De conformidad con lo establecido en el Artículo 2.2.1.2.1.5.1. del Decreto 1082 de 2015, se realizan los presentes estudios previos así:

1. DESCRIPCIÓN DE LA NECESIDAD QUE SE PRETENDE SATISFACER CON LA CONTRATACIÓN.

De conformidad con lo establecido en el Artículo 2.2.1.2.1.5.1. del Decreto 1082 de 2015, se realizan los presentes estudios previos **para sustentar la necesidad de contratar una solución de seguridad endpoint para los equipos de propiedad de la Unidad Administrativa Especial del Servicio Público de Empleo - UAESPE.**

Mediante el artículo 26 de la Ley 1636 de 2013 se creó la Unidad Administrativa Especial del Servicio Público de Empleo, como entidad del orden nacional con personería jurídica, patrimonio propio, autonomía administrativa y financiera, adscrita al Ministerio del Trabajo, encargada de la administración del Servicio Público de Empleo y la Red de Prestadores del Servicio Público de Empleo, la promoción de la prestación del servicio público de empleo, el diseño y operación del Sistema de Información del Servicio Público de Empleo, el desarrollo de instrumentos para la promoción de la gestión y colocación de empleo y la administración de recursos públicos relacionados con la gestión y colocación de empleo.

La operación institucional de la UAESPE depende del uso continuo de equipos de cómputo, servicios digitales, sistemas de información, correo electrónico, acceso a internet, plataformas de colaboración y herramientas ofimáticas que procesan información institucional y soportan las actividades administrativas, técnicas y misionales de la Entidad. En consecuencia, la protección de los equipos endpoint constituye un control básico y necesario para preservar la confidencialidad, integridad y disponibilidad de la información, así como para reducir la exposición frente a malware, ransomware, software malicioso, ataques de ingeniería social, ejecución no autorizada de archivos y otros eventos de seguridad digital.

Actualmente la Entidad cuenta con una solución de antivirus/EDR desplegada en sus equipos institucionales, la cual se toma como línea base técnica. Sin embargo, la necesidad de la Entidad no se limita a la renovación de una marca específica, sino a mantener o mejorar las capacidades de protección endpoint, detección y respuesta. Por esta razón, el proceso se estructura mediante condiciones funcionales y técnicas neutrales frente a fabricantes o marcas. Para efectos del proceso, se entenderá como solución equivalente aquella que, aun cuando corresponda a un fabricante, producto, arquitectura o denominación comercial diferente de la solución actualmente instalada, cumpla integralmente con las capacidades mínimas de cobertura, compatibilidad, protección antivirus y antimalware, EDR o XDR, detección, investigación, respuesta, administración centralizada, soporte, instalación, puesta en marcha y demás condiciones previstas en el Anexo Técnico y en la matriz de cumplimiento.

La equivalencia se verificará por los resultados funcionales y niveles mínimos de desempeño exigidos, y no por la identidad de tecnologías, módulos o nombres comerciales. Una solución se considerará superior cuando, además de cumplir todos los requisitos mínimos, incorpore capacidades adicionales que mejoren la protección, visibilidad, administración o respuesta, sin generar costos adicionales ni dependencias tecnológicas no previstas para la UAESPE. Las funcionalidades adicionales no compensarán el incumplimiento de requisitos técnicos mínimos.

La falta de una solución endpoint vigente y soportada podría generar exposición a código malicioso, pérdida o indisponibilidad de información, afectación de los equipos institucionales, interrupción de actividades administrativas y misionales, incremento de incidentes de seguridad y mayores tiempos de recuperación ante eventos de malware o ransomware. Igualmente, podría afectar la capacidad de la Entidad para identificar oportunamente eventos de seguridad en los equipos de cómputo y responder de manera controlada.

En consecuencia, se requiere renovar o adquirir una solución de seguridad endpoint para ochenta y cinco (85) equipos de propiedad de la UAESPE, compatible con Windows 10, Windows 11 y Linux Rocky, con capacidades de antivirus, antimalware, EDR o XDR, detección y respuesta, administración centralizada o administrada, configuración, soporte y puesta en marcha, incluyendo acompañamiento en la instalación o migración cuando la solución seleccionada sea diferente a la actualmente utilizada.

1.2. CONVENIENCIA

La contratación resulta conveniente, necesaria y oportuna porque permite a la UAESPE preservar la protección de sus equipos de cómputo, mantener actualizadas las capacidades de detección y respuesta frente a amenazas, contar con soporte técnico durante la vigencia del licenciamiento y garantizar la continuidad del control de seguridad endpoint en los equipos institucionales.

Adicionalmente, el proceso se estructura en términos funcionales y técnicos, evitando referencias restrictivas a una marca determinada. Lo anterior permite promover pluralidad de oferentes, comparabilidad técnica y económica, transparencia en la adquisición y selección objetiva de la oferta que cumpla los requisitos exigidos y presente el menor precio, de conformidad con las reglas de la mínima cuantía.

2. OBJETO

500001Renovar o adquirir una solución de seguridad endpoint con capacidades de antivirus EDR o XDR, detección y respuesta, que incluya los servicios de configuración, soporte y puesta en marcha de la solución para equipos de propiedad de la Unidad Administrativa Especial del Servicio Público de Empleo - UAESPE.

2.1. ALCANCE DEL OBJETO

Las especificaciones para la ejecución del contrato se encuentran descritas en el Anexo Técnico, el cual hace parte integral del presente documento. Sin perjuicio de lo anterior, el alcance mínimo comprende:

- Licenciamiento para ochenta y cinco (85) equipos endpoint de propiedad de la UAESPE, por el término de un (1) año contado a partir de la activación o entrega de la licencia.
- Solución de seguridad endpoint con capacidades de antivirus, antimalware, protección contra ransomware, EDR o XDR, detección, alertamiento, investigación y respuesta ante amenazas.
- Consola de administración centralizada, en nube, local o híbrida, o mecanismo administrado equivalente, para gestionar políticas, alertas, reportes, eventos y estado de los equipos protegidos.
- Compatibilidad con la última versión de Windows 10 utilizada por la Entidad, con Windows 11 x64 y Rocky Linux.
- Configuración inicial, puesta en marcha y validación de operación de la solución.
- Instalación, actualización o despliegue de agentes de forma centralizada, administrada o asistida. En caso de cambio de solución, el contratista deberá incluir acompañamiento para la desinstalación o retiro controlado del agente actual y la instalación del nuevo agente.
- Soporte técnico durante la vigencia del licenciamiento, con canales de atención, tiempos de respuesta y protocolo de soporte.
- Transferencia de conocimiento para el personal técnico designado por la UAESPE.
- Entrega de documentación, reporte de instalación, reporte de licenciamiento activo, evidencia de consola operativa y acta o informe de puesta en marcha.

