

	UNIDAD ADMINISTRATIVA ESPECIAL JUSTICIA PENAL MILITAR Y POLICIAL	Adquisición de Bienes y Servicios	CODIGO: ABS-FO-013
		Formato Estudios Previos Subasta Inversa	VERSIÓN:001
			FECHA VIGENCIA:2023-12-28

ESTUDIOS PREVIOS PARA PROCESO DE SELECCIÓN ABREVIADA POR SUBASTA INVERSA

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

1.1 NECESIDAD - POR QUÉ O PARA QUE SE REQUIERE EL BIEN O SERVICIO, Y CUALES SON LOS RESULTADOS ESPERADOS	La Oficina de Tecnologías de la Información y las Comunicaciones (OTIC) de la Unidad Administrativa Especial de la Justicia Penal Militar y Policial tiene el deber legal y operativo de garantizar la continuidad, disponibilidad, integridad e interoperabilidad de la plataforma tecnológica y los servicios informáticos de la Entidad. Para responder a estas exigencias, LA UNIDAD desde la vigencia 2010, cuenta con una arquitectura integral de ciberseguridad sobre la solución del fabricante Trellix anteriormente llamada McAfee. Esta infraestructura protege la red corporativa, los centros de datos, las instancias en la nube (AWS) y las estaciones de trabajo operativas en los despachos a nivel nacional. Ahora bien, a raíz del incidente de ciberseguridad (Ransomware) presentado en el mes de junio de 2025, la Entidad fortaleció sustancialmente su postura defensiva. En virtud de ello, mediante el Contrato de Compraventa No. 057-2025 se migró de un esquema tradicional de punto final (Suite CEB) hacia una solución avanzada de detección y respuesta gestionada (MDR/EDR), complementada con inspección profunda de red y análisis dinámico de amenazas mediante los componentes Network Security NX Edition, Sistema de Prevención de Intrusiones (IPS NS3600) y el entorno de sandboxing en la nube IVX Enterprise Cloud: Por lo anterior, las suscripciones de licenciamiento y los servicios de soporte técnico anteriormente referidas vencen el próximo 29 de diciembre de 2026, razón por la cual, se requiere con carácter imperativo la renovación del ecosistema de seguridad para las próximas vigencias, con el fin de atender los siguientes criterios técnicos, operativos y económicos: 1. Protección activa en tiempo real: Garantizar la continuidad en la descarga automática de firmas de virus, parches de seguridad, motores heurísticos y el intercambio de inteligencia global de amenazas (Threat Intelligence Exchange - TIE y DTI), evitando que el valor defensivo del software quede obsoleto ante el crecimiento y sofisticación de ataques informáticos. 2. Optimización presupuestal y protecciones de inversión: El Grupo de Plataforma Tecnológica de la Entidad ha adquirido el conocimiento y la
---	---

experiencia requerida para la administración centralizada de la consola ePO (ePolicy Orchestrator) y de las herramientas Trellix. Mantener la misma arquitectura evita sobrecostos por licenciamiento nuevo, migraciones traumáticas o extensas labores de instalación y reconfiguración que generarían costos adicionales a la Entidad.

3. Capacidades integradas de la suite: La solución opera de forma centralizada coordinando la protección de puntos finales mediante Trellix Endpoint detection and response (EDR), la prevención de fuga de datos (CDA/DLP), el monitoreo gestionado de eventos (MDR) y la detonación aislada de código malicioso en la nube (IVX).
4. Cumplimiento normativo y contable: La actualización de las suscripciones permite mantener vigentes los activos intangibles de la Entidad en cumplimiento de las normas contables, de inventarios, la normatividad sobre derechos de autor, así como los lineamientos del Modelo Integrado de Planeación y Gestión (MIPG) y la Política de Gobierno Digital del Estado Colombiano, los cuales conciben la seguridad de la información como un propósito habilitador fundamental para la función pública.

Por lo expuesto la Unidad ha determinado las cantidades de licenciamiento, suscripciones de soporte de hardware y servicios requeridos para la continuidad de la plataforma de ciberseguridad Trellix, fundamentadas en el parque informático activo, la infraestructura de red perimetral y los centros de datos institucionales.

El parque informático activo se compone de los siguientes equipos y servidores así:

Vigencia de Compra	Descripción del Equipo	Fabricante	Tipo	Cantidad	Condición Operativa
GRUPO 1 – EN USO ACTIVO					
2019	All in one pro One 600-400	HP	Escritorio	127	Activo
2019	All in one M800 -72	Lenovo	Escritorio	35	Activo
2019	All in One Compumax One Saturno	Compumax	Escritorio	42	Activo
2020	All in One HP ProOne 600 G6	HP	Escritorio	221	Activo
2020	Portátil HP ProBook	HP	Portátil	30	Activo
2020	Portátil HP 4420S	HP	Portátil	11	Activo
2021	Lenovo Desktop TC M75S-Gen2 Durham AMD	Lenovo	Escritorio	378	Activo
2021	Lenovo ThinkPad E14 Gen 3	Lenovo	Portátil	14	Activo
Subtotal Grupo 1 – EOL activos				858	
GRUPO 2 – CON SOPORTE ACTIVO DEL FABRICANTE					
2022	All in One HP ProOne 600 G7	HP	Escritorio	163	Activo
2023	HP EliteBook 645 14" G10 / HP Z Book Fury 16 G9	HP	Portátil	124	Activo
2023	PC Corporativo Todo en Uno Lenovo	Lenovo	Escritorio	25	Activo
2024	HP ProOne 440 G9 24 AIO + Diadema	HP	Escritorio	93	Activo
Subtotal Grupo 2 – Con soporte				405	
GRUPO 3 – SERVIDORES					
2025	Servidores Windows Server	HP	Servidor	37	Activo
Subtotal Grupo 3				37	

Por lo anterior, la necesidad del licenciamiento para la protección de puntos finales y prevención de fuga de datos se establece de la siguiente manera:

1. Protección de Puntos Finales (Endpoints) y Prevención de Fuga de Datos:

- Endpoint Enterprise Cloud + Managed Detection and Response (MDR) (1.300 Licencias- Déficit: 0): La Entidad requiere proteger la totalidad de su parque informático, compuesto por 1.300 dispositivos (computadores de escritorio, portátiles y servidores distribuidos en la sede principal y en los despachos a nivel nacional).
- Data Security Endpoint Protection Suite - Subscription (Renovación de 170 Licencias - Déficit 0): Se identificó una necesidad institucional de 170 licencias de protección contra la fuga de información (DLP/Data Security) para los equipos de cómputo que gestionan datos sensibles y críticos de la Entidad, como lo son los Juzgados y Fiscalías que se encuentran ubicados en el segundo y tercer piso del Palacio de la Justicia Penal Militar y Policial en Bogotá.

2. Infraestructura de Prevención de Intrusiones de Red (IPS NS3600)

- Network Security Manager Software Subscription Starter Edition (2 Suscripciones - Déficit: 0): Se requiere la renovación de 2 suscripciones para asegurar la gestión centralizada y la administración de políticas de seguridad de los appliances de IPS ubicados en los dos centros de datos de la Entidad (Palacio de la Justicia Penal Militar y Policial y Fortaleza sede CAN)
- Advanced RMA Hardware Support IPS NS3600 (2 Unidades- Déficit: 0): Cobertura de soporte y reemplazo avanzado de hardware para los 2 appliances físicos de IPS NS3600 instalados en el centro de datos principal y alterno.
- IPS NS3600 - 5Gbps Software License (2 Licencias - Déficit: 0): Habilitación del licenciamiento de rendimiento (*throughput*) de 5 Gbps por cada uno de los 2 dispositivos IPS, garantizando el ancho de banda suficiente para la inspección y filtrado de tráfico en ambos centros de cómputo.
- Advanced RMA Hardware Support Network Security 4-Port 10/1 (2 Unidades - Déficit: 0): Cobertura de soporte y garantía con reemplazo al día hábil siguiente para los 2 módulos de expansión de red con Fail-Open integrados en los appliances IPS.

3. Integración, seguridad de red y análisis dinámico en la nube:

- API de Integración del Fabricante (1 Licencia- Déficit: 0): Permite la interconexión e interoperabilidad de la plataforma de ciberseguridad Trellix con los sistemas institucionales de monitoreo e información de la UNIDAD.
- Network Security NX Edition Enterprise (1.500 Licencias/Sensores - Déficit: 0): Cobertura de licenciamiento de sensores virtuales para el análisis de tráfico de red y detección de vectores de ataque avanzados directa a la infraestructura corporativa de la Entidad.
- IVX Enterprise Cloud - Banded Submission Pack (10.000 Entregas/Submisiones- Déficit: 0): Paquete de 10.000 ejecuciones anuales para el análisis detonativo de archivos sospechosos y código

	malicioso en el entorno seguro e aislado en la nube (<i>sandboxing</i> IVX Cloud). 5. Soporte Técnico: Es relevante que la entidad no solo renueve los servicios de seguridad, sino que también asegure un soporte técnico experto y una transferencia de conocimiento efectiva para la actualizar, configurar, administrar, afinar y optimizar el rendimiento de la solución de licencias de endpoint existentes, la integración de los componentes (EDR/MDR, IPS, NX), y el acceso a inteligencia de amenazas y a soporte de fábrica, que permitan la continuidad operativa de los servicios de TIC. Finalmente, se precisa que el presente proceso contractual se encuentra contemplado en el Plan Anual de Adquisiciones de la vigencia 2026.
--	---

1.2 ANTECEDENTES CONTRACTUALES	A continuación, se relaciona los diferentes contratos que se han suscrito por parte de la Unidad en vigencias anteriores.				
	CONTRATISTA	No. DE CONTRATO	FECHA DE INICIO	FECHA FINAL	VALOR DEL CONTRATO
	SOFTSECURITY S.A.S.	038-2010	22/12/2010	29/12/2010	\$ 45.936.000,00
	SOFTSECURITY S.A.S.	035-2012	11/12/2012	31/12/2012	\$ 54.520.000,00
	SOFTSECURITY S.A.S.	Aceptación de Oferta 000411	27/07/2015	31/12/2015	\$130.170.000,00
	SOFTSECURITY S.A.S.	018 de 2017 DEJPM-MDN	21/11/2017	31/12/2017	\$125.220.249,00
	SOFTSECURITY S.A.S.	Aceptación de Oferta 000719	09/12/2019	31/12/2019	\$73.503.325,00
	SOFTSECURITY S.A.S.	049 de 2020 DEJPM-MDN	29/12/2020	31/12/2020	\$66.083.987,80
	SOFTSECURITY S.A.S.	045 de 2021 UAEJPMP	7/12/2021	31/12/2021	\$103.234.730,00
	SOFTSECURITY S.A.S.	035 de 2022 UAEJPMP	09/12/2022	20/12/2022	\$158.358.200,00
	SOFTSECURITY S.A.S.	046 de 2023 UAEJPMP	19/10/2023	3/12/2023	\$178.111.100,00
	SOFTSECURITY S.A.S.	064-2024 UAEJPMP	19/12/2024	31/12/2024	\$225.706.700,00
	SOFTSECURITY S.A.S.	057-2025 UAEJPMP	29/10/2025	31/12/2025	\$1.625.566.740,00

1.3. CANTIDADES QUE REQUIERE LA ENTIDAD PARA SATISFACER LA NECESIDAD FRENTE A LO QUE SE PUEDE ADQUIRIR DE ACUERDO CON EL ESTUDIO DE MERCADO					
Tabla 1. Cantidades					
Ítem	Descripción del bien o servicio	Unidad de Medida	Necesidad Real	Cantidad a adquirir según estudio de mercado	Cantidad pendiente por adquirir
	Tipo de Licencia Trellix				
1	Endpoint Enterprise Cloud +managed detection y response	UND	1300	1300	0
2	Renovación Solución Data Security Endpoint Protection Suite - Subscription	UND	170	170	0
3	Network Security Manager Software Subscription Starter Edition	UND	2	2	0

4	Advanced RMA (next business day ship) Hardware Support IPS NS3600	UND	2	2	0
5	IPS NS3600 - 5Gbps Software license (Throughput based entitlement)	UND	2	2	0
6	Advanced RMA (next business day ship) Hardware Support Network Security 4-Port 10/1	UND	2	2	0
7	API de integración del fabricante	UND	1	1	0
8	Network Security NX Edition (Enterprise)	UND	1500	1500	0
9	IVX Enterprise Cloud -Banded Submission Pack	UND	10000	10000	0
10	Servicio de soporte técnico	UND	1	1	0

Nota: Las cantidades relacionadas en la Tabla 1 corresponden a la necesidad real y cantidad a adquirir por cada período anual de licenciamiento y servicio. Teniendo en cuenta que el proceso contempla una cobertura de cuatro (4) períodos anuales, las mismas cantidades serán objeto de renovación en cada período de licenciamiento durante la ejecución contractual, de conformidad con las condiciones establecidas en el estudio de mercado.

