
4.3	Tipo de suscripción	Protección unificada contra amenazas
	5. ACCESORIOS	
5.1	Conexión eléctrica	Compatible con tomas de 120-240 V
5.2	Fuentes	2
5.3	Módulos SFP+	2 incluidos
5.4	Tipo de módulo	LC-LC para FO MMF OM3
5.5	Velocidad	10 Gbps
5.6	STP	Habilitador y configurado
	6. ENERGIA	
6.1	Fuente de poder	Mínimo 2 (Se debe garantizar la capacidad máxima del equipo en óptimo funcionamiento)
6.2	Categoría	Platinum o similar
	7. REDUNDANCIA	
7.1	Redundancia de Fuentes de poder	Sí, mínimo dos (2) fuentes de poder hot plug redundantes
7.2	Redundancia de Ventiladores	Sí,

8. ADMINISTRACION REMOTA Y SEGURIDAD		
8.1	Administración Remota	Sí, administración de infraestructura remota tipo Onboard Administrator, y con token de seguridad
9. INSTALACION, CONFIGURACION Y PUESTA A PUNTO		
9.1	Instalación	Instalación, migración completa de la configuración y aseguramiento del equipo en rack. Instalación de los demás elementos de hardware adicionales. Conectar a las redes eléctricas reguladas y redes de datos necesarias. Debe incluir la configuración del direccionamiento de acuerdo con la solicitud que presente el instituto
9.2	Configuración de hardware	Configuración del hardware del equipo que garantice el correcto funcionamiento de los accesorios y de sus partes redundantes. Configuración de los equipos para su funcionamiento en alta disponibilidad
9.3	Instalación y Configuración del Sistema Operativo	Preparación del hardware, configuración y puesta a punto del sistema operativo del equipo. Se debe garantizar la firma digital de los dispositivos en modo kernel y el correcto funcionamiento del Sistema Operativo con los procesadores y hardware.
9.4	Configuración de Servicios	La configuración podría incluir (sin limitarse a algunos en particular) los siguientes servicios, los cuales durante esta etapa podrán ser requeridos por el Instituto: - Configuración del Sistema Operativo - Servidor DHCP - Servidor DNS - Conexión servicios de archivo (incluido Administrador de recursos del servidor de archivos) - Conexión con servidor de Controlador de dominio. - Configuración direccionamiento, switches, máquinas virtuales y demás elementos relacionados. - Enrutamiento y acceso remoto y los siguientes subroles: - Agente de conexión a Servicios de Escritorio remoto - Virtualización - Se debe configurar todas las políticas, direcciones, objetos, direcciones, eyc necesarias para garantizar el correcto funcionamiento del equipo
9.5	Puesta a punto	Realizar las pruebas que determinen el correcto desempeño de los dispositivos, del sistema operativos instalado, de la interacción con los equipos de red, y en general garantizar y configurar el acceso de los diferentes usuarios del Instituto de acuerdo con los perfiles definidos por la entidad.
10, GARANTIA Y SOPORTE DE FABRICANTE		