2.2. ESPECIFICACIONES TÉCNICAS GENERALES

No.	Componente	Condición Técnica Mínima
1	Cobertura	La solución debe cubrir 85 equipos endpoint de propiedad de la UAESPE.
2	Tipo de solución	Seguridad endpoint con capacidades de antivirus, antimalware, EDR o XDR, detección y respuesta.
3	Compatibilidad	Debe soportar Windows 10, Windows 11 x64 y Rocky linux, de acuerdo con las versiones instaladas en la Entidad.
4	Consola	Debe contar con consola centralizada o mecanismo administrado equivalente para gestión de políticas, alertas, eventos y reportes.
5	Protección antimalware	Debe detectar, bloquear, limpiar, poner en cuarentena o eliminar malware, virus, spyware, troyanos, ransomware y amenazas conocidas o emergentes.
6	EDR/XDR	Debe permitir detección avanzada, investigación y respuesta ante incidentes en los equipos endpoint.

No.	Componente	Condición Técnica Mínima
7	Respuesta remota	Debe permitir acciones como aislamiento del equipo, cuarentena, eliminación de archivo, bloqueo de ejecución, terminación de procesos o acciones equivalentes.
8	Telemetría y eventos	Debe recolectar eventos relevantes del endpoint para alertamiento, análisis, trazabilidad e investigación de amenazas.
9	Integraciones	Debe permitir exportar, consultar o notificar eventos mediante API REST, syslog, correo electrónico, archivo de log, SIEM o mecanismo equivalente, para integración directa o indirecta con herramientas de monitoreo o mesa de servicios, tales como Zabbix y GLPI.
10	Sandbox o análisis equivalente	Debe permitir análisis de archivos, adjuntos, URLs, hashes o artefactos sospechosos mediante sandbox, reputación, inteligencia de amenazas, detonación en nube, motor de comportamiento o mecanismo equivalente.
11	Instalación	La instalación, actualización, renovación o despliegue de agentes deberá poder realizarse de forma centralizada, administrada o asistida mediante funcionalidades propias, herramientas del fabricante, o mecanismos del proveedor.
12	Soporte	Debe incluir soporte técnico durante la vigencia, con canales de atención y protocolo de escalamiento.
13	Capacitación	Debe incluir transferencia de conocimiento al personal técnico designado por la UAESPE.
14	Entregables	Debe entregar evidencia de licenciamiento, consola operativa, reporte de equipos protegidos, políticas aplicadas, informe de puesta en marcha y documentación técnica.

3. FUNDAMENTOS JURÍDICOS QUE SOPORTAN LA MODALIDAD DE SELECCIÓN

A este proceso de selección y al contrato que de él se derive le son aplicables los principios y normas de la Constitución Política, la Ley 80 de 1993, la Ley 1150 de 2007, la Ley 1474 de 2011, la Ley 1882 de 2018, la Ley 2069 de 2020, el Decreto 1082 de 2015, el Decreto 1860 de 2021 y demás normas concordantes o complementarias. Para los aspectos no regulados en las normas anteriores se aplicarán las normas comerciales y civiles pertinentes, así como las reglas previstas en la invitación pública y documentos del proceso.

La modalidad de selección adoptada para el presente proceso es la SELECCIÓN DE MÍNIMA CUANTÍA, teniendo en cuenta que el valor estimado de la contratación no excede el diez por ciento (10%) de la menor cuantía de la Entidad.

El numeral 5 del artículo 2 de la Ley 1150 de 2007, modificado por el artículo 30 de la Ley 2069 de 2020, establece que la contratación cuyo valor no excede el 10% de la menor cuantía de la entidad, independientemente de su objeto, se efectuará bajo la modalidad de mínima cuantía. Bajo esta modalidad se publicará una invitación por un término no inferior a un día hábil, el término para presentar oferta no podrá ser inferior a un día hábil,

la entidad seleccionará la propuesta de menor precio que cumpla las condiciones exigidas, y la comunicación de aceptación junto con la oferta constituirán el contrato estatal.

De acuerdo con la información suministrada para la vigencia 2026, la mínima cuantía de la UAESPE corresponde a CUARENTA Y OCHO MILLONES NOVECIENTOS DOCE MIL SEISCIENTOS NOVENTA Y SEIS PESOS M/CTE ($48.912.696). Por tanto, el presente proceso se adelantará bajo la modalidad de mínima cuantía, siempre que el presupuesto oficial definitivo se mantenga igual o inferior a dicho umbral.

El proceso se adelantará a través de SECOP II, plataforma en la cual se publicarán los documentos del proceso, se recibirán observaciones, se recibirán ofertas, se realizará la evaluación correspondiente, se publicará el informe de evaluación y se comunicará la aceptación de la oferta que cumpla los requisitos y presente el menor precio.

3.1. TIPO DE CONTRATO

El contrato corresponde a una compraventa de licenciamiento de software con servicios complementarios de configuración, soporte técnico, puesta en marcha, transferencia de conocimiento y acompañamiento técnico.

4. ESTUDIO HISTÓRICO DE LA DEMANDA

En los últimos años la Entidad ha adelantado procesos relacionados con la adquisición o renovación de soluciones de seguridad endpoint para proteger los equipos institucionales. Como antecedente técnico, en el Contrato No. 052 de 2023 se estructuró la renovación de licenciamiento antivirus Kaspersky Endpoint Detection and Response Optimum, incluyendo licencias, soporte por un año y una bolsa de horas de afinamiento, lo cual sirve como referencia histórica del tipo de necesidad, sin que constituya una exigencia de marca para el presente proceso.

Vigencia	Proceso / contrato	Objeto / Alcance	Cantidad	Valor
2023	Contrato No. 052 de 2023 - ITSEC SAS	Renovación de licenciamiento antivirus Kaspersky Endpoint Detection and Response Optimum, soporte por un año y bolsa de afinamiento.	100 licencias	$23.510.000,00
2024	CONTRATO No. 108 DE 2024	Renovar el licenciamiento del antivirus kaspersky next edr optimum, incluido los servicios de configuración, soporte, afinamiento y puesta en marcha de la solución.	100 licencias	$12.499.000,00
2025	CONTRATO No. 114 DE 2025	Renovar el licenciamiento del antivirus Kaspersky Next EDR Optimum, incluido los servicios de configuración, soporte,	89 licencias	$13.623.853,00

Vigencia	Proceso / contrato	Objeto / Alcance	Cantidad	Valor
		afinamiento y puesta en marcha de la solución		

4.2. HISTÓRICO DE ADQUISICIONES DE OTRAS ENTIDADES

Para complementar el estudio de mercado se consultaron procesos publicados en SECOP II, Tienda Virtual del Estado Colombiano y demás fuentes públicas sobre adquisiciones similares de soluciones antivirus, EDR, XDR o seguridad endpoint por parte de entidades estatales. Los resultados finales de la consulta forman parte del estudio de sector o estudio de mercado.