1.4. EXPLICACIÓN DEL ESCENARIO QUE SE PRESENTARÍA SI “NO” SE REALIZA LA RENOVACIÓN DEL BIEN O SERVICIO SOLICITADO:

En el evento en que LA UNIDAD no lleve a cabo la renovación e implementación del licenciamiento, hardware y soporte especializado de la solución de ciberseguridad Trellix, se deshabilitarían los mecanismos de prevención, detección y mitigación de amenazas informáticas. Esto generaría una exposición crítica de la infraestructura tecnológica institucional ante los siguientes escenarios de riesgo:

- Pérdida de protección y actualización en tiempo real: Se suspendería la descarga automática de firmas de virus, motores heurísticos y el intercambio de inteligencia global de amenazas (DTI/TIE), dejando desactualizada la base de conocimientos necesaria para mitigar ataques emergentes.
- Exposición severa ante malware avanzado y Ransomware: La infraestructura quedaría vulnerable frente a vectores de ataque sin firma (Zero-Day) y amenazas avanzadas, al quedar inoperativas las capacidades de detonación y análisis dinámico en entorno aislado (sandboxing IVX), así como el monitoreo proactivo gestionado (MDR/EDR).
- Pérdida de Soporte Técnico y Garantía de Hardware Perimetral: Los componentes de red (como el sistema de prevención de intrusiones IPS NS3600) perderían la cobertura de soporte técnico directo del fabricante, actualizaciones de firmware y el servicio de reemplazo avanzado de hardware (RMA) ante fallas físicas.
- Incumplimiento Normativo y Riesgo Legal: Mantener en operación licencias vencidas contraviene las normas vigentes en materia de derechos de autor, la regulación contable de inventarios para activos intangibles, así como los lineamientos del Modelo Integrado de Planeación y Gestión (MIPG) y la Política de Gobierno Digital del Estado Colombiano.
- Impacto Operacional y Misional: Como consecuencia de las vulnerabilidades descritas, los servidores, estaciones de trabajo y servicios on-premise de la Entidad quedarían expuestos a intrusiones no autorizadas, infecciones por malware o ataques de cifrado de datos mediante *ransomware*. Esto podría ocasionar la pérdida parcial o total de la información institucional almacenada y la interrupción prolongada de servicios cibernéticos críticos, tales como el sistema misional de la Justicia Penal Militar y Policial, el correo electrónico corporativo, los repositorios de archivos, el acceso a internet y los servicios de impresión.

Dicha situación provocaría la parálisis de la operación diaria de los servidores y de los funcionarios a nivel nacional, afectando de manera directa la continuidad de la función pública encomendada a LA UNIDAD.

1.5 DEFINICIÓN DE DÓNDE SE VAN A DISTRIBUIR LOS BIENES O SERVICIOS A ADQUIRIR

Infraestructura de Hardware (Appliances IPS NS3600): La renovación de garantías, soporte técnico y licenciamiento de throughput aplicará para los equipos físicos instalados en los Centros de datos de la UNIDAD (Sede Palacio de Justicia Penal Militar y Policial y Sede Fortaleza), ubicados en la ciudad de Bogotá D.C.

Licenciamiento de Punto Final (Endpoints MDR/DLP) y Red (NX / IVX Cloud): Las suscripciones de software se desplegarán de manera centralizada e interactuarán con las estaciones de trabajo, servidores e instancias en la nube (AWS) ubicados en la sede principal (Bogotá D.C.) y en los diferentes despachos de la Justicia Penal Militar y Policial a nivel nacional. (ver directorio de despachos de la página web de la UNIDAD enlace <https://www.justiciamilitar.gov.co/directorio-institucional>).

2. DESCRIPCIÓN DEL OBJETO A CONTRATAR, ESPECIFICACIONES TÉCNICAS E IDENTIFICACIÓN DEL CONTRATO A CELEBRAR

2.1. OBJETO

DEFINICIÓN DEL OBJETO DEL PRESENTE PROCESO DE CONTRATACIÓN

Renovación y actualización del licenciamiento EDR/MDR, NX, IPS e IVX, así como la ampliación de las garantías y el servicio de soporte técnico especializado para los Sistemas de Prevención de Intrusos (IPS) y módulos de red, que conforman la solución integral de ciberseguridad y protección perimetral de Trellix para la Unidad Administrativa Especial de la Justicia Penal Militar y Policial.

2.2. TIPO DE CONTRATO A CELEBRAR

De acuerdo con la naturaleza del objeto, las especificaciones técnicas y las obligaciones contractuales, el tipo de contrato que se celebrará es el siguiente (marcar con una X) el tipo que corresponda:

Prestación de servicios

Compraventa X

Suministro

Otro. ¿Cuál? _____

2.3. ESPECIFICACIONES TÉCNICAS:

Las especificaciones técnicas se encuentran detalladas en el archivo Anexo Técnico No. 1 "ESPECIFICACIONES TÉCNICAS MÍNIMAS EXIGIDAS", el cual hace parte integral del presente documento.

El proponente deberá cumplir con las especificaciones técnicas mínimas, de conformidad con la ficha técnica publicada en el SECOP II.

2.4. OBLIGACIONES ESPECÍFICAS DEL CONTRATISTA

- 1.** Cumplir con el objeto del contrato en los términos establecidos en los estudios y documentos previos, en el pliego de condiciones, especificaciones técnicas y sus adendas si fueran expedidas.
- 2.** EL CONTRATISTA deberá realizar las gestiones necesarias para la consulta de la respectiva renovación del licenciamiento de solución integral de ciberseguridad y protección perimetral Trellix, adquirida por la Entidad a través del portal web del fabricante, con el usuario de LA UNIDAD.
- 3.** Durante el plazo de ejecución del contrato, EL CONTRATISTA entregará la certificación donde conste la vigencia del licenciamiento renovado y adquirido, incluida la garantía y soporte suscrita por el representante legal y el registro a través del portal web del fabricante, con el usuario de LA UNIDAD, indicando los códigos NAI de ésta.
- 4.** EL CONTRATISTA deberá realizar las gestiones necesarias para la visualización de la respectiva renovación del licenciamiento con el que cuenta LA UNIDAD a través del portal web del fabricante con el usuario de Justicia Penal Militar y Policial.
- 5.** EL CONTRATISTA deberá tener una (1) reunión de seguimiento mensual durante la vigencia de la garantía y renovación del licenciamiento, en las instalaciones de LA UNIDAD con el supervisor del contrato, de esta reunión se levantará un acta que será suscrita por las partes.
- 6.** El Contratista deberá presentar a la supervisión del contrato, dentro de los primeros cinco (5) días hábiles de cada mes un informe de ejecución y los reportes técnicos detallados de las actividades, mantenimientos, afinamientos, atenciones de mesa de ayuda y procedimientos realizados en el periodo reportado, de conformidad con las especificaciones técnicas mínimas exigidas y los niveles de servicio (SLA) establecidos por la unidad.
- 7.** EL CONTRATISTA garantizará que las actividades desarrolladas durante la ejecución del contrato no interfieran en la continuidad, disponibilidad, integridad e interoperabilidad de los servicios informáticos de LA UNIDAD.
- 8.** Responder sin perjuicio de la respectiva garantía, por la calidad del servicio prestado.
- 9.** EL CONTRATISTA deberá realizar las gestiones necesarias para garantizar el óptimo y correcto funcionamiento de la solución del fabricante y mantener actualizados cada uno de los componentes de esta. Para esto, deberá implementar durante la renovación del licenciamiento, las actualizaciones liberadas por el fabricante y prestar soporte de fábrica.
- 10.** EL CONTRATISTA deberá garantizar la gestión, escalamiento y participación activa de su personal técnico experto en el evento en que se requiera la intervención directa del fabricante para la atención o solución de cualquier tipo de novedad, incidente o falla técnica presentada en las soluciones objeto del contrato.
- 11.** EL CONTRATISTA asumirá la responsabilidad directa por la resolución definitiva de la novedad y mantendrá debidamente informado y actualizado a la supervisión del contrato designado por LA UNIDAD sobre los avances y la solución implementada.
- 12.** EL CONTRATISTA deberá cumplir con las políticas de seguridad y privacidad de la información y con el Sistema de Seguridad y Privacidad de la información de LA UNIDAD.
- 13.** EL CONTRATISTA y el personal que presta los servicios de seguridad, deben firmar el acuerdo de confidencialidad en la semana siguiente a la firma del acta de inicio del Contrato.
- 14.** Obrar con lealtad y buena fe en las distintas etapas contractuales, evitando dilaciones que puedan presentarse y en general se obliga a cumplir con lo establecido en las Leyes 80 de 1993, 1150 de 2007, 1474 de 2011 y sus decretos reglamentarios.
- 15.** Mantener la debida reserva frente a los temas y asuntos tratados y conocidos dentro del desarrollo y ejecución del contrato, de conformidad con el compromiso de confidencialidad que se suscribe con el contrato por parte del representante legal y/o apoderado, el cual hace parte integral del mismo, así como por todos aquellos que intervengan en la ejecución del proyecto.
- 16.** Cumplir cabalmente con sus obligaciones frente al Sistema de Seguridad Social Integral (Salud, Pensión y Riesgos Laborales) y Aportes Parafiscales (Cajas de Compensación

Familiar, SENA e ICBF). Para la realización de los pagos derivados del contrato. EL CONTRATISTA, deberá entregar a la supervisión certificación expedida por el revisor fiscal en la que acredite que se encuentra al día en el pago de las citadas obligaciones, exonerándose del mismo para aquellos casos que se encuentran contemplados en la ley.

17. Dar buen uso y custodia de los bienes y elementos que LA UNIDAD le entregue o permita su acceso para el desarrollo del objeto contractual.
18. Proveer todos los bienes y servicios necesarios para el cumplimiento de los objetivos y funcionalidades requeridas en el presente contrato.
19. Constituir en debida forma y aportar a LA UNIDAD, las garantías dentro del término señalado para el efecto en el cronograma del proceso.
20. EL CONTRATISTA deberá cumplir con la normatividad vigente en pro de la seguridad y salud de sus trabajadores, de conformidad con lo exigido en el Decreto Único Reglamentario 1072 de 2015, libro 2, título 4, capítulo 6, Sistema de Gestión de la Seguridad y Salud en el Trabajo, que le permitan a EL CONTRATISTA anticipar, reconocer, evaluar y controlar los riesgos que puedan afectar la seguridad y salud en el trabajo.
21. Asistir a las reuniones que se programen en el desarrollo del contrato.
22. Allegar en los dos (2) días hábiles siguientes al perfeccionamiento del contrato el certificado de curso virtual de cincuenta (50) horas sobre Seguridad y Salud en el Trabajo (Artículo 2.2.4.6.35 del Decreto Único Reglamentario 1072 de 2015) y mantenerlo vigente.
23. En general, la obligación de cumplir cabalmente con las condiciones y modalidades previstas contractualmente para la ejecución y desarrollo del contrato, para lo cual EL CONTRATISTA deberá actuar razonablemente en el marco de sus obligaciones contractuales.
24. Las demás obligaciones que se deriven de la naturaleza del objeto contractual.

2.5. PLAZO Y LUGAR DE EJECUCIÓN DEL CONTRATO

Requiere Acta de Inicio: X

No Requiere Acta de Inicio:

El plazo de ejecución del contrato será hasta el 31 de julio de 2030, contado a partir de la suscripción del acta de inicio, previo cumplimiento de los requisitos de ejecución, esto es, la expedición del registro presupuestal y la aprobación de las garantías.

Vigencia del licenciamiento: La renovación del licenciamiento tendrá una vigencia del 30 de diciembre de 2026 al 29 de diciembre de 2030, debidamente registrado en el portal web de Trellix.

El contrato se ejecutará en instalaciones de la UNIDAD ubicada en la Carrera 46 No. 20 C - 01 (Puente Aranda) Cantón Militar Occidental "Coronel Francisco José de Caldas" Bogotá D.C, Colombia.

Nota. Tener en cuenta las reglas para los plazos establecidas en el Artículo 829 del Código de Comercio.