10.1	Tiempo	Tres (3) años, Certificado por el fabricante.
10.2	Cobertura	En partes, mano de obra al equipo completo, accesorios y periféricos relacionados en estas especificaciones. Los repuestos deberán ser originales, nuevos y embalados en su respectivo empaque. Igualmente, el servicio debe incluir diagnóstico, soporte remoto y actualizaciones, además de reparación de hardware en el sitio, si se requiere para resolver un problema, durante el tiempo de la garantía.
10.3	Período de cobertura	24x7x6: Disponibilidad del servicio 24 horas al día, 7 días por semana, incluyendo los festivos. Desde el reporte de la falla hasta la reparación, máximo 6 horas para que el hardware cubierto vuelva a su condición operativa.
11. SOPORTE Y ATENCIÓN DE FALLAS POR PARTE DEL PROVEEDOR O CONTRATISTA		
11.1	Tiempo	Tres (3), Certificado por el proveedor o contratista
11.2	Cobertura	Este servicio debe incluir software de gestión y monitoreo, graficas de tráfico, estadísticas e informes, reconfiguraciones, atención de escalamientos, Instalación de nuevas partes y hardware adicional al equipo, plan de contingencia con equipo básico provisional durante el tiempo de garantía de fabricante (si es requerido), acompañamiento en consultoría tecnológica. El proponente deberá anexar un Acuerdo de Nivel de Servicio (ANS) donde describa el procedimiento de atención, generación de un número de caso para seguimiento de daños o solicitudes, los niveles de criticidad de los casos, el nivel de escalamiento, los tiempos máximos de respuesta según nivel de criticidad, y todo aquello que el proponente considere necesario para dar solución oportuna a los reportes de falla y/o solicitudes.
11.3	Período de cobertura	24x7x6: Disponibilidad del servicio 24 horas al día, 7 días por semana, incluyendo los festivos. Desde el reporte de la falla hasta la reparación, máximo 6 horas para que el hardware cubierto vuelva a su condición operativa.

CARACTERÍSTICAS ADICIONALES:

La infraestructura deberá contar con las siguientes especificaciones:

- Seguridad de Red de Próxima Generación (NGFW)
  - Inspección de Tráfico Cifrado: Utiliza aceleración por hardware (CP9/NP7) para realizar inspección SSL/TLS 1.3 a escala, evitando que el malware se oculte en túneles cifrados sin degradar el rendimiento.

- IPS y Protección contra Malware: El sistema de prevención de intrusiones utiliza firmas de laboratorios y análisis de comportamiento para bloquear ataques dirigidos y movimientos laterales.
- Filtrado de Contenido V10: Incluye categorización de URLs basada en IA, filtrado de DNS para bloquear dominios maliciosos antes de que se establezca la conexión y control granular sobre aplicaciones de video (ej. bloquear comentarios, pero permitir el video).

- SD-WAN y SD-Branch (Conectividad)
  - SD-WAN Basado en Aplicaciones: Reconoce más de 5,000 aplicaciones. Puede medir la latencia, el jitter y la pérdida de paquetes en tiempo real para mover el tráfico de voz (VoIP) al mejor enlace disponible automáticamente.
  - Controlador de Red Unificado: El sistema operativo actúa como el controlador central para Switches y APs, permitiendo que un puerto de switch o un SSID de Wi-Fi hereden las mismas políticas de seguridad del firewall.
  - Orquestación de VPN: Simplifica la creación de topologías complejas (Hub-and-Spoke) mediante ADVPN (Auto-Discovery VPN), que establece túneles dinámicos directos entre sucursales para reducir la latencia.
- Acceso Universal de Confianza Cero (ZTNA)
  - Proxy de Acceso: Reemplaza el acceso VPN tradicional. El usuario solo accede a la aplicación específica (no a toda la red) tras verificar su identidad y el estado de salud de su dispositivo.
  - Postura del Dispositivo: El sistema operativo puede denegar el acceso si el antivirus del endpoint está desactivado o si el sistema operativo no tiene los parches de seguridad al día.
- Security Services (Suscripciones IA)
  - Inline CASB: Protege los datos en movimiento hacia aplicaciones SaaS (Salesforce, Office 365), permitiendo el control de actividades específicas para prevenir la pérdida de datos (DLP).
  - Antivirus de IA: Utiliza modelos de aprendizaje profundo locales en el firewall para detectar variantes de malware nunca antes vistas, sin depender exclusivamente de una base de datos de firmas.
  - Protección OT e IoT: Incluye una base de datos específica para identificar dispositivos médicos, industriales o de hogar inteligente, aplicando políticas de segmentación automática para aislarlos.
- Operaciones de Seguridad y Automatización
  - Fabric Management Center: Provee una vista de topología de 360 grados que muestra visualmente dónde están las brechas de seguridad en toda la red.
  - Ecosistema de Automatización: Permite crear "Stitches" (puntadas) de seguridad. Por ejemplo: “Si un sensor detecta un compromiso en el servidor X, poner automáticamente la dirección IP del atacante en una lista negra global de todos los firewalls de la empresa”.
- Limitaciones y Requisitos de Hardware