Proceso / contrato	Entidad	Descripción	Cantidad	Valor
MC-013-2026	MUNICIPIO DE DAGUA	ADQUISICIÓN DE LICENCIAS DE ANTIVIRUS PARA LOS COMPUTADORES DE LA ALCALDÍA DEL MUNICIPIO DE DAGUA - VALLE DEL CAUCA.	82	$20.500.000,00
MC-021-2026	CORPORACIÓN AUTÓNOMA REGIONAL DE CUNDINAMARCA (CAR)	Renovación de licencias de antivirus para los equipos informáticos de la alcaldía municipal de Chinchiná, Caldas.	270	$28.527.600,00
CTO-1361-2025	UNIDAD DE SALUD DE IBAGUE	CONTRATAR LA RENOVACION POR UN AÑO DE 300 LICENCIAS DE USO DEL ANTIVIRUS KASPERDKY ENSPOINT SECURITY FOR BUSINESS SELECT, ACTUALMENTE DENOMINADO ENDPOINT KAPERSKY ON PREMISE NEXT EDR OPTIMUM UTILIZADO	300	$23.130.000,00
2026.10.05.05.495	Departamento General y de Servicios Administrativos (La Ceja Antioquia)	Antivirus más consola web, IA que permita administrar todos los sistemas operativos (Windows 11, 10, 8.1, 8 y 7, servidores con server 2012 y 2019) de la administración	450	$29.786.400,00

Proceso / contrato	Entidad	Descripción	Cantidad	Valor
INVITACIÓN PÚBLICA DE MÍNIMA CUANTÍA No. MC – 021-2026	Alcaldía Municipal Calarcá Quindío	ADQUISICIÓN DE LICENCIAS DE SOFTWARE DE SEGURIDAD INFORMÁTICA, ANTIVIRUS DESTINADAS A GARANTIZAR EL SOPORTE, MANTENIMIENTO Y PROTECCIÓN DE LOS SISTEMAS INFORMÁTICOS DE LAS DEPENDENCIAS DE LA ALCALDÍA DE CALARCÁ Y DEMÁS ESPACIOS PÚBLICOS DEL MUNICIPIO	100	$13.578.000,00
SA 003 2026 (Manifestación de interés (Menor Cuantía)) (Presentación de oferta)	MUNICIPIO DE RIONEGRO - ANTIOQUIA	RENOVACIÓN Y ACTUALIZACIÓN DEL LICENCIAMIENTO ANTIVIRUS ESET PROTECT ELITE CLOUD PARA EL MUNICIPIO DE RIONEGRO - ANTIOQUIA	1000	$155.247.040
MC-MCM-2026-0011	Museo Casa de la Memoria - Medellín	ADQUISICIÓN DE LICENCIAMIENTOS ANTIVIRUS Y PUNTOS DE ACCESO INALÁMBRICO PARA INTERIORES CORPORATIVA DE LA AGENCIA PARA LA INFRAESTRUCTURA DEL META	68	$6.888.400

5. PLAN ANUAL DE ADQUISICIONES

Una vez revisado el Plan Anual de Adquisiciones de la Entidad para la vigencia 2026, se evidencia que la necesidad se encuentra contemplada dentro de la planeación contractual de la UAESPE y está descrita en el Sistema Electrónico para la Contratación Pública www.contratos.gov.co o www.colombiacompra.gov.co.

6. CLASIFICACIÓN UNSPSC

El objeto contractual se enmarca principalmente en los siguientes códigos del Clasificador de Bienes y Servicios de Naciones Unidas - UNSPSC, sin perjuicio de que el Grupo de Contratación valide el código final aplicable en SECOP II:

Código	Segmento	Familia	Clase	Producto / Descripción
43233205	43 - Difusión de Tecnologías de Información y Telecomunicaciones	4323 - Software	432332 - Software de seguridad y protección	Software de seguridad de transacciones y de protección contra virus. Código recomendado para licenciamiento antivirus / protección contra virus.
43233200	43 - Difusión de Tecnologías de Información y Telecomunicaciones	4323 - Software	432332 - Software de seguridad y protección	Clase general de software de seguridad y protección.
81112200	81 - Servicios basados en ingeniería, investigación y tecnología	8111 - Servicios informáticos	811122 - Mantenimiento y soporte de software	Puede aplicar a servicios complementarios de soporte, mantenimiento o acompañamiento, si contratación lo considera pertinente.

7. VALOR ESTIMADO DEL PRESUPUESTO Y JUSTIFICACIÓN DEL MISMO

7.1. ANÁLISIS DE LA OFERTA.

Para determinar el valor estimado del proceso, la Entidad adelanta estudio de mercado mediante Solicitud de Información a Proveedores / solicitud de cotizaciones a través de SECOP II. La solicitud debe incluir el anexo técnico, el formato de oferta económica y la matriz de cumplimiento, con el fin de obtener cotizaciones comparables sobre licenciamiento, configuración, soporte, puesta en marcha, capacitación y demás componentes necesarios para dejar operativa la solución.

Las cotizaciones deben presentar, como mínimo, la descripción del producto, fabricante, edición, cantidad de licencias, valor unitario, IVA, valor total, horas de capacitación, horas de soporte, horas de afinamiento si aplica, alcance de instalación, migración y costos adicionales. Las cotizaciones recibidas en esta etapa serán utilizadas exclusivamente como insumo de planeación y no constituyen oferta formal dentro del proceso de mínima cuantía. La solicitud de cotizaciones del proceso PE-SIP-CD-008-2026 de SECOP II fue atendida por los siguientes oferentes:

Proveedor	Producto / edición ofertada	Cantidad	Valor total incluido IVA	Valor unitario	Observaciones
HIGH TECH SERVICES CORP (HTS CORP) S.A.S.	TREND MICRO	85	$53.218.500	$626.100	Supera el tope de mínima cuantía; incluye 20 horas de soporte y 20 horas de afinamiento valorizadas como ítems independientes. Producto distinto a la línea base.
SINERGY & LOWELLS SAS	BITDEFENDER	85	$110.699.750	$1.302.350	Valor altamente superior al histórico institucional y al tope de mínima cuantía; incluye configuración, migración, capacitación, soporte, afinamiento, integración y otros componentes.