2.6. FORMA DE PAGO

LA UNIDAD pagará el valor del contrato al **CONTRATISTA** mediante cinco (5) pagos, con un porcentaje fijo sobre el valor total del mismo, distribuidos según el periodo de licenciamiento cubierto y previa radicación de la factura y soportes por parte del **CONTRATISTA**, como se establece en la siguiente tabla:

Periodo de Licenciamiento	Rango de fechas del periodo	Fecha de Radicación Factura	% del pago con respecto al valor del contrato
Primer Periodo	30 de diciembre de 2026 – 29 de diciembre de 2027	Diciembre de 2026	2,50%
		Enero de 2027	22,90%
Segundo Periodo	30 de diciembre de 2027 – 29 de diciembre de 2028	Enero de 2028	25,50%
Tercer Periodo	30 de diciembre de 2028 – 29 de diciembre de 2029	Enero de 2029	25,50%
Cuarto Periodo	30 de diciembre de 2029 – 29 de diciembre de 2030	Enero de 2030	23,60%
TOTAL			100,00%

Los pagos se realizarán en moneda legal colombiana a través de la Tesorería de **LA UNIDAD**, una vez se encuentre aprobado el P.A.C. (Programa Anual Mensualizado de Caja) por parte del Ministerio de Hacienda y Crédito Público, dentro de los cuarenta y cinco (45) días calendario siguientes a la radicación de los documentos requeridos para pago, así: 1) Informe de supervisión y acta de recibo a satisfacción suscritos por el supervisor. 2) Presentación de la factura de venta a través de la plataforma electrónica de contratación pública SECOP II y el cumplimiento del “Modelo de Recepción de Facturas de Venta, Notas Débito y/o Notas Crédito” a través del buzón dispuesto para el efecto por el Ministerio de Hacienda y Crédito Público (siifnacion.facturaelectronica@minhacienda.gov.co). 3) Constancia del pago de aportes al sistema de seguridad social integral y aportes parafiscales, de sus trabajadores y de sus contratistas, mediante certificación expedida por el representante legal y/o revisor fiscal según sea en caso, exonerándose del mismo para aquellos casos que se encuentran contemplados en la ley, certificación emitida por parte del revisor fiscal deberá acompañarse de la copia de la tarjeta profesional, la cédula de ciudadanía y el certificado de la Junta Central de Contadores con una fecha de emisión no mayor a noventa (90) días calendario. **PARÁGRAFO PRIMERO-CUENTA PARA PAGOS:** Los pagos previstos en esta cláusula se realizará en la cuenta bancaria que **EL CONTRATISTA** acredite como propia o en otra cuenta bancaria de la que sea titular **EL CONTRATISTA** y lo informe por escrito a **LA UNIDAD** con no menos de treinta (30) días de anticipación a la presentación de la factura enviando la respectiva certificación bancaria en donde se acredite su apertura y titularidad. **PARÁGRAFO SEGUNDO:** Si la factura no ha sido correctamente elaborada o no se acompaña de los documentos requeridos para el pago y/o se presentan de manera incorrecta, el término para éste sólo empezará a contarse desde la fecha en que se aporte en debida forma o se allegue el último de los documentos y aplicará la misma regla para todos los pagos que se deriven del contrato si la corrección no se hace dentro de los primeros cinco (5) días hábiles siguientes. Las demoras que se presenten por estos conceptos serán responsabilidad de **EL CONTRATISTA** y no tendrán por ello derecho al pago de intereses o compensación de ninguna naturaleza. **PARÁGRAFO TERCERO – REAJUSTE AL PESO: EL CONTRATISTA** con la aprobación del contrato en el SECOP II, acepta que en el evento que el valor total a pagar tenga centavos, estos se ajusten o aproximen al peso, ya sea por exceso o por defecto, si la suma es mayor o menor a 50 centavos. Lo anterior, sin que sobrepase el valor total establecido en el contrato.

2.7. SUPERVISIÓN

Con el fin de proteger la moralidad administrativa, de prevenir la ocurrencia de actos de corrupción y de tutelar la transparencia de la actividad contractual, LA UNIDAD designará como supervisor al Jefe de la Oficina de Tecnologías de la Información y las Comunicaciones y al Coordinador del Grupo de Plataforma Tecnológica o al funcionario que se designe de la Unidad

Administrativa Especial de la Justicia Penal Militar y Policial quienes cumplirán con lo consagrado en el Estatuto General de Contratación Pública y en las demás normas vigentes dispuestas para ello.

3. FUNDAMENTOS JURÍDICOS QUE SOPORTAN LA MODALIDAD DE SELECCIÓN

Teniendo en cuenta que se trata de bienes y servicios de características técnicas uniformes, con independencia de su diseño o de sus características descriptivas, y de común utilización por parte de las entidades, atendiendo que comparten patrones de desempeño y calidad objetivamente definidos, la modalidad de selección será la de Selección Abreviada por Subasta Inversa Electrónica a través de la plataforma del SECOP II, de acuerdo con lo consagrado por la Ley 80 de 1993, el literal a, numeral 2, del artículo 2 de la Ley 1150 de 2007, y los artículos 2.2.1.2.1.2.1., 2.2.1.2.1.2.2 y siguientes del Decreto Único Reglamentario 1082 de 2015 y lo modificado y adicionado por el Decreto 1860 de 2021.

Para la selección del contratista la Entidad aplicará los principios de economía, transparencia y responsabilidad definidos en la Ley 80 de 1993 y los postulados que rigen la función administrativa.

Se deja constancia de que se efectuó la consulta correspondiente en la Tienda Virtual del Estado Colombiano, verificándose que actualmente no existe un Acuerdo Marco de Precios (AMP) para renovación y actualización del licenciamiento para la solución de seguridad con la que cuenta la Entidad.

4. ANÁLISIS QUE SOPORTA EL VALOR ESTIMADO DEL CONTRATO

4.1. ESTUDIO DEL SECTOR Y DE COSTOS:

El presente estudio de consulta de precios techo de mercado se adelantó siguiendo la metodología establecida en el numeral 4º del artículo 2.2.1.1.2.1.1 del Decreto Único Reglamentario No 1082 de 2015, modificado parcialmente por el Decreto 399 de 2021, con el objeto de conocer el comportamiento del mercado, por lo cual se consultó el mercado con el fin de decidir las diferentes variables a determinar en los estudios y documentos previos.

Para el desarrollo de la consulta del comportamiento de los precios de mercado, se lanzó a través de la plataforma de SECOP II el evento de cotización No. CO1.BDOS.10414112 el 03 de julio de 2026, el cual cerró el 14 de julio de la presente vigencia, presentándose tres (3) cotizaciones. De igual forma, a través de correo electrónico se solicitaron cotizaciones a diferentes empresas recibándose una como a continuación se describe:

Item	Descripción	Cantidad	ITSC SAS	Multisoft	PCM	SOFTSECURITY	Promedio Unitario	Valor Total Periodo
1	Endpoint Enterprise Cloud +managed detection y response	1300	\$654.397,00	\$616.500,00	\$615.307,00	\$559.370,00	\$611.393,50	\$794.811.550,00
2	Solución Data Security Endpoint Protection Suite - Subscription	170	\$241.202,00	\$229.000,00	\$227.579,00	\$206.890,00	\$226.167,75	\$38.448.517,50
3	Network Security Manager Software Subscription Starter Edition	2	\$12.461.834,70	\$11.672.115,00	\$11.670.925,00	\$10.806.390,00	\$11.652.816,18	\$23.305.632,35
4	Advanced RMA (next business day ship) Hardware Support IPS NS3600	2	\$22.033.453,33	\$20.872.243,00	\$20.872.233,48	\$19.148.837,40	\$20.731.691,80	\$41.463.383,61
5	IPS NS3600 - 5Gbps Software license (Throughput based entitlement)	2	\$99.126.756,05	\$93.498.300,00	\$93.486.400,00	\$86.570.981,56	\$93.170.609,40	\$186.341.218,81
6	Advanced RMA (next business day ship) Hardware Support Network Security 4-Port 10/1	2	\$49.375.070,64	\$46.462.833,62	\$46.462.738,42	\$43.021.054,93	\$46.330.424,40	\$92.660.848,81
7	API	1	\$73.617.755,00	\$67.990.000,00	\$67.900.000,00	\$62.864.971,00	\$68.093.181,50	\$68.093.181,50
8	Network Security NX Edition (Enterprise)	1500	\$310.735,18	\$292.718,58	\$292.706,68	\$273.557,20	\$292.429,41	\$438.644.115,00
9	IVX Enterprise Cloud	10000	\$7.555,00	\$7.000,00	\$7.000,00	\$6.365,00	\$6.980,00	\$69.800.000,00
10	Servicio de soporte técnico	1	\$220.399.506,11	\$204.680.000,00	\$202.300.000,00	\$196.350.000,00	\$205.932.376,53	\$205.932.376,53
TOTAL								\$1.959.500.824,09

Segundo periodo de licenciamiento del 30 de diciembre de 2027 al 29 diciembre de 2028.

Item	Descripción	Cantidad	ITSC SAS	Multisoft	PCM	SOFTSECURITY	Promedio Unitario	Valor Total Periodo
1	Endpoint Enterprise Cloud +managed detection y response	1300	\$591.850,00	\$551.524,00	\$551.324,00	\$501.204,00	\$548.975,50	\$713.668.150,00
2	Solución Data Security Endpoint Protection Suite - Subscription	170	\$235.602,00	\$221.990,00	\$221.790,00	\$201.628,00	\$220.252,50	\$37.442.925,00
3	Network Security Manager Software Subscription Starter Edition	2	\$11.479.476,61	\$10.774.188,60	\$10.773.950,60	\$9.975.902,09	\$10.750.879,48	\$21.501.758,95
4	Advanced RMA (next business day ship) Hardware Support IPS NS3600	2	\$19.415.986,45	\$18.470.130,42	\$18.232.130,42	\$17.058.907,04	\$18.294.288,58	\$36.588.577,17
5	IPS NS3600 - 5Gbps Software license (Throughput based entitlement)	2	\$91.161.363,72	\$84.963.541,46	\$84.892.141,46	\$77.079.056,04	\$84.524.025,67	\$169.048.051,34
6	Advanced RMA (next business day ship) Hardware Support Network Security 4-Port 10/1	2	\$43.179.636,71	\$40.544.852,95	\$40.544.852,95	\$38.294.451,09	\$40.640.948,43	\$81.281.896,85
7	API	1	\$45.570.252,00	\$42.789.028,00	\$42.739.028,00	\$39.578.573,00	\$42.669.220,25	\$42.669.220,25
8	Network Security NX Edition (Enterprise)	1500	\$303.489,27	\$337.993,32	\$278.493,32	\$240.625,14	\$290.150,26	\$435.225.393,75
9	IVX Enterprise Cloud	10000	\$6.728,00	\$6.800,00	\$6.400,00	\$5.812,00	\$6.435,00	\$64.350.000,00
10	Servicio de soporte técnico	1	\$235.693.607,45	\$223.244.000,00	\$220.864.000,00	\$214.200.000,00	\$223.170.401,86	\$223.170.401,86
TOTAL								\$1.825.276.375,17

Tercer periodo de licenciamiento del 30 diciembre de 2028 al 29 de diciembre de 2029.

Item	Descripción	Cantidad	ITSC SAS	Multisoft	PCM	SOFTSECURITY	Promedio Unitario	Valor Periodo	Total
1	Endpoint Enterprise Cloud +managed detection y response	1300	\$166.212,00	\$157.975,00	\$156.975,00	\$149.525,00	\$157.671,75	\$204.973.275,00	
2	Solución Data Security Endpoint Protection Suite - Subscription	170	\$272.534,00	\$257.424,00	\$253.424,00	\$229.313,00	\$253.173,75	\$43.039.537,50	
3	Network Security Manager Software Subscription Starter Edition	2	\$12.129.886,58	\$11.519.452,28	\$11.459.952,28	\$10.832.065,44	\$11.485.339,15	\$22.970.678,29	
4	Advanced RMA (next business day ship) Hardware Support IPS NS 3600	2	\$20.498.917,39	\$19.968.940,18	\$19.611.940,18	\$18.530.866,83	\$19.652.666,15	\$39.305.332,29	
5	IPS NS3600 - 5Gbps Software license (Throughput based entitlement)	2	\$90.766.179,00	\$84.594.501,04	\$84.582.601,04	\$83.782.759,20	\$85.931.510,07	\$171.863.020,14	
6	Advanced RMA (next business day ship) Hardware Support Network Security 4-Port 10/1	2	\$49.198.423,47	\$47.301.537,29	\$46.111.537,29	\$41.623.066,73	\$46.058.641,20	\$92.117.282,39	
7	API	1	\$74.656.007,00	\$71.992.669,00	\$71.892.669,00	\$69.732.478,00	\$72.068.455,75	\$72.068.455,75	
8	Network Security NX Edition (Enterprise)	1500	\$290.174,36	\$285.241,81	\$273.341,81	\$265.888,84	\$278.661,71	\$417.992.557,50	
9	IVX Enterprise Cloud	10000	\$14.398,00	\$13.959,00	\$13.459,00	\$12.567,00	\$13.595,75	\$135.957.500,00	
10	Servicio se soporte técnico	1	\$250.760.286,70	\$248.430.708,19	\$240.100.708,19	\$271.201.000,00	\$252.623.175,77	\$252.623.175,77	
TOTAL								\$1.452.910.814,63	

Cuarto periodo de licenciamiento del 30 diciembre de 2029 al 29 de diciembre de 2030.