- Gestión de Memoria: Los equipos con 2GB de RAM o menos operan en Modo Flow únicamente, eliminando las funciones de Proxy para preservar la estabilidad del sistema.
- Optimización NP7: Los modelos de gama alta aprovechan el procesador de red NP7 para manejar millones de conexiones simultáneas y tráfico de elefante (grandes flujos de datos) con latencia cercana a cero.

La suscripción deberá contar con las siguientes características y funcionalidades:

- Seguridad de Red y Archivos (núcleo ATP)
  - Intrusion Prevention System (IPS): Analiza el tráfico en tiempo real mediante IA/ML para detectar y bloquear intrusiones y ataques conocidos mediante parches virtuales.
  - Advanced Malware Protection (AMP): Incluye antivirus, protección contra malware móvil y Sandbox Cloud para analizar archivos sospechosos en un entorno seguro.
  - Application Control: Ofrece visibilidad y control sobre miles de aplicaciones para garantizar el cumplimiento de políticas de seguridad.
- Seguridad Web y de Contenido
  - Filtrado Web y de URL: Bloquea el acceso a sitios web maliciosos o no deseados y verifica enlaces en correos electrónicos.
  - Filtrado de DNS: Protege contra amenazas basadas en el dominio, como el acceso a sitios de phishing.
  - Video Filtering: Permite controlar y filtrar el contenido de video en plataformas como YouTube.
  - Anti-Botnet y Reputación de IP: Previene la comunicación con redes de bots (C2) y bloquea ataques desde fuentes con mala reputación.
- Servicios Adicionales
  - Anti-Spam: Filtra el correo electrónico no deseado y malicioso.

Soporte Premium: Incluye soporte técnico 24x7 y reemplazo avanzado de hardware

14. Servicios complementarios a la oferta

Prestar los servicios de soporte tecnológico para el Instituto de Cultura y Patrimonio de Antioquia contemplados en el **plan estratégico de las tecnologías de la información y la comunicación,** para lo cual deberá contar con el recurso humano, personal certificado e idóneo que garantice el correcto funcionamiento de equipos y procesos, requerido para todo el proceso de configuración y puesta en marcha de los productos referidos según las especificaciones técnicas, es el que se relaciona a continuación, y con el que el contratista deberá contar:

- Dos (2) Ingenieros Certificado en la solución de FORTINET NSE4, y uno de ellos en Seguridad de arquitectura de red NSE7
- Dos (2) Ingenieros Certificado en ArcServe.
- Uno (1) Ingeniero Certificado en Windows Server MCSE
- Uno (1) Ingeniero Certificado en Solutions Expert: Core Infrastructure (Integración con AD)
- Uno (1) Ingeniero Certificado en Solutions Expert: Cloud Platform and Infrastructure
- Uno (1) Ingeniero Certificado en CCNA.

- Uno (1) Ingeniero Certificado en la marca HP y ARUBA de Core y Borde
- Uno (1) Ingeniero Certificado en la marca RUCKUS para Red inalámbrica
- Uno (1) técnico certificado en instalación y configuración de pantallas interactivas.
- Uno (1) técnico certificado en instalación y configuración en sistemas de sonido y conferencias.

Para acreditar lo anterior, el contratista deberá presentar la hoja de vida y certificados que acrediten el recurso humano requerido.

8.4 Acuerdos de Nivel de Servicio ANS.

El tiempo máximo de respuesta y solución de casos con soporte será del 99.2% equivalente a 6 horas a partir del reporte de la falla por periodo.

Un PERÍODO significa un (1) mes calendario, que comienza el primer día de cada mes.