8. PRESUPUESTO OFICIAL ESTIMADO Y JUSTIFICACIÓN

Para la determinación del presupuesto oficial del presente proceso, la Entidad tomó como base principal los valores efectivamente adjudicados en las tres últimas contrataciones relacionadas con soluciones antivirus, EDR o seguridad endpoint, por cuanto estos reflejan el comportamiento real de contratación de la UAESPE para necesidades funcionalmente comparables, con vigencia anual, licenciamiento para equipos institucionales y servicios asociados de configuración, soporte, afinamiento o puesta en marcha.

La Entidad no toma como base exclusiva las cotizaciones recibidas en la solicitud de información publicada en SECOP II, toda vez que únicamente se recibieron dos cotizaciones y sus valores presentan una diferencia significativa frente al histórico institucional, al presupuesto previsto en el Plan Anual de Adquisiciones y al alcance mínimo requerido para el presente proceso. Dichas cotizaciones se conservan como referencia complementaria de mercado, pero no se consideran representativas por sí solas para fijar el presupuesto oficial.

Para evitar que el presupuesto se limite al valor adjudicado histórico sin reconocer las condiciones actuales del proceso, la Entidad aplicó una metodología de corrección y actualización compuesta por los siguientes elementos:

1. Normalización de los valores adjudicados históricos a valor unitario por licencia o endpoint.
2. Ajuste de dichos valores a la cantidad actual requerida por la Entidad, correspondiente a ochenta y cinco (85) endpoints.
3. Actualización de los valores históricos a precios de la vigencia 2026, utilizando como referencia los factores de variación del IPC disponibles para las vigencias 2024, 2025 y 2026.
4. Aplicación de un factor de ajuste tecnológico del ocho por ciento (8%), teniendo en cuenta que el alcance actual no se limita a una renovación simple de antivirus, sino que incorpora capacidades de antivirus, EDR o XDR, detección y respuesta, consola o mecanismo de administración, configuración, soporte, puesta en marcha, análisis de artefactos sospechosos y posibilidades de integración o entrega de eventos hacia herramientas institucionales.
5. Aplicación de un factor de movilidad de oferentes del uno por ciento (1%), con el fin de evitar que el presupuesto oficial quede restringido exclusivamente al comportamiento adjudicado histórico y permita una participación razonable de posibles oferentes.
6. Aplicación de un factor de redondeo y variación menor de mercado del uno por ciento (1%), orientado a cubrir diferencias menores asociadas a costos de soporte, activación, puesta en marcha, variación de precios, impuestos, tasas, contribuciones u otros costos indirectos necesarios para dejar operativa la solución.

Como resultado de esta metodología, el valor base derivado del promedio de los valores adjudicados históricos, una vez normalizado, actualizado y ajustado a la cantidad actual de endpoints, arroja una referencia aproximada de $16.096.599. Al aplicar los factores de ajuste señalados, se obtiene un valor estimado aproximado de $17.706.259.

En consecuencia, y con el fin de establecer un presupuesto razonable, proporcional, trazable y compatible con la modalidad de mínima cuantía, la Entidad estima procedente fijar el presupuesto oficial en la suma de DIECIOCHO MILLONES DE PESOS M/CTE ($18.000.000), incluido IVA, impuestos, tasas, contribuciones, costos directos e indirectos, configuración, soporte, puesta en marcha y demás costos asociados a la correcta ejecución del objeto contractual.

Esta estimación permite reconocer el comportamiento histórico real de contratación de la UAESPE, actualizar los valores a condiciones de la vigencia 2026, dar un margen razonable de movilidad a los oferentes y mantener el proceso dentro del umbral de mínima cuantía aplicable a la Entidad.

9. CERTIFICADO DE DISPONIBILIDAD PRESUPUESTAL

La presente contratación cuenta con Certificado de Disponibilidad Presupuestal N° 16326 del 19 de junio de 2026 por valor de DIECIOCHO MILLONES OCHOCIENTOS MCTE ($18.000.000) expedido por el Coordinador del Grupo Financiero de la Unidad.

10. ANÁLISIS DE RIESGO Y FORMA DE MITIGARLO

De conformidad con el artículo 4 de la Ley 1150 de 2007 y el Decreto 1082 de 2015, la Entidad debe incluir la estimación, tipificación y asignación de los riesgos previsibles involucrados en la contratación. Para el presente proceso se identifican los siguientes riesgos previsibles:

No	Riesgo identificado	Consecuencia	Prob.	Impacto	Valoración	Asignación	Tratamiento / controles
1	No activación oportuna del licenciamiento endpoint o fallas en la instalación de agentes. Clase: específico. Fuente: externa. Etapa: ejecución. Tipo: operacional.	Equipos sin protección o pérdida de continuidad del control antivirus/EDR.	3 Posible	4 Mayor	7 Alto	Contratista	Plan de implementación, cronograma, evidencias de activación, validación de consola y reporte de equipos protegidos.
2	La solución ofertada no es compatible con las versiones de Windows 10, Windows 11 o Rocky linux instaladas en la Entidad. Clase: específico. Fuente: externa. Etapa: ejecución. Tipo: tecnológico.	Imposibilidad de proteger todos los equipos objeto del contrato o necesidad de actividades no previstas.	2 Improbable	4 Mayor	6 Medio	Contratista	Exigir matriz técnica, ficha del fabricante y validación previa de compatibilidad antes de aceptación a satisfacción.
3	Uso indebido, divulgación o acceso no autorizado a información de la Entidad durante soporte, configuración o análisis de eventos. Clase: general. Fuente: externa. Etapa: ejecución. Tipo: seguridad de la información.	Fuga de información o afectación de confidencialidad institucional.	1 Raro	5 Catastrófico	5 Medio	Compartido	Acuerdo de confidencialidad, accesos controlados, acompañamiento del supervisor, mínimo privilegio y registro de actividades.
4	Dificultades en la migración si la solución seleccionada es diferente a la actualmente instalada.	Conflictos entre agentes, equipos sin protección o retrasos en la implementación.	3 Posible	3 Moderado	6 Medio	Contratista	Plan de migración, desinstalación controlada, instalación administrada, pruebas por

No	Riesgo identificado	Consecuencia	Prob.	Impacto	Valoración	Asignación	Tratamiento / controles
	Clase: específico. Fuente: interna/externa. Etapa: ejecución. Tipo: operacional.						muestra y validación final.
5	Ofertas incompletas o no comparables por exclusión de soporte, capacitación, puesta en marcha, IVA o costos asociados. Clase: general. Fuente: externa. Etapa: selección. Tipo: económico.	Distorsión del presupuesto oficial y riesgo de selección de oferta no integral.	3 Posible	3 Moderado	6 Medio	Entidad	Formato económico estandarizado, aclaraciones en SECOP II y evaluación del menor precio total que cumpla requisitos.