Item	Descripción	Cantidad	ITSCSAS	Multisoft	PCM	SOFTSECURITY	Promedio Unitario	Valor Total Periodo
1	Endpoint Enterprise Cloud +managed detection y response	1300	\$314.472,00	\$304.358,00	\$303.358,00	\$293.177,00	\$303.841,25	\$394.993.625,00
2	Solución Data Security Endpoint Protection Suite - Subscription	170	\$165.215,00	\$157.928,00	\$157.328,00	\$149.733,00	\$157.551,00	\$26.783.670,00
3	Network Security Manager Software Subscription Starter Edition	2	\$9.174.230,03	\$8.804.141,22	\$8.798.191,22	\$7.823.159,96	\$8.649.930,61	\$17.299.861,22
4	Advanced RMA (next business day ship) Hardware Support IPS NS3600	2	\$14.413.565,60	\$13.912.042,48	\$13.888.242,48	\$13.541.837,05	\$13.938.921,90	\$27.877.843,81

5	IPS NS3600 - 5Gbps Software license (Throughput based entitlement)	2	\$68.499.682,02	\$66.266.630,36	\$65.076.630,36	\$61.172.944,84	\$65.253.971,90	\$130.507.943,79
6	Advanced RMA (next business day ship) Hardware Support Network Security 4-Port 10/1	2	\$33.747.378,98	\$32.075.813,35	\$31.837.813,35	\$30.832.921,42	\$32.123.481,78	\$64.246.963,55
7	API	1	\$63.258.297,00	\$59.999.932,00	\$59.932.932,00	\$60.834.078,00	\$61.006.309,75	\$61.006.309,75
8	Network Security NX Edition (Enterprise)	1500	\$245.579,11	\$232.821,12	\$231.631,12	\$195.422,99	\$226.363,59	\$339.545.377,50
9	IVX Enterprise Cloud	10000	\$14.983,00	\$14.755,00	\$14.455,00	\$12.749,00	\$14.235,50	\$142.355.000,00
10	Servicio de soporte técnico	1	\$179.974.301,71	\$177.479.046,64	\$171.529.046,64	\$192.780.000,00	\$180.440.598,75	\$180.440.598,75
TOTAL								\$1.385.057.193,36

Análisis estadístico de las ofertas

Validación de atipicidad sobre el valor total de la oferta: Antes de construir el precio de referencia por ítem, se validó si alguna de las cuatro ofertas económicas resultaba atípica (anormalmente baja o alta) en su valor total a 4 años. Esta validación se realizó sobre el valor global de cada propuesta y no sobre ítems individuales, en atención a que cada oferente estructura su propuesta como un paquete integral: puede fijar márgenes distintos entre ítems según su propio modelo de negocio, sin que ello implique una distorsión real en la competitividad de su oferta.

Oferente	Total 4 años (con IVA)	Desviación vs. media	Resultado
ITSC SAS	\$ 6.999.344.886	+5,69%	Dentro de rango
Multisoft S.A.S.	\$ 6.735.052.395	+1,70%	Dentro de rango
PCM	\$ 6.582.536.110	-0,61%	Dentro de rango
Softsecurity S.A.S.	\$ 6.174.047.438	-6,78%	Dentro de rango

El valor total de las cuatro ofertas presenta una media de \$6.622.745.207 y una desviación estándar de \$345.151.987. Al expresar esta desviación como proporción de la media se obtiene un coeficiente de variación de 5,21%, cifra que indica una dispersión baja entre las ofertas y, por tanto, un mercado homogéneo: las cuatro propuestas se mueven dentro de un rango relativamente estrecho alrededor del valor promedio. Esto se confirma al verificar los límites del Rango Intercuartílico (1,5 × RIC): límite inferior \$5.999.346.578 y límite superior \$7.282.192.882. Ninguna de las cuatro ofertas se ubica por fuera de estos límites, por lo que ninguna se considera atípica y las cuatro se incorporan en igualdad de condiciones al cálculo estadístico por ítem.

Metodología estadística aplicada

Para cada uno de los 10 ítems y las 4 vigencias se calcularon las siguientes medidas estadísticas:

- Media Aritmética: promedio simple de las ofertas.
- Media Geométrica: medida de tendencia central menos sensible a valores extremos que la media aritmética, sin necesidad de excluir datos.
- Desviación Estándar: dispersión de las ofertas respecto a su media, como indicador de heterogeneidad de precios en cada ítem.

Se adoptó la Media a la Baja como criterio para la construcción del presupuesto de referencia por ítem, al considerar que esta metodología permite establecer un valor de referencia sustentado en los precios efectivamente observados en el mercado y en el comportamiento conjunto de las ofertas recibidas, sin excluir información del análisis estadístico realizado. El detalle del cálculo, efectuado ítem por ítem y vigencia por vigencia, así como las fórmulas empleadas (PROMEDIO, MEDIA.GEOM, DESVEST y media condicional a la baja), se encuentra en el archivo "Análisis_Estadístico_Ofertas_Trellix.xlsx", hoja "Consolidado por Ítem", el cual se adjunta como soporte del presente documento.

La tabla presenta la consolidación de las cantidades requeridas por la Entidad para los cuatro (4) periodos de licenciamiento, así como el valor unitario de referencia obtenido mediante la metodología de Media a la Baja aplicada a cada ítem.

PRECIOS DE REFERENCIA

A continuación, se relaciona los valores promedios establecidos por ítem en el estudio de mercado que serán los precios máximos o techo estimados a cotizar por parte del (los) proponente(s) al momento de elaborar su propuesta económica a través del SECOP II, el cual será base para iniciar el evento de subasta con los oferentes habilitados.

NOTA: Para efectos de la estimación presupuestal, las cantidades correspondientes a cada periodo fueron acumuladas para determinar la cantidad total a contratar, y sobre esta se aplicó el respectivo valor unitario de referencia. Como resultado, se obtiene un presupuesto estimado, el cual corresponde a la sumatoria del valor total de cada uno de los diez (10) ítems del bien o servicio.

Ítem	Descripción del bien o servicio	Necesidad real y cantidad a adquirir según estudio de mercado				Total	Valor Unitario Media a la Baja	Valor Total
	Tipo de Licencia Trellix	Periodo 1- 2027	Periodo 2- 2028	Periodo 3- 2029	Periodo 4- 2030			
1	Endpoint Enterprise Cloud +managed detection y response	1300	1300	1300	1300	5200	\$ 378.023,00	\$ 1.965.719.600,00
2	Renovación Solución Data Security Endpoint Protection Suite - Subscription	170	170	170	170	680	\$ 197.840,50	\$ 134.531.540,00
3	Network Security Manager Software Subscription Starter Edition	2	2	2	2	8	\$ 9.937.865,25	\$ 79.502.922,00
4	Advanced RMA (next business day ship) Hardware Support IPS NS3600	2	2	2	2	8	\$ 17.411.616,75	\$ 139.292.934,00
5	IPS NS3600 - 5Gbps Software license (Throughput based entitlement)	2	2	2	2	8	\$ 77.773.695,00	\$ 622.189.560,00
6	Advanced RMA (next business day ship) Hardware Support Network Security 4-Port 10/1	2	2	2	2	8	\$ 39.005.256,00	\$ 312.042.048,00

7	API de integración del fabricante	1	1	1	1	4	\$ 59.322.954,00	\$ 237.291.816,00
8	Network Security NX Edition (Enterprise)	1500	1500	1500	1500	6000	\$ 249.538,50	\$ 1.497.231.000,00
9	IVX Enterprise Cloud -Banded Submission Pack	10000	10000	10000	10000	40000	\$ 9.558,25	\$ 382.330.000,00
10	Servicio de soporte técnico	1	1	1	1	4	\$ 210.826.008,25	\$ 843.304.033,00
	Total							\$ 6.213.435.453,00

Los proponentes no podrán superar, en ningún caso, los VALORES UNITARIOS MÁXIMOS TECHO, incluido IVA y demás impuestos, tasas, contribuciones, costos y erogaciones a que haya lugar, establecidos para cada ítem, so pena de que la oferta sea RECHAZADA ECONÓMICAMENTE.

Los valores unitarios máximos techo establecidos para cada ítem serán fijos e invariables durante toda la ejecución del contrato y, por tanto, no estarán sujetos a reajustes, actualizaciones, indexaciones ni incrementos durante los cuatro (4) periodos de licenciamiento y servicios previstos.

En consecuencia, los interesados deberán considerar en la estructuración de su oferta económica todos los costos directos e indirectos, así como las demás variables que puedan incidir en el precio durante el periodo de licenciamiento.

Así mismo, se precisa que la adjudicación del presente proceso de selección se realizará teniendo en cuenta los valores unitarios de los ítems, razón por la cual el proponente seleccionado luego del evento de subasta, si a ello hubiere lugar, deberá presentar su estructura de costos ajustada.

4.2 CONCLUSIONES ANÁLISIS DEL SECTOR

Los precios históricos corresponden a los procesos realizados por LA UNIDAD en vigencias anteriores de acuerdo con las necesidades de cada vigencia, las cuales han venido aumentando con la entrada de las fases i, ii iii y iv del SPOA que han demandado mayor licenciamiento para los despachos que se crearon por la Ley 1407 de 2010 y a la necesidad de ampliar la superficie de protección de la Unidad con el fin de controlar las nuevas capacidades de ataques presentes en el mercado.

Sin embargo, teniendo en cuenta los productos integrados en la solución de seguridad, dichos valores se tienen en cuenta la definición del presupuesto, por las escalas que se logran al integrar en una sola administración y solución los productos endpoint Enterprise con los productos adicionales de IPS, seguridad de Red NX e IVX.

Adicionalmente, el presente proceso se va a realizar por selección abreviada por subasta inversa, para lo cual se solicitaron cotizaciones a empresas distribuidoras de Trellix en Colombia, para ello se solicitó formalmente cotización soluciones de seguridad a través de la plataforma SECOP II y por correo, teniendo en cuenta las condiciones técnicas del proceso, con el fin conocer el comportamiento de los precios de mercado ajustados por análisis estadísticos y así mismo lograr la estimación del presupuesto oficial para el presente proceso de contratación.

4.3. PRESUPUESTO

De acuerdo con el valor obtenido en el análisis del sector realizado, se tiene como presupuesto oficial estimado para el presente proceso de selección será hasta la suma de **SEIS MIL**

DOSCIENTOS TRECE MILLONES CUATROCIENTOS TREINTA Y CINCO MIL CUATROCIENTOS CINCUENTA Y TRES PESOS M/CTE (\$6.213.435.453,00) incluido IVA y todos los costos directos e indirectos y los impuestos nacionales a que haya lugar.

La presente contratación será atendida con cargo al rubro de:

NOMBRE DEL RUBRO	RECURSO
A-02-02-02-008-003 SERVICIOS PROFESIONALES, CIENTÍFICOS Y TÉCNICOS (EXCEPTO LOS SERVICIOS DE INVESTIGACION, URBANISMO, JURÍDICOS Y DE CONTABILIDAD)	10

El cual afecta recursos de: **Funcionamiento X** Inversión

De acuerdo con lo señalado en el artículo 2o de la Ley 1150 de 2007, adicionado por el artículo 4 de la Ley 1882 de 2018, No es obligatorio contar con disponibilidad presupuestal para realizar la publicación del proyecto de Pliego de Condiciones.

5. CLASIFICACIÓN UNSPSC

Los bienes o servicios objeto del presente Proceso de Contratación está codificado en el Clasifica de Bienes y Servicios de Naciones Unidas (UNSPSC), como se indica en la Tabla <http://www.colombiacompra.gov.co/es/Clasificacion>.

Tabla 2 - Codificación del bien o servicio en el sistema UNSPSC

Clasificación UNSPSC	Descripción
43233200	Software de seguridad y protección
81111800	Servicio de sistemas y administración de componentes de sistemas
81112200	Mantenimiento y soporte de software

6. REQUISITOS HABILITANTES

6.1. REQUISITOS MÍNIMOS HABILITANTES

La verificación de los requisitos habilitantes se realizará individualmente por parte de los miembros que conformen el Comité Evaluador y se efectuará de la siguiente manera:

La Unidad debe verificar con el Registro Único de Proponentes el cumplimiento de los requisitos habilitantes. Esta verificación se hará de acuerdo con los artículos 2.2.1.1.1.5.2 y 2.2.1.1.1.5.3 del Decreto 1082 de 2015 y los lineamientos expedidos por Colombia Eficiente.

De conformidad con el numeral 6.1 del artículo 6 de la Ley 1150 de 2007, solo en aquellos casos en que por las características del objeto a contratar se requiera la verificación de requisitos del Proponente, adicionales a los contenidos en el RUP, la Entidad Estatal puede hacer tal verificación en forma directa.

6.1.1. CAPACIDAD JURÍDICA

En el presente Proceso de Contratación pueden participar personas naturales o jurídicas, nacionales o extranjeras; consorcios, uniones temporales o promesas de sociedad futura, cuyo objeto social esté relacionado con el objeto del contrato a celebrarse.