El porcentaje de disponibilidad será calculado y medido respecto a cada servicio instalado, de conformidad con la siguiente fórmula:

P=A/B X 100

- A: es el número de horas en las cuales el servicio estuvo disponible durante el mes
- B: es el número de horas al mes que debería estar disponible el servicio, es decir veinticuatro (24) horas multiplicado por el número de días del período
- P: es el porcentaje de disponibilidad

El PERÍODO de disponibilidad de cualquier enlace será medido a partir del momento en que la No disponibilidad es reportada por Instituto o detectada por el contratista. La no disponibilidad deberá terminar en el momento en que la falla sea solucionada y el Instituto sea avisado por el contratista de que el sistema está disponible.

El contratista debe notificar al Instituto de cualquier trabajo llevado a cabo sobre el sistema para el propósito de modificar y mejorar el mismo.

Definición de Prioridades

- Prioridad 1. Desconexión total: se entiende que la comunicación entre dos o más puntos de la red en el Instituto se ha interrumpido totalmente, es decir no hay transferencia de datos.
- Prioridad 2. Por operación degradada: se entiende como el incumplimiento de los estándares de calidad y disponibilidad. Esto no significa que haya desconexión del servicio, pero existe la posibilidad de que ocurran retransmisiones.
- Prioridad 3. Fallas intermitentes: se entiende que la comunicación entre dos o más puntos de la red en el Instituto es inestable. Son inconvenientes que se pueden presentar esporádicamente y que pueden causar interrupción en el servicio por periodos de tiempo cortos. El tiempo de duración de las fallas intermitentes formará parte de la indisponibilidad, siempre y cuando sea medible y mayor a 10 segundos por más de tres veces, en un periodo de tiempo de una (1) hora.
- Prioridad 4. Falla no grave: se entiende por la falla que no afecta ni degrada la prestación del servicio.

Para el soporte técnico, se debe contar con un número telefónico en la ciudad de Medellín y un móvil que es portado por el Ingeniero de Soporte disponible, a través de estas líneas se dará el soporte necesario para la recepción y solución de la falla reportada por el Instituto, además debe contar con un software para creación y seguimiento de casos, debe entregarse la documentación para la atención de casos y los niveles de escalamiento del soporte.

Las fases del servicio de soporte deben ser las siguientes:

1. Reporte o detección del problema.
- 2. Generación del tiquete y Diagnostico.
- 3. Plan de acción.
- 4. Solución de la falla.
- 5. Cierre del tiquete.

– Para el presente proceso se requiere de una solución integral que abarque todos los componentes. Esta solución debe darse por un solo proponente, ya que se tiene que garantizar el suministro, la instalación, la configuración, la puesta a punto, el soporte y la garantía sobre todos y cada uno de los bienes y servicios integrantes de la misma; de igual manera asegurar la operatividad, la conectividad y la confidencialidad de los sistemas de información del Instituto de Cultura y Patrimonio de Antioquia durante el tiempo establecido de soporte. Así mismo en la instalación, al depender los elementos unos de otros para su funcionalidad, se pone en riesgo la garantía de estos, ya que en el mercado es más eficiente y confiable la oferta de la garantía y soporte por la solución completa. Es importante resaltar que la integralidad de la solución permitirá que sólo sea un proveedor el que se encargue de garantizar la operación normal de la solución.

A continuación, se relacionan de manera general los componentes que integran la solución requerida

8.5 Condiciones Generales Aplicables Para Todos Los Componentes.

p. Una vez firmada el acta de inicio del contrato y antes de iniciar su ejecución, el contratista deberá presentar el Plan de Trabajo y Cronograma de actividades que den cuenta de las etapas, los tiempos y horarios para el desarrollo de las obligaciones contractuales, generando el mínimo impacto en las labores habituales de la entidad. Las respectivas actividades serán revisadas y concertadas con la supervisión y/o interventoría y apoyos a la supervisión y/o interventoría del respectivo contrato.