Forma de mitigación y seguimiento: el supervisor del contrato verificará la entrega oportuna de licencias, la activación de la consola, la instalación de agentes, la configuración de políticas, la entrega de documentación, el protocolo de soporte, las evidencias de puesta en marcha y la transferencia de conocimiento. Los riesgos se monitorearán durante la ejecución del contrato y hasta la recepción a satisfacción de los entregables.

11. GARANTÍAS QUE LA ENTIDAD ESTATAL CONTEMPLA EXIGIR EN EL PROCESO DE CONTRATACIÓN

Teniendo en cuenta la naturaleza del objeto y alcance de las obligaciones del contrato, independientemente del valor del mismo y de conformidad con numeral 7° del artículo 2.2.1.1.2.1.1. del Decreto 1082 de 2015, se ha considerado necesario que el proveedor constituya una garantía única que avale el cumplimiento de las obligaciones surgidas en el contrato, en los siguientes términos y porcentajes.

Amparo	Valor asegurado sugerido	Vigencia sugerida
Cumplimiento	Veinte por ciento (20%) del valor del contrato.	Plazo de ejecución del contrato y seis (6) meses más.

El contratista deberá constituir y cargar las garantías en SECOP II dentro del término previsto en los documentos del proceso, y mantenerlas vigentes durante la ejecución contractual.

Pago de salarios, prestaciones sociales legales e indemnizaciones laborales: La Entidad no exigirá este amparo, teniendo en cuenta que el objeto contractual corresponde principalmente al suministro o renovación de licenciamiento de software de seguridad

endpoint, y que los servicios de configuración, instalación, puesta en marcha, capacitación y soporte tienen carácter complementario, puntual y especializado. El proceso no exige personal dedicado, permanente o exclusivo para la UAESPE, ni contempla actividades intensivas en mano de obra que generen una exposición laboral significativa para la Entidad.

Adicionalmente, el contratista deberá acreditar el cumplimiento de sus obligaciones frente al Sistema de Seguridad Social Integral y aportes parafiscales, cuando corresponda. En consecuencia, conforme al análisis de riesgos y atendiendo a los principios de proporcionalidad y razonabilidad, no se identifica la necesidad de exigir el amparo de pago de salarios, prestaciones sociales legales e indemnizaciones laborales.

12. INDICACIÓN DE SI LA CONTRATACIÓN RESPECTIVA ESTÁ COBIJADA POR UN ACUERDO INTERNACIONAL O TRATADO DE LIBRE COMERCIO

En cumplimiento del numeral 8 del artículo 2.2.1.1.2.1.1 del Decreto 1082 de 2015, la Entidad debe establecer si el presente proceso está cobijado por un Acuerdo Comercial. Teniendo en cuenta que se trata de un proceso de mínima cuantía cuyo valor estimado se encuentra por debajo de los umbrales aplicables, se deberá diligenciar la matriz de acuerdos comerciales con la validación correspondiente del Grupo de Contratación.

Acuerdo comercial	Entidad estatal incluida	Valor superior al umbral	Excepción aplicable	Proceso cubierto
Alianza del Pacífico - Chile	Sí	No	No	No
Alianza del Pacífico - México	Sí	No	No	No
8. No instalar software adicional, agentes, herramientas, scripts o componentes no autorizados por la UAESPE. Comunidad Andina	Sí	No	No	No
Alianza del Pacífico - Perú	Sí	No	No	No
Canadá	Sí	No	No	No
Chile	Sí	No	No	No
Corea	Sí	No	No	No
Costa Rica	Sí	No	No	No
Estados AELC	Sí	No	No	No
Estados Unidos	Sí	No	No	No
México	Sí	No	No	No
Unión Europea	Sí	No	No	No

13. CONDICIONES CONTRACTUALES

13.1. OBLIGACIONES DEL CONTRATO

13.1.1. OBLIGACIONES GENERALES DEL CONTRATISTA

1. Asumir los riesgos establecidos en la matriz de riesgos del proceso que le sean asignados.
2. Acreditar el pago de aportes al Sistema de Seguridad Social Integral y parafiscales, cuando aplique, conforme a la normatividad vigente.
3. Responder por el pago de tributos, tasas, contribuciones y demás costos que se causen con ocasión de la celebración, ejecución y liquidación del contrato, cuando haya lugar.
4. Presentar y cargar en SECOP II los informes de ejecución, soportes, factura electrónica o documento equivalente, y demás documentos requeridos para el pago.
5. Atender los requerimientos, instrucciones y recomendaciones del supervisor del contrato para el cumplimiento oportuno e idóneo del objeto contractual.
6. Guardar estricta reserva sobre la información, documentos, configuraciones, políticas, eventos, logs, reportes y demás información institucional a la que tenga acceso en desarrollo del contrato.
7. Utilizar los accesos, información y recursos de la Entidad únicamente para las actividades autorizadas en el contrato.
9. Mantener vigentes las garantías que se exijan, si a ello hubiere lugar, y cargarlas en SECOP II para revisión y aprobación.
10. Entregar la documentación física o electrónica generada durante la ejecución del contrato.
11. Cumplir las políticas internas de seguridad de la información, protección de datos, uso aceptable de recursos tecnológicos y demás lineamientos aplicables de la UAESPE.
12. Las demás inherentes al objeto, la naturaleza del contrato, la buena fe y las indicadas por el supervisor para el cabal cumplimiento del objeto contractual.

13.1.2 OBLIGACIONES ESPECÍFICAS DEL CONTRATISTA

1. Cumplir a cabalidad el objeto del contrato, de acuerdo con los términos y condiciones pactadas, el estudio previo, anexo técnico, invitación pública, oferta presentada y demás documentos del proceso.
2. Entregar licenciamiento válido, legal, vigente y soportado por el fabricante para ochenta y cinco (85) equipos endpoint de propiedad de la UAESPE.
3. Garantizar que la solución ofertada cuente con capacidades de antivirus, antimalware, protección contra ransomware, EDR o XDR, detección, alertamiento, investigación y respuesta ante amenazas.
4. Configurar o habilitar la consola de administración centralizada, en nube, local o híbrida, o mecanismo administrado equivalente, de acuerdo con la solución ofertada.
5. Configurar políticas iniciales de protección, actualización, alertamiento, reportes, grupos de equipos y parámetros básicos definidos con la Entidad.