La duración de esta asociación debe ser, por lo menos, por la vigencia del Contrato y un año más.

La Unidad también revisará que los Proponentes no se encuentren en causales de inhabilidad, incompatibilidad o conflictos de interés para celebrar o ejecutar el contrato. Para ello, revisará el boletín de responsables fiscales, el certificado de antecedentes disciplinarios, el certificado de antecedentes judiciales y el RUP para verificar que no haya sanciones inscritas.

Las personas jurídicas extranjeras deben acreditar su existencia y representación legal con el documento idóneo expedido por la autoridad competente en el país de su domicilio no anterior a tres (3) meses desde la fecha de presentación de la oferta, en el cual conste su existencia, fecha de constitución, objeto, duración, nombre representante legal, o nombre de la persona que tenga la capacidad de comprometerla jurídicamente, y sus facultades, señalando expresamente que el representante no tiene limitaciones para contraer obligaciones en nombre de la misma, o aportando la autorización o documento correspondiente del órgano directo que lo faculta.

6.1.2. LEGALIZACIÓN DE DOCUMENTOS OTORGADOS EN EL EXTERIOR

Para que los documentos otorgados en el extranjero cuenten con eficacia probatoria en Colombia, deben ser aportados por el proponente de acuerdo con lo previsto en el artículo 251 del Código General del Proceso y el artículo 480 del Código de Comercio es decir debidamente apostillados o legalizados, concordante con la Sentencia de Unificación No. 25000232600019971393001 del 25 de septiembre de 2013 – consejero Ponente Mauricio Fajardo.

6.1.3. EXPERIENCIA

El proponente deberá acreditar experiencia en máximo tres (03) contratos ejecutados y/o certificaciones cuyo objeto sea renovación, actualización, suministro y/o adquisición de licencias Endpoint Enterprise y/o soluciones de Network Security IPS y/o servicio de monitoreo de red NX, dentro de los diez (10) años anteriores a la fecha del cierre de proceso de selección y donde la sumatoria (individual o conjunta) de los mismos sea igual o superior al cien por ciento (100%) del presupuesto oficial estimado. Dichos contratos estarán comprendidos en mínimo uno (01) de los siguientes códigos de clasificación UNSPSC relacionados en la Tabla No. 3.

Tabla 3 - Experiencia requerida

Código del Clasificador de Bienes y Servicios		Cuantía - SMMLV
43233200	Software de seguridad y protección	3.548,69
81111800	Servicio de sistemas y administración de componentes de sistemas	
81112200	Mantenimiento y soporte de software	

REQUISITO DIFERENCIAL PARA INCENTIVAR LOS EMPRENDIMIENTO Y EMPRESAS DE MUJERES

En cumplimiento a lo establecido en el artículo 2.2.1.2.4.2.14 del Decreto 1082 de 2015, modificado por el artículo 3 del Decreto 1860 de 2021, si los proponentes acreditan su condición de emprendimiento de mujeres, se dará aplicación al siguiente criterio diferencial:

El proponente deberá acreditar experiencia en máximo cinco (05) contratos ejecutados y/o certificaciones cuyo objeto sea renovación, actualización, suministro y/o adquisición de licencias Endpoint Enterprise y/o soluciones de Network Security IPS y/o servicio de monitoreo de red NX, dentro de los diez (10) años anteriores a la fecha del cierre de proceso de selección y donde la sumatoria (individual o conjunta) de los mismos sea igual o superior al cien por ciento (100%) del presupuesto oficial estimado. Dichos contratos estarán comprendidos en mínimo uno (01) de los siguientes códigos de clasificación UNSPSC relacionados en la Tabla No. 3.

Tabla 3 - Experiencia requerida

Código del Clasificador de Bienes y Servicios		Cuantía - SMMLV
43233200	Software de seguridad y protección	3.548,69
81111800	Servicio de sistemas y administración de componentes de sistemas	
81112200	Mantenimiento y soporte de software	

REQUISITO DIFERENCIAL PARA INCENTIVAR LAS MIPYMES

En cumplimiento a lo establecido en el artículo 3 del Decreto 1860 de 2021, si los proponentes acreditan su condición de MIPYME dando cumplimiento al artículo 2.2.1.2.4.2.18 del Decreto 1860 de 2021, se dará aplicación al siguiente criterio diferencial:

El proponente deberá acreditar experiencia en máximo cinco (05) contratos ejecutados y/o certificaciones cuyo objeto sea renovación, actualización, suministro y/o adquisición de licencias Endpoint Enterprise y/o soluciones de Network Security IPS y/o servicio de monitoreo de red NX, dentro de los diez (10) años anteriores a la fecha del cierre de proceso de selección y donde la sumatoria (individual o conjunta) de los mismos sea igual o superior al cien por ciento (100%) del presupuesto oficial estimado. Dichos contratos estarán comprendidos en mínimo uno (01) de los siguientes códigos de clasificación UNSPSC relacionados en la Tabla No. 3.

Tabla 3 - Experiencia requerida

Código del Clasificador de Bienes y Servicios		Cuantía - SMMLV
43233200	Software de seguridad y protección	3.548,69
81111800	Servicio de sistemas y administración de componentes de sistemas	
81112200	Mantenimiento y soporte de software	

CRITERIOS HABILITANTES DIFERENCIALES DE EXPERIENCIA PARA EMPRENDIMIENTOS Y EMPRESAS DE PERSONAS CON DISCAPACIDAD, EN EL SISTEMA DE COMPRAS PÚBLICAS EXPERIENCIA ESPECIFICA.

En cumplimiento a lo establecido en el artículo 2.2.1.2.4.2.7.3. del Decreto 0287 de 2026, si los proponentes acreditan su condición de emprendimientos y empresas de personas con discapacidad, se dará aplicación al siguiente criterio diferencial:

El proponente deberá acreditar experiencia en máximo cinco (05) contratos ejecutados y/o certificaciones cuyo objeto sea renovación, actualización, suministro y/o adquisición de licencias Endpoint Enterprise y/o soluciones de Network Security IPS y/o servicio de monitoreo de red NX, dentro de los diez (10) años anteriores a la fecha del cierre de proceso

de selección y donde la sumatoria (individual o conjunta) de los mismos sea igual o superior al cien por ciento (100%) del presupuesto oficial estimado. Dichos contratos estarán comprendidos en mínimo uno (01) de los siguientes códigos de clasificación UNSPSC relacionados en la Tabla No. 3.

Tabla 3 - Experiencia requerida

Código del Clasificador de Bienes y Servicios		Cuantía - SMMLV
43233200	Software de seguridad y protección	3.548,69
81111800	Servicio de sistemas y administración de componentes de sistemas	
81112200	Mantenimiento y soporte de software	

NOTAS APLICABLES PARA LA ACREDITACIÓN DE LA EXPERIENCIA HABILITANTE PARA TODOS LOS PROPONENTES.

NOTA 1: Las certificaciones aportadas por los oferentes las cuales deben contener como mínimo la siguiente información: Contratante, nombre del contratista, porcentaje de participación del valor que ejecutó, como miembro de un consorcio, unión temporal, objeto del contrato, fecha de inicio y terminación, duración del contrato, cumplimiento o recibo a satisfacción del servicio contratado, monto del contrato incluido adiciones a la fecha de terminación del contrato, persona de contacto para su verificación, número telefónico, dirección, e-mail, firma de la persona autorizada, indicando nombre completo y cargo.

Nota 2: Los contratos que se tendrá en cuenta para acreditar la experiencia requerida deberán estar debidamente clasificados en el RUP con el código UNSPSC hasta el tercer nivel y su cuantía expresada en SMMLV, lo cual indica que los contratos se encuentran ejecutados y las inscripciones de estos en firme. No se aceptarán los contratos que en el RUP aparezcan en la sección de contratos adjudicados o contratos en ejecución.

Nota 3: La experiencia del oferente plural (unión temporal, consorcio o promesa de sociedad futura) podrá ser acreditada por uno o varios de sus integrantes. Sin embargo, para efectos de la verificación, la experiencia derivada de un contrato en el que el proponente haya participado como integrante de un contratista plural se ponderará en proporción al valor del contrato y su porcentaje de participación en el mismo registrado en el RUP.

Nota 4: Para el cálculo de los valores de los contratos expresados en salarios mínimos mensuales legales vigentes (SMMLV) para la acreditación de la experiencia, se tomará como referencia el salario fijado por los Ministerios del Trabajo y de Hacienda y Crédito Público para la vigencia correspondiente a la fecha de terminación del contrato.

Nota 5: En caso de que se alleguen documentos del contrato cuyo objeto relacione otros bienes o servicios, se deberá especificar claramente el valor ejecutado de los bienes o servicios que estén relacionados con el objeto del presente proceso de selección.

Nota 6: En caso de que el proponente allegue un número superior de contratos y/o certificaciones a los exigidos, **LA UNIDAD**, tomará en cuenta solo los tres (3) primeros en orden cronológico de la más reciente a la más antigua. Si las certificaciones de cumplimiento de los contratos allegadas no cumplen con lo requerido por **LA UNIDAD**, se verificarán las certificaciones adicionales que se presenten, las cuales en todo caso deberán acreditar todos los requisitos solicitados por la Entidad.

Nota 7: Para el caso de los criterios diferenciales, en caso de que el proponente allegue un número superior de contratos y/o certificaciones a los exigidos, **LA UNIDAD**, tomará en cuenta solo los cinco (5) primeros en orden cronológico de la más reciente a la más antigua.

Nota 8: Los criterios diferenciales para MIPYMES, para oferentes plurales sólo se aplicarán si por lo menos uno de los integrantes acredita la calidad de Mipyme y tiene una participación igual o superior al diez por ciento (10%) en el consorcio o unión temporal.

Nota 9: Cuando las certificaciones expresen su valor en moneda extranjera, se tendrá en cuenta la TRM a la fecha en que se celebró el contrato certificado.

Nota 10: En caso de que el oferente presente con su oferta los formatos o certificaciones de experiencia y éstos no cumplan con la totalidad de la información solicitada, **LA UNIDAD** requerirá al oferente a fin de que subsane lo correspondiente dentro del plazo que le señale para el efecto.

Nota 11: El proponente que no acredite experiencia, su oferta será rechazada.

Nota 12: La **UNIDAD** se reserva el derecho de verificar la información suministrada por el proponente y de solicitar las aclaraciones que considere convenientes.

Nota 13: No se aceptarán auto certificaciones.

6.1.4. REQUISITO TÉCNICO HABILITANTE ADICIONAL

6.1.4.1 CERTIFICACIÓN DEL FABRICANTE.

El oferente deberá presentar con su propuesta certificación vigente a la fecha del cierre del presente proceso como distribuidor autorizado en Colombia, expedido por el fabricante TRELIX, donde indique que se encuentra autorizado para vender y dar soporte a sus productos de seguridad requeridos.

Cuando se trate de un consorcio o una unión temporal, uno de sus miembros deberá presentar dicha certificación.

6.1.4.2 CERTIFICACIÓN COMO PARTNER

El oferente deberá presentar con su propuesta certificación vigente a la fecha del cierre del presente proceso expedida por el fabricante TRELIX donde lo acredite como canal Gold o superior en Colombia. Adicionalmente deberá presentar con su propuesta certificación vigente, expedida por el fabricante, donde lo acredite como service provider Specialization, la cual acredita la experiencia y conocimiento para la gestión de los servicios objeto del presente proceso para la Entidad.

Cuando se trate de un consorcio o una unión temporal, uno de sus miembros deberá presentar dicha certificación.

6.1.4.3 MANIFESTACIÓN DEL OFERENTE SOBRE EL SISTEMA EN SEGURIDAD Y SALUD EN EL TRABAJO (REQUISITO HABILITANTE).

El proponente deberá diligenciar y presentar con su oferta el Formulario "*MANIFESTACIÓN DEL OFERENTE SOBRE SISTEMA DE GESTIÓN EN SEGURIDAD Y SALUD EN EL TRABAJO (SG-SST)*", mediante el cual hace constar que dispone de un Sistema de Gestión de la Seguridad y Salud en el Trabajo, que le permita a la organización anticipar, reconocer, evaluar y controlar los

riesgos que puedan afectar la seguridad y la salud en el trabajo, de conformidad con el Decreto único Reglamentario 1072 de 2015 y la Resolución No. 312 de 2019, y las normas que las modifiquen o sustituyan.

Si la propuesta es presentada bajo la modalidad de Consorcio o Unión Temporal, cada uno de los miembros de estos deberá cumplir con el requisito en mención

6.1.4.4 PLAN DE MANEJO INTEGRAL DE RESIDUOS APARATOS ELÉCTRICOS Y ELECTRÓNICOS

El proponente deberá presentar con su propuesta un documento donde describa el procedimiento que llevará a cabo para la recolección y disposición final de los RAEE (Residuos de los Aparatos Eléctricos y Electrónicos) bajo los lineamientos de la norma ISO 14001 2015, de los dispositivos o partes reemplazadas durante la ejecución del presente contrato, garantizando que no dejará estos residuos en las instalaciones de la Entidad.