q. Una vez firmada el acta de inicio del contrato y antes de iniciar su ejecución, el contratista deberá adjuntar las hojas de vida del personal que será el responsable de implementar la solución y con experiencia mínima de 2 años, relacionada con el objeto a contratar. Se entenderá que dentro de este personal se encontrarán quienes deben contar con las respectivas certificaciones solicitadas cuando se presentó la propuesta. El personal debe cumplir con las respectivas exigencias en cuanto a la normatividad de seguridad y salud en el trabajo como son los respectivos permisos de altura, seguridad social, entre otros en los casos requeridos según actividades a desarrollar.

r. El proponente deberá proporcionar la totalidad de la herramienta y estructuras requeridas para el desarrollo de los trabajos con las debidas certificaciones y condiciones establecidas por la normatividad vigente.

s. Garantizar el suministro, instalación, configuración y puesta a punto del hardware y software en el (los) lugar (es) específico (s) señalado (s) por el Instituto dentro de sus instalaciones. El contratista deberá suministrar la mano de obra calificada y requerida para la ejecución del contrato.

t. Garantizar la configuración y puesta a punto de la infraestructura de Red en el (los) lugar (es) específico (s) señalado (s) por el Instituto dentro o fuera de sus instalaciones. El contratista deberá suministrar la mano de obra calificada y requerida para la ejecución del contrato.
u. El contratista debe garantizar que la solución ofertada sea de última tecnología cumpliendo con las características técnicas mínimas exigidas y ofertadas.
v. Los bienes ofrecidos deberán ser nuevos (no se permiten equipos remanufacturados) y el contratista deberá garantizar las condiciones de calidad de estos.
w. El contratista deberá incluir todas las licencias de los equipos en caso de ser necesario.
x. Las licencias suministradas, instaladas y configuradas (Componente 7) deberán estar a nombre del INSTITUTO DE CULTURA Y PATRIMONIO DE ANTIOQUIA, para lo cual se deberá entregar los respectivos soportes que evidencien dicha exigencia.
y. El contratista deberá garantizar que el licenciamiento de los equipos, las actualizaciones de software y firmware sean perpetuas en los casos de licenciamiento vitalicios, tal como se establece en las fichas técnicas del presente proceso o durante el tiempo de garantía.
z. El contratista deberá entregar los manuales correspondientes a los equipos y a la configuración de la red de datos de los nuevos equipos y las redes de datos intervenidas durante el proceso de configuración y puesta a punto de la solución.
aa. El contratista deberá anexar un Acuerdo de Nivel de Servicio (ANS) por cada componente de la solución, donde describa el procedimiento de atención, generación de un número de caso para seguimiento de daños o solicitudes, los niveles de criticidad de los casos, el nivel de escalamiento, los tiempos máximos de respuesta según nivel de criticidad, y todo aquello que el Instituto considere necesario para dar solución oportuna a los reportes de falla y/o solicitudes, dentro del soporte que se dará por un (1) año. Lo anterior durante la ejecución del contrato. Los mismos deben ser revisados y aprobados por la Supervisión y/o interventoría del contrato.
bb. Durante la implementación de la solución integral el contratista deberá brindar una capacitación y acompañamiento de treinta (30) horas en las instalaciones del instituto y al personal que designe la entidad. La entidad ofrecerá el uso de las instalaciones y de los recursos tecnológicos para el desarrollo de las capacitaciones, los demás costos asociados a la presente serán asumidos por el contratista. Para esto se deberá concertar el contenido de esta y los tiempos con el supervisor y/o interventor designado.
cc. Dentro del soporte (cinco -5- años) el proveedor o contratista deberá garantizar visita técnica por un tiempo no inferior a dos (2) horas semanales en sitio durante los primeros seis (6) meses de un especialista el primer día hábil de cada semana, a primera hora y durante el horario laboral del Instituto. Igualmente, los horarios de permanencia se podrán concertar con la Entidad. Lo anterior en aras de garantizar la estabilidad y la integridad de la solución.
dd. La instalación, la configuración, la puesta a punto, el soporte y la garantía del hardware, software e infraestructura suministrada corre por cuenta del contratista.