6. Realizar o acompañar la instalación, actualización, renovación o despliegue de agentes en los equipos objeto del contrato mediante mecanismo centralizado, administrado o asistido.
7. En caso de ofertar una solución diferente a la actualmente instalada, realizar o acompañar la desinstalación o retiro controlado del agente actual, instalación del nuevo agente y validación de protección de los equipos.
8. Realizar pruebas de operación que evidencien comunicación de agentes con consola, estado de protección, actualización, generación de alertas y reportes.
9. Entregar protocolo de soporte donde se indiquen canales de atención, horario, tiempos de respuesta, escalamiento y personal o mesa de soporte designada.
10. Atender los requerimientos de soporte durante la vigencia del licenciamiento, de acuerdo con los canales y tiempos ofrecidos.
11. Realizar transferencia de conocimiento al personal técnico designado por la UAESPE sobre administración básica, alertas, reportes, políticas, instalación y respuesta inicial ante eventos.
12. Entregar informe de puesta en marcha, reporte de equipos protegidos, reporte de políticas aplicadas, evidencia de licenciamiento y documentación técnica del fabricante.
13. Informar en la oferta y antes del inicio de la implementación todas las limitaciones técnicas, operativas o de licenciamiento, prerrequisitos, incompatibilidades, dependencias, componentes adicionales o restricciones de uso de la solución ofertada que puedan afectar su instalación, migración, administración, integración, soporte u operación en el ambiente tecnológico de la UAESPE.
    La información deberá incluir, cuando aplique, requerimientos de sistemas operativos, infraestructura, hardware, conectividad, puertos, proxy, privilegios de instalación, herramientas de despliegue, coexistencia con otros agentes, licencias o módulos adicionales, límites de almacenamiento o retención, capacidades de integración y condiciones de operación en nube.
    Las limitaciones informadas no podrán implicar el incumplimiento de las condiciones técnicas mínimas. Todo prerrequisito, componente, licencia o servicio necesario para dejar la solución operativa deberá estar incluido en la oferta económica, sin generar costos adicionales para la Entidad durante la ejecución contractual.

.

14. Mantener confidencialidad sobre la información institucional y suscribir el compromiso de confidencialidad cuando sea requerido.

13.2. OBLIGACIONES DE LA UAESPE

1. Realizar el pago del valor del contrato conforme a lo pactado y previo cumplimiento de los requisitos de pago.
2. Entregar al contratista la información necesaria para la ejecución del contrato, incluyendo la cantidad de equipos y responsables técnicos designados.
3. Designar el supervisor del contrato.
4. Exigir al contratista la ejecución idónea y oportuna del objeto contractual.

5. Facilitar, dentro de sus posibilidades, el acceso técnico necesario para instalación, configuración y validación de la solución, previa coordinación con el supervisor.
6. Validar y aprobar los entregables presentados por el contratista cuando cumplan las condiciones pactadas.
7. Coordinar ventanas de trabajo, autorizaciones de acceso remoto y acompañamiento técnico cuando se requiera.
8. Adelantar las acciones conducentes a obtener la indemnización de los daños que sufra en desarrollo o con ocasión del contrato, cuando haya lugar.
9. Ejercer supervisión y control a la ejecución del contrato a través de la persona designada por el ordenador del gasto.

14. FORMA DE PAGO

La Unidad Administrativa Especial del Servicio Público de Empleo - UAESPE pagará el valor del contrato resultante de la siguiente manera:

Un (1) único pago, previa entrega, activación y puesta en marcha de la solución de seguridad endpoint para 85 equipos, conforme al anexo técnico, la oferta presentada y los documentos del proceso; previa presentación de factura electrónica o documento equivalente, recibo a satisfacción del supervisor, certificación de pago de aportes al Sistema de Seguridad Social Integral y parafiscales cuando aplique, certificación bancaria, RUT y demás documentos requeridos para el trámite de pago.

Los pagos estarán sujetos a la programación de recursos del Programa Anual de Caja - PAC y a los descuentos de ley aplicables. La factura electrónica deberá cumplir con los requisitos del SIIF Nación y las instrucciones vigentes de la Entidad para recepción y gestión de documentos electrónicos.

15. SUPERVISIÓN DEL CONTRATO

La supervisión de la presente contratación será ejercida por la Subdirectora de Desarrollo y Tecnología o por quien designe expresamente el ordenador del gasto, de conformidad con las competencias internas de la UAESPE y con lo previsto en los artículos 83 y 84 de la Ley 1474 de 2011, el manual interno de contratación y supervisión de la Entidad. El supervisor será responsable del seguimiento técnico, administrativo, financiero y jurídico de la ejecución, así como de la verificación del cumplimiento de las obligaciones a cargo del proveedor. La Entidad deberá designar formalmente el supervisor y comunicar dicha designación al proveedor.

16. PLAZO DE EJECUCIÓN

El plazo del contrato será de 15 días hábiles, los cuales empezarán a contar con la suscripción del acta de inicio, previo cumplimiento de los requisitos de perfeccionamiento y ejecución del contrato, sin perjuicio de que las licencias que se adquieren por medio del

presente contrato son por el término de un (1) año, razón por la cual el contratista deberá mantener las prestaciones de estas por ese término específico.

Durante el término de esos 15 días hábiles, el contratista deberá entregar a satisfacción las licencias de los productos adquiridos, y haber realizado la correcta instalación y puesta en funcionamiento de las mismas en los equipos de cómputo, así como haber realizado todas las actividades conexas descritas.

17. LUGAR DE EJECUCIÓN DEL CONTRATO

El domicilio contractual será la ciudad de Bogotá D.C. y el lugar de ejecución será la sede de la UAESPE ubicada en la Carrera 7 No. 31 - 10 pisos 13 y 14 de Bogotá D.C., así como los equipos de propiedad de la Entidad objeto de protección. Las actividades podrán ejecutarse de forma presencial, remota o híbrida, previa coordinación con el supervisor del contrato y observando las políticas de seguridad de la información de la Entidad.

18. INHABILIDADES E INCOMPATIBILIDADES PARA CONTRATAR

Aplican las inhabilidades e incompatibilidades para contratar previstas en la Constitución Política y en las leyes, en particular las establecidas en la Ley 80 de 1993, Ley 1150 de 2007, Ley 1474 de 2011 y demás normas que las modifiquen, adicionen o sustituyan. Los proponentes deberán declarar que no se encuentran incursos en causales de inhabilidad, incompatibilidad o conflicto de interés para contratar con la Entidad.

19. CRITERIOS PARA SELECCIONAR LA OFERTA MÁS FAVORABLE

En este proceso podrán participar personas naturales o jurídicas, nacionales o extranjeras, directamente o mediante consorcios o uniones temporales, cuyo objeto social comprenda actividades relacionadas con el suministro, comercialización, implementación, soporte o prestación de servicios asociados a soluciones de software de seguridad endpoint, y que cumplan las condiciones jurídicas, técnicas y económicas previstas en la invitación pública. La UAESPE aceptará la oferta de MENOR PRECIO TOTAL OFERTADO, siempre que cumpla con las condiciones jurídicas, técnicas y económicas exigidas en la invitación pública y sus anexos. La Entidad revisará las ofertas económicas y verificará inicialmente la oferta de menor precio. Si esta no cumple con las condiciones exigidas, se verificará la oferta con el segundo menor precio, y así sucesivamente.