FOMENTO A LA EJECUCIÓN DE CONTRATOS ESTATALES POR PARTE DE POBLACIÓN EN POBREZA EXTREMA, DESPLAZADOS POR LA VIOLENCIA, PERSONAS EN PROCESO DE REINTEGRACIÓN O REINCORPORACIÓN Y SUJETOS DE ESPECIAL PROTECCIÓN CONSTITUCIONAL

En relación con el artículo 2.2.1.2.4.2.16. Decreto 1082 de 2015 adicionado por el artículo 3º del Decreto 1860 de 2021, mediante el cual se establece la obligación por parte de las entidades estatales de incluir la obligatoriedad de vincular bienes o servicios prestados por población en pobreza extrema, desplazados por la violencia, personas en proceso de reintegración o reincorporación y sujetos de especial protección constitucional, y previo al análisis de la naturaleza del tipo de contrato a celebrarse y su objeto contractual, para el presente proceso de contratación no se considera conveniente ni oportuno dar aplicación a lo dispuesto en el mencionado precepto normativo, teniendo en cuenta que el objeto contractual solo puede ejecutarse por empresas dedicadas al comercio de comercio de software y tecnologías de la información y ciberseguridad, lo que limita la cantidad de participantes que puedan presentarse al proceso contractual.

6.1.5. CAPACIDAD FINANCIERA

INDICADOR FINANCIERO	REQUERIDO
Índice de Liquidez (Activo Corriente / Pasivo Corriente)	$\geq$ (mayor o igual a) 1,70
Índice de Endeudamiento (Pasivo Total / Activo Total)	$\leq$ (menor o igual a) 0,60
Índice de Cobertura de Intereses (Utilidad Operacional / Gastos de Intereses)	$\geq$ (mayor o igual a) 1,53

6.1.6. CAPACIDAD ORGANIZACIONAL

INDICADOR ORGANIZACIONAL	REQUERIDO
Rentabilidad del Patrimonio (Utilidad Operacional / Patrimonio)	$\geq$ (mayor o igual a) 0,11
Rentabilidad del Activo (Utilidad Operacional / Activo Total)	$\geq$ (mayor o igual a) 0,07

6.1.7. INFORMACIÓN FINANCIERA PARA PROPONENTES EXTRANJEROS

Los Proponentes extranjeros deben presentar la información financiera que se relaciona a continuación, de conformidad con la legislación propia del país de origen, avalados con la firma de quien se encuentre en obligación de hacerlo de acuerdo con la normativa vigente del país de origen:

- (i) Balance general
- (ii) Estado de resultados

Los anteriores documentos también deben ser presentados utilizando el Plan Único de Cuentas para Colombia (PUC).

7. FACTORES DE SELECCIÓN

Para el caso de la SELECCIÓN ABREVIADA PARA LA ADQUISICIÓN DE BIENES Y SERVICIOS DE CARACTERÍSTICAS TÉCNICAS UNIFORMES Y DE COMÚN UTILIZACIÓN debe tenerse en cuenta que la oferta más favorable a la entidad será aquella con el menor precio y, por tanto, en las subastas inversas para la adquisición de estos bienes o servicios se tendrá como único criterio de evaluación el precio.

8. EVALUACIÓN DE LA OFERTA

La **UNIDAD** adjudicará al proponente que haya ofertado el menor valor válido dentro del evento de subasta, incluido el impuesto al valor agregado IVA, y demás impuestos, tasas, contribuciones, costos directos e indirectos a que haya lugar.

Así mismo, se precisa que la adjudicación del presente proceso de selección se realizará teniendo en cuenta los valores unitarios de los ítems, razón por la cual el proponente seleccionado luego del evento de subasta, si a ello hubiere lugar, deberá presentar su estructura de costos ajustada.

En consecuencia, los proponentes deben presentar su oferta dando cabal cumplimiento de los requisitos mínimos exigidos y cotizar la totalidad de los **ítems** que lo componen.

Para la presentación de la propuesta económica se deberá diligenciar el presente anexo económico:

ITEM	DESCRIPCIÓN	CANTIDAD	VALOR UNITARIO INCLUIDO IVA	PRECIO TOTAL CON IVA
1	Endpoint Enterprise Cloud +managed detection y response	5200		
2	Solución Data Security Endpoint Protection Suite - Subscription	680		
3	Network Security Manager Software Subscription Starter Edition	8		
4	Advanced RMA (NBD) Hardware Support IPS NS3600	8		
5	IPS NS3600 - 5Gbps Software license	8		

	(Throughput based entitlement)			
6	Advanced RMA (NBD) Hardware Support Network Security 4-Port 10/1	8		
7	API	4		
8	Network Security NX Edition (Enterprise)	6000		
9	IVX Enterprise Cloud	40000		
10	Servicio de soporte técnico	4		

El margen mínimo de mejora **será mayor o igual $\geq$ al 2%** del valor total de la oferta.

9. FACTORES DE DESEMPATE

Método Aleatorio:

1. La Unidad ordenará a los proponentes empatados en orden alfabético según el nombre de la persona natural, persona jurídica o el proponente plural registrado en el SECOP. Una vez ordenados, le asignará un número entero a cada uno de estos de forma ascendente, de tal manera que al primero de la lista le corresponda el número 1.
2. Seguidamente, la Unidad tomará la parte entera (números a la izquierda de la coma decimal) de la TRM que rigió el día del cierre y procederá a dividir esta parte entera entre el número total de proponentes en empate, para posteriormente tomar su residuo y utilizarlo en la selección final.
3. Realizados estos cálculos, la Unidad seleccionará a aquel proponente que presente coincidencia entre el número asignado y el residuo encontrado. En caso de que el residuo sea cero (0), se escogerá al proponente con el mayor número asignado.
4. La Unidad ordenará a los proponentes empatados en orden alfabético según el nombre de la persona natural, persona jurídica o el proponente plural registrado en el SECOP. Una vez ordenados, le asignará un número entero a cada uno de estos de forma ascendente, de tal manera que al primero de la lista le corresponda el número 1.
5. Seguidamente, la Unidad tomará la parte entera (números a la izquierda de la coma decimal) de la TRM que rigió el día del cierre y procederá a dividir esta parte entera entre el número total de proponentes en empate, para posteriormente tomar su residuo y utilizarlo en la selección final.
6. Realizados estos cálculos, la Unidad seleccionará a aquel proponente que presente coincidencia entre el número asignado y el residuo encontrado. En caso de que el residuo sea cero (0), se escogerá al proponente con el mayor número asignado.

Nota 1: Los factores de desempate deberán aplicarse en armonía con los Acuerdos Comerciales vigentes suscritos por Colombia. De esta manera, en el evento en que el empate se presente entre ofertas cubiertas por un Acuerdo Comercial, se aplicarán los factores de desempate que sean compatibles con los mencionados Acuerdos.

Nota 2: Si el empate entre las propuestas se presenta con un Proponente, bien o servicio extranjero cuyo país de origen no tiene Acuerdo Comercial con Colombia, ni trato nacional por reciprocidad o con ocasión de la normativa comunitaria, se dará aplicación a todos los criterios de desempate previstos en el presente numeral.

Nota 3: Conforme con el artículo 18 de la Ley 1712 de 2014 y los artículos 5 y 6 de la Ley 1581 de 2012, la Entidad garantizará el derecho a la reserva legal de toda aquella información que acredita el cumplimiento de los factores de desempate de: i) las mujeres víctimas de violencia intrafamiliar, ii) las personas en proceso de reincorporación y/o reintegración y iii) la población indígena, negra, afrocolombiana, raizal, palenquera, Rrom o gitana.

De acuerdo con lo anterior, en la plataforma del SECOP no se publicará la información relacionada con los factores de desempate de personas en procesos de reincorporación o reintegración o mujeres víctimas de violencia intrafamiliar o la población indígena, negra, afrocolombiana, raizal, palenquera, Rrom o gitana, puesto que su público conocimiento puede afectar el derecho a la intimidad de los oferentes o de sus trabajadores o socios o accionistas.

Nota 4: Para efectos de los factores de desempate dispuestos en este numeral, se entiende por experiencia acreditada en la oferta, la sumatoria de los contratos que demuestren la experiencia general de la actividad principal, expresados en salarios mínimos mensuales legales vigentes (SMMLV).

Nota 5: La omisión de la información requerida las reglas previstas en el artículo 2.2.1.2.4.2.17 del Decreto 1082 de 2015 desde la presentación de la oferta, no será subsanables por considerarse factores relevantes en la adjudicación del proceso de selección. En todo caso, su no presentación no restringe la participación del proponente, ni es causal de rechazo de la propuesta.

10. RIESGOS

De acuerdo con la metodología de Colombia Compra Eficiente, a continuación, se identifican los Riesgos del Proceso de Contratación desde su planeación hasta su terminación o liquidación si aplica (ver anexo No. 2).

11. GARANTÍAS

11.1. GARANTÍA DE SERIEDAD DE LA OFERTA

El Proponente debe presentar junto con la oferta una garantía de seriedad de la oferta a favor de la UNIDAD ADMINISTRATIVA ESPECIAL DE LA JUSTICIA PENAL MILITAR Y POLICIAL con NIT. 900.384.997-1, por un valor de diez por ciento (10%) del valor del presupuesto oficial estimado y con vigencia de noventa (90) días calendario, contados desde la fecha de presentación de ofertas establecida en el cronograma.

11.2. GARANTÍA DE CUMPLIMIENTO

El contratista deberá asumir por su cuenta y costo, a fin de asegurar el cumplimiento de las obligaciones emanadas del contrato, cualquiera de las garantías establecidas en el artículo 2.2.1.2.3.1.2 del Decreto 1082 de 2015 a favor de la UNIDAD ADMINISTRATIVA ESPECIAL DE LA JUSTICIA PENAL MILITAR Y POLICIAL con NIT. 900.384.997-1, de conformidad con la Subsección 1 de la Sección 3 del Decreto 1082 de 2015. La garantía deberá ser subida a través de la plataforma del SECOP II y deberá amparar los siguientes riesgos:

Tabla 4. Suficiencia y vigencia de los amparos de la garantía de cumplimiento

AMPARO	SUFICIENCIA	VIGENCIA
Cumplimiento del contrato	20% del valor total del contrato	Por el término de ejecución del contrato y doce (12) meses más.
Pago de salarios prestaciones sociales legales e indemnizaciones laborales	10% del valor total del contrato	Por el término de ejecución del contrato y tres (3) años más
Calidad de servicio	20% del valor total del contrato	Por el término de ejecución del contrato y doce (12) meses más.
Calidad y correcto funcionamiento de los bienes	20% del valor total del contrato	Por el término de ejecución del contrato y doce (12) meses más.

10.3. RESPONSABILIDAD CIVIL EXTRA CONTRACTUAL

El contratista debe presentar una garantía de responsabilidad civil extracontractual, a favor de la UNIDAD ADMINISTRATIVA ESPECIAL DE LA JUSTICIA PENAL MILITAR Y POLICIAL con NIT. 900.384.997-1, de conformidad con la Subsección 1 Sección 3 del Decreto 1082 de 2015. La garantía deberá ser presentada al Grupo de Contratos:

Tabla 5. Responsabilidad Civil Extracontractual

AMPARO	SUFICIENCIA	VIGENCIA
Responsabilidad civil extracontractual	400 SMMLV	Por el plazo de ejecución del contrato

11. ACUERDOS INTERNACIONALES O TRATADOS DE LIBRE COMERCIO VIGENTE

De conformidad con lo previsto en el literal a) del artículo 2.2.1.2.4.1.3 del Decreto 1082 de 2015, el Proceso de Contratación está sujeto a los siguientes Acuerdos Comerciales. En consecuencia, las Ofertas de bienes y servicios de países con los cuales Colombia tiene Acuerdos Comerciales vigentes que cubren el presente Proceso de Contratación, serán tratados como Ofertas de bienes y servicios colombianos, tendrán derecho al puntaje para estimular la industria nacional si aplica, y la Unidad elaborará el cronograma de acuerdo con los plazos previstos en dichos Acuerdos Comerciales.