8.6 Condiciones adicionales específicas aplicables a todos los elementos.

b. El alcance del soporte de proveedor o contratista tanto en la ejecución del contrato como en los años siguientes debe incluir la configuración y puesta a punto de los equipos que actualmente tiene el Instituto y que serán integrados a la solución propuesta. Estos se describen a continuación:

-Toda la infraestructura de Networking, incluida la alta disponibilidad entre el switche de core nuevo del instituto y el switche de core con el que actualmente cuenta el instituto.
-El proveedor o contratista debe garantizar que la solución sea alcanzable a los equipos de cómputo que indique el instituto, sean de escritorio o portátiles.
-El licenciamiento debe ser instalado y configurado, y entregar las respectivas certificaciones de uso, así como los certificados de soporte y actualización en línea cuando sean requeridos.

OCTAVA. SUPERVISIÓN: El Director del INSTITUTO designará un supervisor para el mismo, quien ejercerá, conforme al artículo 83 de la Ley 1474 de 2011, el seguimiento técnico, administrativo, financiero, contable y jurídico sobre el cumplimiento del objeto del contrato. **NOVENA. AUSENCIA DE RELACIÓN LABORAL:** El presente contrato será ejecutado por el CONTRATISTA con absoluta autonomía e independencia y, en desarrollo del mismo, el INSTITUTO no contrae obligación laboral alguna con el CONTRATISTA, ni con las personas que éste a su vez contrate para la prestación del servicio. En consecuencia, el pago de salarios, honorarios y prestaciones de este personal estará a cargo exclusivamente del CONTRATISTA. **DÉCIMA. LUGAR DE EJECUCIÓN:** La ejecución del presente contrato será en el Palacio de la Cultura "Rafael Uribe Uribe", Medellín, Antioquia. **DÉCIMA PRIMERA. CESIÓN:** El presente contrato se celebra teniendo en cuenta las calidades y condiciones del CONTRATISTA, por lo tanto, éste no podrá cederse total o parcialmente a otra persona o entidad alguna. **DÉCIMA SEGUNDA. CONTROL FISCAL:** Corresponde a la Contraloría Departamental ejercer el control fiscal posterior del presente contrato. **DÉCIMA TERCERA. INHABILIDADES E INCOMPATIBILIDADES:** El CONTRATISTA declara bajo la gravedad de juramento que se entiende prestado con la firma de este documento, que no incurre en ninguna de las causales de inhabilidades e incompatibilidades previstas en la Constitución Política de Colombia y la Ley, especialmente en las contempladas en el artículo 8° de la Ley 80 de 1993. **DÉCIMA CUARTA. CLÁUSULAS EXCEPCIONALES:** En el presente contrato se entienden incluidas las cláusulas excepcionales al derecho común de terminación, interpretación, modificación unilateral del contrato y caducidad, de conformidad con lo establecido en los artículos 15, 16, 17 y 18 de la Ley 80 de 1993. **DÉCIMA QUINTA. CADUCIDAD Y EFECTOS:** EL INSTITUTO, mediante resolución motivada podrá declarar la caducidad administrativa del presente contrato en caso de presentarse alguno de los hechos constitutivos de incumplimiento de las obligaciones a cargo de EL CONTRATISTA, que afecte de manera grave y directa la ejecución del presente contrato. **PARÁGRAFO:** Declarada la caducidad del contrato, éste se dará por terminado y se ordenará la devolución de la totalidad de los dineros entregados y no ejecutados. La declaratoria de caducidad será constitutiva del siniestro de incumplimiento y no dará lugar a indemnización alguna a favor de EL CONTRATISTA, quien se hará acreedor a las sanciones e inhabilidades previstas en la ley. **DÉCIMA SEXTA. PAGO DE APORTES A SEGURIDAD SOCIAL INTEGRAL Y PARAFISCALES:** De conformidad con el artículo 50 de la ley 789 de 2002 y el artículo 23 de la Ley 1150 de 2007, el CONTRATISTA deberá acreditar el pago de los aportes de los empleados, a los sistemas de salud, riesgos profesionales, pensiones y aportes a las cajas de compensación familiar, Instituto Colombiano de Bienestar Familiar, Servicio Nacional de Aprendizaje -SENA-, cuando a ello haya lugar, mediante certificación expedida por el revisor fiscal, cuando éste exista de acuerdo con los requerimientos de ley, o por el representante legal. **DÉCIMA SEPTIMA. PERFECCIONAMIENTO Y EJECUCIÓN:** El presente contrato se perfecciona con el acuerdo de las partes sobre su objeto y contraprestación y con la suscripción del mismo. Para su ejecución se requiere el registro presupuestal, aprobación de la póliza y la firma del Acta de Inicio. **DÉCIMA OCTAVA. GARANTÍAS:** El CONTRATISTA deberá constituir garantía única, expedida por compañía de seguros o entidad bancaria, legalmente establecida en Colombia, de acuerdo con lo estipulado en el Decreto 1082 de 2015, con el amparo de:

-CUMPLIMIENTO: Por una cuantía equivalente al diez por ciento (10%) del valor total del contrato, con una vigencia igual al plazo del mismo y cuatro (4) meses más.
-CALIDAD DEL SERVICIO: Por una cuantía equivalente al quince por ciento (15%) del valor del contrato, y una vigencia igual a la duración del contrato y seis (6) meses más.
- CALIDAD Y CORRECTO FUNCIONAMIENTO DE LOS BIENES: Por una cuantía equivalente al quince por ciento (20%) del valor del contrato, y una vigencia igual a la duración del contrato y seis (6) meses más.
DÉCIMA NOVENA. TERMINACIÓN: El presente Contrato podrá darse por terminado:

- Por ejecución del objeto.
- Vencimiento del plazo.
- Por grave incumplimiento de las obligaciones a cargo de cada una de las partes.
- Por fuerza mayor o caso fortuito, que impida la posibilidad de seguir su ejecución.
- Por mutuo acuerdo entre las partes.

VIGÉSIMA. GASTOS E IMPUESTOS: Todos los gastos e impuestos que se originen por causa de este contrato correrán por cuenta del CONTRATISTA. **VIGÉSIMA PRIMERA. LIQUIDACIÓN:** Las partes procederán a la liquidación del contrato, dentro de los cuatro (4) meses siguientes a su finalización, conforme a lo previsto en el artículo 11 de la Ley 1150 de 2007. En esta etapa se acordarán los ajustes, revisiones, reconocimientos y transacciones a que haya lugar, previo el pago total que el INSTITUTO efectúe al CONTRATISTA. Las partes firmarán un acta de liquidación en la cual conste la declaratoria de paz y salvo entre sí, por las obligaciones adquiridas en el desarrollo del contrato. **VIGÉSIMA SEGUNDA. SOLUCIÓN DE CONTROVERSÍAS:** Las partes acuerdan que en el evento de presentarse diferencias en razón de la celebración, ejecución, desarrollo y terminación del presente contrato procederán a realizar la conciliación prejudicial antes de iniciar cualquier acción judicial. **VIGÉSIMA TERCERA. TRANSPARENCIA.** El CONTRATISTA manifiesta que presentó oferta y participo del proceso de selección abreviada por subasta inversa S.I.E 036 – 2022, que concluye con la suscripción del presente contrato, de manera voluntaria, libre, trasparente sin recibir ningún tipo de ayuda ni beneficios por parte de algún funcionario público o de terceras personas. **VIGÉSIMA CUARTA. INDEMNIDAD DE LA ENTIDAD:** El CONTRATISTA será responsable ante el INSTITUTO de mantenerlo libre de cualquier daño o perjuicio originado en reclamaciones de terceros y que se deriven de sus actuaciones, de sus subcontratistas o dependientes por reclamos, demandas o costos que puedan surgir por daños o lesiones a personas o propiedades del INSTITUTO o terceros, ocasionados por actos, hechos u omisiones de éste en desarrollo de la actividad encomendada. Cualquier costo en que incurra el INSTITUTO para la defensa de sus intereses o cualquier suma que deba cancelar como consecuencia de los reclamos previstos en esta cláusula, deberá ser reintegrada al INSTITUTO en su totalidad debidamente actualizada. En caso de no cumplirse esta obligación su valor podrá hacerse efectivo deduciéndolo de cualquier suma que se adeude al CONTRATISTA o a través de cualquier otro procedimiento de cobro establecido por el INSTITUTO en caso de que el contrato hubiere sido liquidado. **VIGÉSIMA QUINTA. PENAL PECUNIARIA:** En