19.1. REQUISITOS HABILITANTES

Requisito	Tipo de verificación	Condición
Verificación jurídica	Habilitante	Cumplimiento de capacidad jurídica, existencia y representación legal, ausencia de inhabilidades e incompatibilidades, y demás documentos exigidos.

Verificación técnica	Habilitante	Aceptación y cumplimiento de las condiciones técnicas mínimas del anexo técnico y matriz de cumplimiento.
Verificación económica	Habilitante / evaluación por precio	Presentación del formato de oferta económica completo, sin superar el presupuesto oficial y con inclusión de IVA y demás costos.

19.2. REQUISITOS TÉCNICOS

El proponente deberá diligenciar el formato de carta de aceptación de especificaciones técnicas, declarando que conoce, entiende y acepta los requisitos técnicos descritos en el estudio previo, anexo técnico, invitación pública y demás documentos del proceso. La omisión de requisitos esenciales o la presentación de una solución que no cubra los 85 endpoints o que no incluya las capacidades mínimas de antivirus, EDR o XDR, detección y respuesta, podrá dar lugar a la no habilitación técnica de la oferta.

19.3. EXPERIENCIA MÍNIMA REQUERIDA DEL PROPONENTE

El proponente debe acreditar experiencia con máximo hasta 3 contratos ejecutados que de manera individual o sumados contemplen el 100% del valor estimado del presupuesto del presente proceso, que reúna y permita evidenciar las siguientes condiciones:

a) Razón social de la empresa o entidad contratante.
b) Nombre del contratista.
c) Objeto del contrato y/u obligaciones relacionado con la venta, instalación, configuración, soporte, afinamiento y puesta en funcionamiento de soluciones de Antivirus.
d) Fecha de inicio y fin de ejecución: Dentro de los últimos cuatro (4) años anteriores al cierre del presente proceso.

Nota: La Entidad solicita que la experiencia presentada por el proponente corresponda a contratos ejecutados y terminados dentro de los cuatro (4) años anteriores a la fecha de cierre del proceso. Esta condición se establece teniendo en cuenta la naturaleza tecnológica, dinámica y especializada del objeto contractual, y busca verificar que el proponente haya participado recientemente en la provisión, renovación, implementación, configuración o soporte de soluciones de seguridad endpoint con características funcionales relacionadas con la necesidad actual de la UAESPE.

El objeto del proceso no se limita al suministro de un antivirus tradicional. Comprende una solución con capacidades de antivirus, antimalware, EDR o XDR, detección, investigación y respuesta; consola de administración centralizada; recolección de telemetría; generación de alertas; acciones remotas de contención; análisis de archivos, URL, hashes o artefactos sospechosos; mecanismos de integración o entrega de eventos; instalación o migración de agentes; soporte técnico y puesta en marcha.

Estas capacidades han evolucionado de manera significativa y requieren que el proveedor conozca modelos actuales de licenciamiento por suscripción, consolas locales o en nube,

políticas de protección, mecanismos de despliegue, gestión de alertas, investigación de eventos y acciones de respuesta. Por tal razón, la experiencia reciente permite reducir el riesgo de que el contratista únicamente acredite contratos antiguos relacionados con antivirus convencional, sin demostrar participación reciente en soluciones que incorporen las capacidades técnicas y operativas requeridas actualmente por la Entidad.

La exigencia de cuatro (4) años se definió como una ventana temporal razonable que permite verificar actualidad técnica sin limitar la experiencia a un período excesivamente corto. Este término comprende varias vigencias anuales de licenciamiento, renovación, implementación y soporte de soluciones endpoint, lo que permite que los proveedores acrediten experiencia obtenida con entidades públicas o privadas durante un período suficientemente amplio.

La experiencia podrá estar relacionada con el suministro, renovación, implementación, configuración, soporte o puesta en marcha de soluciones antivirus, EPP, EDR, XDR, seguridad endpoint o software de seguridad y protección. No se exigirá que el objeto de los contratos acreditados sea idéntico al objeto del presente proceso, siempre que las actividades ejecutadas permitan verificar conocimiento y capacidad para atender sus componentes principales.

a) Valor: El valor del contrato sea igual o superior al 100% del presupuesto oficial estimado para esta contratación, expresado en pesos colombianos.
b) Porcentaje de participación en el Consorcio o Unión Temporal, si la certificación se expide para un contrato ejecutado bajo alguna de estas figuras
c) Fechas de suspensión y reinicio en caso de que se haya presentado suspensión de la ejecución del contrato.
d) Nombre y Firma de quien expide la certificación.

Se tendrán en cuenta para la verificación aquellas certificaciones que reúnan la totalidad de los requisitos exigidos en los presentes estudios previos. No obstante, lo anterior, la Entidad podrá verificar la información contenida y podrá solicitar aclaraciones sobre los datos consignados en las certificaciones.

Para demostrar el cumplimiento de este requisito habilitante, además de lo arriba señalado, el proponente diligenciará el ANEXO EXPERIENCIA MÍNIMA REQUERIDA DEL PROPONENTE, o en documento aportado en la propuesta que contenga la misma información establecida en el citado formato.

Para cumplir con el requisito se deberá aportar una certificación y/o copia del acta de liquidación y/o copia del contrato, siempre que se acompañe con la respectiva acta de liquidación o de recibo final, y de ellos se extracte la información requerida en los literales a) al h) del presente numeral.

No se acepta auto-certificaciones, ni cuentas de cobro ni certificaciones expedidas por el o los otros miembros del Consorcio o Uniones Temporales.

De no diligenciarse en la certificación las fechas de la experiencia con día, mes y año, La Unidad del SPE tomará el último día de cada mes como fecha de inicio y el primer día de cada mes como fecha de terminación.

La Entidad se reserva el derecho de verificar la información durante la etapa de evaluación y hasta el término de traslado del informe de evaluación podrá solicitar las aclaraciones sobre el contenido de los documentos y soportes que estime convenientes.

En caso de presentarse certificación de experiencia de contrato ejecutado que contemple la Venta, instalación, configuración y puesta en funcionamiento de Soluciones de Antivirus junto con otros servicios que no se encuentren dentro de lo requerido por la Entidad; esta será tenida en cuenta sólo respecto del valor y objeto concerniente a los servicios requeridos por la Entidad.
Para tal efecto debe el proponente aportar certificación, copia de contrato, acta de liquidación o de recibo final, factura, anexo técnico o cualquier otro documento expedido por el Contratante que permita realizar la verificación del valor y los bienes contratados.