Tabla 6. Cobertura Acuerdos Comerciales

Acuerdo Comercial		¿Vigente?	Entidad Estatal cubierta	Valor del Proceso de Contratación superior al umbral del Acuerdo Comercial	Excepción Aplicable al Proceso de Contratación	Proceso de Contratación cubierto por el Acuerdo Comercial
		Si/No	Si/No	Si/No	Si/No	Si/No
Alianza Pacífico	Chile	SI	SI	SI	NO	SI
	México	SI	SI	SI	NO	SI
	Perú	SI	SI	SI	NO	SI
Canadá		SI	SI	SI	NO	SI
Chile		SI	SI	SI	NO	SI
Corea		SI	SI	SI	NO	SI
Costa Rica		SI	SI	SI	NO	SI
Estados Unidos		SI	SI	SI	NO	SI
Estados AELC		SI	SI	SI	NO	SI
México		SI	SI	SI	NO	SI
Triángulo Norte	El Salvador	SI	SI	SI	NO	SI
	Guatemala	SI	SI	SI	NO	SI
	Honduras	SI	NO	N/A	NO	No
Unión Europea		SI	SI	SI	NO	SI
Israel		SI	SI	SI	NO	SI
Reino Unido e Irlanda del Norte		SI	SI	SI	NO	SI
Comunidad Andina		SI	N/A	N/A	N/A	SI

12. COMPROMISO ANTICORRUPCIÓN

La UNIDAD ADMINISTRATIVA ESPECIAL DE LA JUSTICIA PENAL MILITAR Y POLICIAL, está comprometida con la prevención de los actos de corrupción en la contratación estatal con base en la Constitución Política, la ley, los tratados internacionales y, en especial, con los principios de transparencia, buena fe, planeación, eficacia, precaución y moralidad administrativa.

Bogotá D.C., 5 de octubre de 2026



PD. FREDY ARBEY ROMERO SILVA

Coordinador Grupo de Plataforma Tecnológica (E)

	NOMBRE	FIRMA	FECHA
Aprobó	ING. Henry Vargas Sierra. Jefe Oficina de las Tecnologías de la Información y las Comunicaciones		05/10/2026
Revisó	ING. Carlos Useda - Contratista		05/10/2026

ANEXO No. 1 ESPECIFICACIONES TÉCNICAS MÍNIMAS EXIGIDAS

1. FECHAS DE RENOVACIÓN

A través del presente anexo se establecen las especificaciones técnicas requeridas para la renovación de los servicios de soporte y mantenimiento del licenciamiento de las suites Trellix, de conformidad con los componentes, características y cantidades que se relacionan a continuación.

La contratación de estos servicios tiene como finalidad garantizar la continuidad operativa, la actualización permanente y el soporte especializado de las soluciones de seguridad actualmente implementadas en la Entidad, asegurando su correcto funcionamiento y la protección de la infraestructura tecnológica institucional.

ÍTEM	DESCRIPCIÓN PRODUCTO ACTUAL	CANTIDAD	FECHA DE VENCIMIENTO	FECHA DE RENOVACION Y/O ACTUALIZACION	PRODUCTOS A SUMINISTRAR
1	Endpoint Enterprise Cloud +managed detection y response	1300	29 diciembre de 2026	29 de diciembre de 2030	1300 licencias de la solución Endpoint Enterprise Cloud+ managed detection y response
2	Solución Data Security Endpoint Protection Suite - Subscription	170	29 diciembre de 2026	29 de diciembre de 2030	170 licencias de la solución Data Security Endpoint Protection Suite - Subscription
3	Network Security Manager Software Subscription Starter Edition	2	29 diciembre de 2026	29 de diciembre de 2030	2 licencias de la solución Network Security Manager Software Subscription Starter Edition
4	Advanced RMA (next business day ship) Hardware Support IPS NS 3600	2	29 diciembre de 2026	29 de diciembre de 2030	2 licencias Advanced RMA (next business day ship) Hardware Support para el equipo IPS
5	IPS NS3600 - 5Gbps Software license (Throughput based entitlement)	2	29 diciembre de 2026	29 de diciembre de 2030	2 licencias IPS NS3600 - 5Gbps Software license (Throughput based entitlement)
6	Advanced RMA (next business day ship) Hardware Support Network Security 4-Port 10/1	2	29 diciembre de 2026	29 de diciembre de 2030	2 licencias Advanced RMA (next business day ship) Hardware Support para módulo de expansión
7	API	1	29 diciembre de 2026	29 de diciembre de 2030	1 licencia de API
8	Network Security NX Edition (Enterprise)	1500	29 diciembre de 2026	29 de diciembre de 2030	Licencia por valor de 1500 para Network Security NX Edition (Enterprise)
9	IVX Enterprise Cloud -Banded Submission Pack	10000	29 diciembre de 2026	29 de diciembre de 2030	Licencia por valor de 10000 para IVX Enterprise Cloud -Banded Submission Pack
10	Servicio de soporte técnico	1	29 diciembre de 2026	29 de diciembre de 2030	

El contratista se obliga a entregar y registrar a nombre de LA UNIDAD ante el fabricante TRELLIX (indicando los respectivos códigos NAI / Grant Number asignados a la Entidad) la renovación total del licenciamiento, soporte de hardware, suscripciones y servicios descritos en el cuadro técnico de productos, con fecha de inicio a partir del 30 de diciembre de 2026 y vigencia garantizada y continua hasta el 29 de diciembre de 2030, en las siguientes cantidades y especificaciones:

- 1. 1.300 licencias de la solución Endpoint Enterprise Cloud + Managed Detection and Response (MDR).
- 2. 170 licencias de la solución Data Security Endpoint Protection Suite - Subscription.
- 3. 2 licencias/suscripciones de Network Security Manager Software Subscription Starter Edition.
- 4. 2 licencias/suscripciones de Advanced RMA (next business day ship) Hardware Support para el equipo IPS NS3600.
- 5. 2 licencias de IPS NS3600 - 5Gbps Software License (Throughput based entitlement).
- 6. 2 licencias/suscripciones de Advanced RMA (next business day ship) Hardware Support para el módulo de expansión de red Network Security 4-Port 10/1.
- 7. 1 licencia de API de integración del fabricante.
- 8. 1.500 licencias para Network Security NX Edition (Enterprise).
- 9. 10.000 licencias/submisiones para IVX Enterprise Cloud - Banded Submission Pack.
- 10.Soporte técnico de la solución de seguridad.

EL CONTRATISTA deberá entregar a la supervisión del contrato la certificación escrita expedida y firmada por el fabricante TRELLIX, junto con la visualización en el portal web institucional de LA UNIDAD, que acredite la vigencia ininterrumpida y activa de todos los ítems hasta el 29 de diciembre de 2030.

2. CARACTERÍSTICAS DE LA RENOVACIÓN DE LAS SOLUCIONES.

ITEM	RENOVACIÓN DE LAS SOLUCIONES.
1.	1. CARACTERÍSTICAS DE LA RENOVACIÓN DE SOLUCIONES DE CIBERSEGURIDAD
	REQUERIMIENTOS NX
	1.1. Capacidades del Sistema de Prevención de Intrusiones (IPS) El contratista deberá mantener en correcta operación las funcionalidades del Sistema de Prevención de Intrusiones (IPS) de la solución NX, garantizando, como mínimo, el cumplimiento de los siguientes requerimientos: a) Actualizar y configurar la tecnología IPS para habilitar la validación automática de alertas y fortalecer el cumplimiento de los requisitos normativos, regulatorios y de seguridad aplicables a la Entidad. b) Configurar la inspección y análisis de archivos comprimidos en formatos ZIP, RAR, TNEF y 7-ZIP, así como de encabezados X-Forwarded-For (XFF) y objetos web ofuscados mediante técnicas XOR (Exclusive-OR). Adicionalmente, deberá habilitar las funcionalidades de restablecimiento de conexiones TCP y bloqueo fuera de banda (Out-of-Band Blocking) para fortalecer la capacidad de respuesta frente a amenazas. c) Actualizar y configurar las políticas del sistema IPS utilizando criterios avanzados de clasificación y correlación, tales como objetivo del ataque (cliente o servidor), nivel de severidad, categoría, dirección del tráfico, identificador CVE y protocolo, con el fin de optimizar la detección, clasificación y respuesta ante eventos de seguridad. d) Actualizar y configurar el motor de reglas IPS para garantizar su compatibilidad con el formato de reglas Snort 2.9 o superior, asegurando la interoperabilidad con reglas existentes y facilitando la adopción de nuevas firmas de seguridad. e) Configurar la importación y administración de reglas IPS personalizadas mediante archivos en formato ASCII o CSV, permitiendo la incorporación de atributos como identificador único de firma, mensaje descriptivo, protocolo, nivel de severidad, categoría y subcategoría, con el propósito de facilitar la personalización,

ITEM	RENOVACIÓN DE LAS SOLUCIONES.
	administración y fortalecimiento de los controles de seguridad implementados por la Entidad. 1.2. Análisis y Detección de Malware: a) Configurar la extracción de objetos directamente desde el sensor mediante la interfaz de línea de comandos (CLI), facilitando las labores de análisis e investigación de eventos de seguridad. b) Actualizar y configurar la compatibilidad con el formato de reglas YARA, permitiendo mejorar las capacidades de análisis y detección de malware avanzado. c) Configurar el motor de análisis para identificar objetos y direcciones URL maliciosas asociadas a ataques de múltiples flujos (multiflow attacks), fortaleciendo la detección de amenazas complejas. d) Actualizar y configurar los mecanismos de identificación de malware para reconocer una amplia variedad de tipos de archivos y objetos, incluyendo formatos PDF, SWF, CAB, XML, EXE, JNLP, XDP, JS, IMG, CHM, MACHO, XAP, HTML, JAR, HWP, CLASS, XAR y DLL. e) Configurar la extracción automática de archivos comprimidos sospechosos para su análisis mediante el motor avanzado de detección de malware, optimizando la identificación de amenazas ocultas. f) Configurar la detección y el envío de objetos web ofuscados mediante técnicas XOR (Exclusive-OR) para su análisis especializado, incrementando la capacidad de detección frente a técnicas de evasión. g) Configurar la detección de eventos asociados a mensajes de "bloqueo por proxy", mediante la identificación de cadenas de texto específicas dentro del tráfico de red, contribuyendo a una mejor visibilidad y correlación de eventos de seguridad. 1.3. Intercepción de Tráfico y Metadatos: El contratista mantener en operación la solución de análisis avanzado de amenazas que cumpla, como mínimo, con los siguientes requisitos técnicos: a) Configurar la solución como un appliance virtual especializado, con capacidad de operar en modo en línea para analizar, detectar y bloquear amenazas en tiempo real. Asimismo, deberá habilitar la inspección de tráfico SSL/TLS entrante mediante un esquema de proxy inverso (Reverse Proxy) y la descryptación segura del tráfico HTTPS utilizando certificados de servidor y claves privadas importadas. b) Configurar la solución para operar en modo mirror o en línea, permitiendo el análisis y bloqueo de amenazas en tiempo real. c) Implementar la inspección de tráfico SSL/TLS entrante mediante un mecanismo de proxy inverso. d) Configurar la interceptación y descryptación segura del tráfico HTTPS utilizando certificados de servidor y claves privadas importadas. e) Habilitar la activación y desactivación de la inspección de hashes MD5 y SHA-256, así como la extracción e identificación de bibliotecas dinámicas (DLL) maliciosas, incorporando los resultados en los detalles de las alertas generadas por el motor avanzado de análisis de malware y los entornos de sandboxing. f) Configurar mecanismos de identificación de las diferentes fases de los ataques basados en la web, incluyendo explotación inicial, descarga de malware y comunicaciones de retorno (callbacks) hacia infraestructuras de comando y control (C2/CnC). g) Implementar capacidades para detectar actividades maliciosas dentro de la red interna, tales como movimiento lateral, reconocimiento interno y exfiltración de información. h) Configurar la clasificación del ciclo de vida de una infección en, como mínimo, dos fases: Fase de Infección, relacionada con la explotación de vulnerabilidades y descarga de código malicioso, y Fase de Callback, asociada a las comunicaciones hacia servidores de comando y control y la extracción de información. i) Alinear las capacidades de detección con el marco de referencia MITRE ATT&CK™, proporcionando mecanismos de detección multicapa que permitan