caso de incumplimiento total o parcial por parte del CONTRATISTA de cualquiera de las obligaciones contraídas con el contrato o de declaratoria de caducidad, la entidad podrá hacer valedera la cláusula penal pecuniaria al CONTRATISTA hasta por un valor del diez por ciento (10%) del valor del contrato, suma que la entidad hará efectiva mediante el cobro de la garantía única de cumplimiento o, a su elección, de los costos que adeude al CONTRATISTA, si los hubiere, para lo cual se entiende expresamente autorizado con la firma del contrato; si esto no fuere posible, se cobrará por vía judicial. La aplicación de la cláusula penal no excluye la indemnización de perjuicios tal como lo permiten los artículos 870 del Código de Comercio y 1546 del Código Civil. **VIGÉSIMA SEXTA. MULTAS:** Por el incumplimiento de cualquier obligación contractual, el contratista se hará acreedor a una multa equivalente hasta por el cinco por ciento (5%) del valor básico del contrato. En el caso de que el CONTRATISTA se haga acreedor a cualquiera de las multas por incumplimiento, su valor será tomado de cualquier saldo a favor del CONTRATISTA o cubierto por la garantía de cumplimiento y en ningún caso su aplicación será entendida por el Contratista como liberatoria o atenuante de

cualquiera de las obligaciones adquiridas en virtud del contrato. El procedimiento de imposición de multas será el establecido por la Ley 1474 de 2011. La aplicación de la multa como consecuencia del incumplimiento de cualquier obligación contractual no agota la posibilidad de volverla a aplicar si se presenta nuevamente el incumplimiento de esa o de cualquiera otra obligación. **VIGÉSIMA SEPTIMA. GARANTÍA DE LEGALIDAD Y TRASPARENCIA. Las PARTES** garantizan que sus negocios y los recursos que utilizan para la ejecución del presente contrato no provienen ni se destinan al ejercicio de ninguna actividad ilícita, Lavado de Activos o Financiación del Terrorismo; Asimismo, se comprometen a entregar toda la información que les sea solicitada para dar cumplimiento a las disposiciones relacionadas con la Prevención del Lavado de Activos y Financiación del Terrorismo y declaran que la misma es veraz y verificable. LAS PARTES se obligan a realizar todas las actividades encaminadas a asegurar que todos sus socios, administradores, clientes, proveedores o empleados, y los recursos de éstos, no se encuentren relacionados o provengan de actividades ilícitas. **PARÁGRAFO.** Si por parte del contratante se identifican recursos de lavado de activos en los contratos celebrados, el supervisor designado para este, en compañía del área de Control Interno y con apoyo del área jurídica de la Subdirección Administrativa y Financiera, deberá reportarlo a la Unidad de Información y análisis financiero "UIAF" y a la Fiscalía General de la Nación. **VIGÉSIMA OCTAVA DOMICILIO:** Para los efectos legales, las partes fijan como domicilio la ciudad de Medellín. **VIGÉSIMA NOVENA. MANIFESTACIÓN:** Las partes manifiestan libremente que han procedido a la lectura total y cuidadosa del presente documento, por lo que, en consecuencia, se obligan en todas sus órdenes y manifestaciones con la aprobación realizada a la minuta electrónica mediante la plataforma SECOP II.