NOTA 1: Si la constitución del Proponente es menor a tres (3) años, puede acreditar esta experiencia con la experiencia registrada de sus accionistas, socios o constituyentes.

NOTA 2: En aplicación del artículo 9 del Decreto-Ley 019 de 2012 "Decreto Ley Anti-trámites", si el proponente ha ejecutado contratos con La Unidad Administrativa Especial del Servicio Público de Empleo, y desea acreditar dicha experiencia, podrá allegar la certificación expedida por La Unidad del SPE, o un documento suscrito por el representante legal donde se mencione el número y año del contrato. i. CERTIFICACIÓN DISTRIBUIDOR AUTORIZADO – PARTNER

El proponente debe ser distribuidor autorizado, para lo cual, debe anexar con la propuesta un Certificado de la casa matriz en donde se le autoriza la distribución de los productos ofertados para Colombia, con fecha de expedición no mayor a dos (2) meses anteriores a la fecha de cierre del proceso, en la que se indique que el oferente es distribuidor autorizado de los productos ofertados y que cuenta con autorización vigente para ofrecer servicios de soporte.

20. CRITERIO DIFERENCIAL PARA MIPYMES

Conforme al artículo 3 del Decreto 1860 de 2021, por el cual se adicionan los artículos 2.2.1.2.4.2.18 del Decreto 1082 de2015, y de acuerdo con el numeral 1° del artículo 33 de la Ley 2069 de 2020, según los resultados del análisis del sector, dentro del proceso se establecerán condiciones habilitantes diferenciales que promuevan y faciliten la participación en los procedimientos de selección competitivos de las Mipymes domiciliadas

en Colombia, incorporando requisitos habilitantes diferenciales relacionados en el valor de los contratos para la acreditación de la experiencia así:

Para acreditar la experiencia conforme con lo establecido en el Decreto 1082 de 2015, el proponente o cualquiera de los miembros del Consorcio o Unión Temporal deberá aportar máximo CUATRO (4) certificaciones de contratos ejecutados y terminados y relacionados con el objeto de este proceso y cuya sumatoria sea igual o superior al 100% de presupuesto oficial.

21. CAUSALES DE RECHAZO

Serán causales de rechazo las previstas en el estudio previo, invitación pública, documentos del proceso y las expresamente señaladas en la ley. La UAESPE rechazará las ofertas, entre otros eventos, cuando:

1. El oferente se encuentre incurso en causal de inhabilidad, incompatibilidad o conflicto de interés.
2. La oferta sea presentada por persona jurídicamente incapaz para obligarse o que no cumpla las condiciones habilitantes exigidas.
3. Se presenten varias ofertas por el mismo oferente, individualmente o como integrante de oferente plural, salvo lo permitido por la normativa aplicable.
4. La oferta contenga condicionamientos que impidan la aceptación pura y simple de las obligaciones y condiciones previstas.
5. El proponente no subsane o subsane incorrectamente o por fuera del término establecido los documentos habilitantes solicitados.
6. La oferta económica supere el presupuesto oficial o no incluya todos los costos requeridos para la ejecución del objeto.
7. La oferta sea presentada de forma extemporánea o por fuera de SECOP II, cuando la plataforma sea el medio establecido para la recepción de ofertas.
8. La Entidad determine que la oferta tiene valor artificialmente bajo y las explicaciones del oferente no resulten suficientes o razonables.
9. El objeto social del oferente no guarde relación con el objeto del proceso.
10. El oferente no acepte o no cumpla las condiciones técnicas mínimas exigidas en el anexo técnico.
11. La solución ofertada no cubra la totalidad de 85 endpoints o no incluya capacidades de antivirus, EDR o XDR, detección y respuesta, soporte, configuración y puesta en marcha.
12. El oferente no presente el formato de oferta económica debidamente diligenciado con ítem, descripción, cantidad, valor unitario, IVA y valor total.

22. CRITERIOS PARA SELECCIONAR LA OFERTA MÁS FAVORABLE

La UAESPE seleccionará, mediante comunicación de aceptación de la oferta, la propuesta con el MENOR PRECIO TOTAL OFERTADO que haya cumplido todas las condiciones exigidas. La comunicación de aceptación junto con la oferta constituirá para todos los

efectos el contrato estatal, con base en lo cual se efectuará el respectivo registro presupuestal.

El menor precio total ofertado corresponderá a la sumatoria de todos los ítems requeridos en el formato de oferta económica, incluidos licenciamiento, configuración, soporte, puesta en marcha, capacitación, horas de soporte o afinamiento cuando aplique, IVA, impuestos y demás costos directos e indirectos necesarios para dejar la solución operativa.

23. DOCUMENTOS ANEXOS

Documento	Archivo	Observación
Estudio del sector	Estudio_Sector_Endpoint	
Anexo técnico	Anexo_Tecnico_Endpoint_UAESPE.xlsx Hojas: 1.Req_Minimos y 1.1.Servicios_Entregables	Debe incluir características técnicas mínimas, soporte, instalación, migración, sandbox e integraciones.
Matriz de cumplimiento técnico	Anexo_Tecnico_Endpoint_UAESPE.xlsx Hojas: 2.Matriz_Proveedor	Diligenciada por los oferentes.
Oferta económica	Anexo_Tecnico_Endpoint_UAESPE.xlsx Hojas: 3.OfertaEconómica	Diligenciada por los oferentes, de acuerdo a la hoja de instrucciones
Carta de aceptación	Anexo_Tecnico_Endpoint_UAESPE.xlsx Hojas: 4.Carta_Aceptacion	Diligenciada por los oferentes.
Experiencia mínima requerida	Anexo_Tecnico_Endpoint_UAESPE.xlsx Hojas: 5.Experiencia_mínima	Diligenciada por los oferentes.
CDP	Documento de 1 página. CDP Antivirus 2026.pdf	Diligenciada por los oferentes y aceptada
Matriz de riesgos	Parte de este documento	Debe ser validada por el oferente

LIBERTAD CORDOBA VARON

Firmado digitalmente por LIBERTAD CORDOBA VARON
Fecha: 2026.06.24 11:01:34 -05'00'

LIBERTAD CORDOBA VARÓN
Subdirectora de Desarrollo y Tecnología

Elaboró: José Manuel Piratoba Lemus – Profesional Especializado -Subdirección de Desarrollo y Tecnología
Revisó: Luis Felipe Salazar Arango- Abogado Contratista / Subdirección de Desarrollo y Tecnología
Aprobó: Libertad Cordoba Varón - Subdirectora de Desarrollo y Tecnología.