ITEM	RENOVACIÓN DE LAS SOLUCIONES.
	priorizar la respuesta de seguridad de acuerdo con la fase del ataque y el nivel de riesgo identificado. j) Configurar el motor de análisis para identificar objetos y URL maliciosas asociadas a ataques multiflujo (multiflow attacks), así como archivos potencialmente utilizados para la distribución de malware, incluyendo formatos PDF, SWF, CAB, XML, EXE, JNLP, XDP, JS, IMG, CHM, MACHO, XAP, HTML, JAR, HWP, CLASS, XAR y DLL. k) Implementar funcionalidades de identificación, monitoreo, generación de alertas y bloqueo de aplicaciones clasificadas como Riskware. l) Configurar capacidades de análisis de tráfico SMB y SMBv2 para la detección de malware, herramientas de postexplotación y otros objetos maliciosos. m) Implementar técnicas avanzadas de detección de alta fidelidad, incorporando múltiples motores y métodos de análisis para identificar amenazas conocidas, desconocidas y emergentes. n) Configurar la integración con servicios de inteligencia de amenazas del fabricante, permitiendo la priorización de alertas mediante análisis avanzados y contextualización de eventos. o) Implementar mecanismos de descarga e instalación automática de actualizaciones de seguridad provenientes de la plataforma de inteligencia de amenazas en la nube del fabricante, sin requerir la transmisión de información sensible hacia servicios externos. p) Configurar la integración con servicios de inteligencia de amenazas basados en la nube del fabricante para obtener información contextual sobre eventos verificados, incluyendo actor de amenaza, objetivo comprometido y recomendaciones de mitigación. q) Implementar mecanismos que permitan identificar eventos asociados a mensajes de "bloqueo por proxy", diferenciando entre bloqueos realizados por la infraestructura de proxy corporativa y aquellos efectuados por la propia solución. r) Permitir la creación y administración de listas blancas (whitelists) personalizadas para dominios autorizados. s) Mantener capacidades de detección que permitan identificar comunicaciones con dominios recién registrados o catalogados como maliciosos, actividades de tunelización mediante DNS e ICMP, intentos de phishing orientados al robo de credenciales, anomalías SSL/TLS, actividad asociada a la red Tor y accesos a URL sospechosas. t) Soportar reglas YARA para el análisis de malware, incluyendo la utilización de reglas personalizadas con ponderaciones asociadas y capacidades avanzadas de detección sobre diferentes tipos de archivos. u) Disponer de un motor de análisis multivectorial para la detonación controlada y evaluación de amenazas avanzadas en entornos aislados. v) Implementar y configurar, como mínimo, un segmento de red con conectividad de 1 Gbps, a través de interfaces RJ45 o fibra óptica. w) Proporcionar capacidades para la detección y análisis de Amenazas Persistentes Avanzadas (APT) y ataques de Día Cero (Zero-Day) con altos niveles de precisión. x) Analizar muestras de malware en entornos de sandboxing, utilizando máquinas virtuales aisladas y alojadas dentro del propio dispositivo o solución, garantizando que el tráfico generado durante el análisis permanezca dentro de la infraestructura controlada. y) Extraer archivos comprimidos sospechosos en formatos ZIP, RAR, TNEF y 7-ZIP para su análisis mediante motores avanzados de detección de malware y entornos de sandboxing. z) Extraer e identificar bibliotecas dinámicas (DLL) maliciosas e incorporarlas en los detalles de las alertas generadas por el motor avanzado de análisis de malware y sandboxing. - aa) Capturar y conservar todos los archivos creados o modificados durante los procesos de análisis en sandboxing, con el fin de apoyar actividades de investigación forense, análisis de incidentes y respuesta ante eventos de seguridad. 1.4. Inteligencia de Amenazas e IOCs: El contratista deberá mantener en operación las funcionalidades de inteligencia de amenazas e indicadores de compromiso (IOC), cumpliendo como mínimo con los siguientes requerimientos técnicos:

ITEM	RENOVACIÓN DE LAS SOLUCIONES.
	a) Implementar mecanismos para la descarga e instalación automática de actualizaciones de seguridad y contenido de inteligencia de amenazas proporcionados por el fabricante, sin requerir la transmisión de información sensible de la Entidad hacia servicios externos. b) Configurar la solución para analizar fuentes personalizadas de Indicadores de Compromiso (IOC), incluyendo direcciones IP, dominios, URL y hashes MD5/SHA-256, mediante la importación de archivos planos o formatos estandarizados XML STIX. c) Implementar capacidades que permitan ejecutar acciones automáticas sobre los IOC asociados a dominios, incluyendo la generación de alertas, el bloqueo de amenazas y la aplicación de políticas de seguridad previamente definidas. d) Garantizar que la solución pueda consumir y utilizar inteligencia de amenazas proveniente de los servicios en la nube del fabricante, con el fin de enriquecer, contextualizar y priorizar las alertas de seguridad generadas. e) Implementar y configurar reglas dinámicas para la detección de comunicaciones de retorno (callbacks) asociadas a actividades maliciosas, compromisos de seguridad o comunicaciones con infraestructuras de comando y control (C2/CnC). f) Implementar funcionalidades para la creación, administración y mantenimiento de listas blancas (whitelists) personalizadas de dominios autorizados, permitiendo excluir recursos confiables de los procesos de inspección y bloqueo definidos por la Entidad. 1.5. Informes y Monitoreo: El contratista deberá mantener en operación las funcionalidades de monitoreo, generación de informes y notificación de eventos, cumpliendo como mínimo con los siguientes requerimientos técnicos: a) Implementar mecanismos para la programación y distribución automática de notificaciones de eventos del sistema e informes a través de correo electrónico, garantizando la entrega oportuna de información relacionada con la operación y seguridad de la plataforma. b) Generar, como mínimo, informes de Detalle de Alertas, Resumen Ejecutivo, Tendencia de Equipos Infectados (Hosts Infectados), Actividad de Malware e Informes de Servidores de Callback, permitiendo el seguimiento y análisis de eventos de seguridad. c) Implementar funcionalidades mediante interfaz de línea de comandos (CLI) que permitan consultar resúmenes de análisis basados en direcciones IP de origen y destino, direcciones URL y valores hash MD5. d) Configurar la interfaz web de administración (Web UI) para permitir la generación, exportación e impresión de informes en formato PDF, con opciones de procesamiento ajustables de acuerdo con los niveles estándar, extendido o intensivo. e) Implementar mecanismos de filtrado para la consulta y análisis de eventos, utilizando criterios como tipo de detección (por ejemplo, Exfiltración de Datos y Beaconing), dirección IP o máscara de red, dominio y país. f) Configurar formatos flexibles de notificación de alertas compatibles, como mínimo, con los estándares CEF, LEEF, CSV, Texto Plano, JSON y XML, permitiendo diferentes niveles de detalle: Normal, Conciso y Extendido. g) Permitir el monitoreo de al menos veinticinco (25) aplicaciones a través de la CLI, utilizando métricas basadas en el número de sesiones o en el volumen de tráfico procesado. h) Actualizar e implementar capacidades de prefiltrado para el análisis de archivos XLS y PDF mediante reglas y scripts YARA, con el fin de fortalecer la detección temprana de amenazas. i) Implementar funcionalidades de monitoreo del estado y rendimiento de la solución, incluyendo información asociada al producto (modelo, nombre, tipo de licencia y estado del licenciamiento) y métricas relacionadas con la carga de procesamiento y desempeño operativo. 1.6. Seguridad y Administración:

ITEM	RENOVACIÓN DE LAS SOLUCIONES.
	El contratista deberá mantener la correcta operación de las funcionalidades de autenticación, autorización, administración y monitoreo de la solución, cumpliendo como mínimo con los siguientes requisitos técnicos: a) Configurar la solución en modo de cumplimiento CC-NDcPP (Common Criteria Protection Profile for Network Devices), garantizando la adopción de controles de seguridad alineados con estándares internacionales para dispositivos de red. b) Permitir la creación, administración y gestión de cuentas de usuario locales mediante la interfaz de línea de comandos (CLI). c) Integrar la solución con servicios de directorio LDAP para la autenticación y autorización centralizada de usuarios. d) Configurar la autenticación basada en SAML, permitiendo que la solución opere como Proveedor de Servicios (Service Provider - SP) y admita la importación de metadatos de proveedores de identidad (IdP) mediante la interfaz web de administración o la CLI. e) Implementar mecanismos de autorización de usuarios basados en atributos de certificados X.509, incluyendo Subject Alternative Name (SAN UPN), Subject Common Name (CN) y el atributo Preferred Username de OpenID Connect (OIDC). f) Soportar certificados digitales en formato PEM, incluidos certificados de autoridades certificadoras (CA) y certificados intermedios, para procesos de autenticación y validación de identidad. g) Configurar parámetros de seguridad para certificados digitales, incluyendo el tamaño mínimo de las claves criptográficas y las versiones soportadas de TLS, con el fin de fortalecer la seguridad de las comunicaciones. h) Disponer de una interfaz web de administración para la consulta, visualización y gestión de certificados digitales. i) Implementar funcionalidades para la gestión y eliminación de cadenas de certificados de autoridades certificadoras (CA) asociadas a servidores web. j) Implementar un esquema de Control de Acceso Basado en Roles (RBAC) con perfiles predefinidos, como mínimo: Administrador, Monitor, Operador, Analista y Auditor, cada uno con privilegios y capacidades diferenciadas. k) Permitir la instalación, activación y administración de licencias mediante la interfaz de línea de comandos (CLI). l) Configurar mecanismos de respaldo local y remoto para la base de datos de configuración, los registros de eventos, los datos detectados y los artefactos generados por la solución. m) Implementar capacidades de monitoreo mediante el protocolo SNMP, incluyendo la recopilación de información operativa y la generación de traps SNMP para eventos críticos y condiciones de alarma. n) Configurar mecanismos de borrado seguro de información en medios de almacenamiento persistente, incluyendo dispositivos basados en arreglos RAID. o) Configurar la comunicación con el sistema de gestión central (CMS) mediante tecnología DTI, soportando esquemas de conectividad por puerto único o doble, con selección automática. p) Implementar mecanismos para la obtención, importación y gestión de claves de host SSH, garantizando procesos de autenticación segura. q) Permitir una configuración flexible de fuentes DTI, incluyendo la incorporación de fuentes personalizadas y parámetros de sobrescritura o anulación de configuración. r) Implementar la descarga e instalación automática de certificados públicos y claves privadas cuando se encuentre habilitada la funcionalidad Helix o equivalente del fabricante. s) Configurar la exportación de eventos y metadatos de Capa 7 hacia plataformas de monitoreo y correlación de eventos de seguridad (SIEM), mediante los protocolos UDP, TCP y HTTPS.
2.	2.1. CARACTERÍSTICAS DE LA RENOVACIÓN DE LA SOLUCIÓN IPS + IVX CLOUD El contratista deberá mantener en correcta operación la solución de Sistema de Prevención de Intrusiones (IPS) y análisis avanzado de amenazas IVX Cloud o equivalente, garantizando el cumplimiento de los siguientes requerimientos mínimos: a) Implementar capacidades avanzadas para la detección, monitoreo y análisis de movimientos laterales dentro de la red corporativa, así como mecanismos de protección específicos para redes de servidores y entornos críticos de la Entidad.

ITEM	RENOVACIÓN DE LAS SOLUCIONES.
	b) Actualizar y configurar la solución de Sistema de Prevención de Intrusiones (IPS) para la protección de la red interna, proporcionando visibilidad sobre movimientos laterales, actividades sospechosas y amenazas avanzadas. Asimismo, deberá integrar capacidades de sandboxing externo que fortalezcan los procesos de detección, análisis y respuesta frente a incidentes de seguridad. c) Actualizar y configurar una solución IPS de última generación, integrada con servicios de análisis avanzado de malware y sandboxing, que permita proteger las redes de servidores con conectividad de hasta 10 Gbps sobre fibra óptica, proporcionando visibilidad integral del tráfico, capacidades de detección avanzada y protección proactiva frente a movimientos laterales no autorizados y amenazas persistentes. La solución deberá soportar y proteger redes de servidores con un tráfico estimado de hasta 4 Gbps por segmento, de acuerdo con las necesidades operativas de la Entidad. d) Configurar la solución conforme a las características técnicas, funcionales, operativas y de seguridad definidas en el presente documento, garantizando su adecuada integración con la infraestructura tecnológica existente y el cumplimiento de los objetivos institucionales de ciberseguridad 2.2. Rendimiento y conectividad del sensor a) Configurar la conexión física directa a dos enlaces de fibra de 10 Gbps para la inspección de tráfico. b) Configurar la protección tanto del datacenter principal como del datacenter alternativo. c) Configurar la conexión física directa a enlaces de fibra de 10 Gbps para la inspección de tráfico en el centro de datos alternativo. d) Configurar un rendimiento agregado de inspección de hasta 5 Gbps, incluyendo la licencia de capacidad correspondiente para soportar dicho caudal de tráfico. e) Configurar la capacidad para manejar hasta 5.000.000 de conexiones concurrentes. f) Configurar la capacidad para procesar hasta 190.000 conexiones por segundo. g) Configurar la capacidad para procesar hasta 120.000 conexiones HTTP por segundo. h) Configurar el procesamiento de tráfico cifrado TLS 1.2 y TLS 1.3, con un rendimiento de hasta 2,46 Gbps. i) Configurar el procesamiento de tráfico cifrado TLS mixto, con un rendimiento de hasta 4 Gbps. j) Configurar puertos fijos 10 GigE/1 GigE SFP+ para conectividad mediante fibra óptica. k) Configurar puertos fijos de cobre Gigabit Ethernet RJ-45, con capacidad de fail-open interno. l) Configurar al menos una ranura para módulos de entrada/salida de red que permita expandir la conectividad Ethernet de 10 Gbps. 2.3. Modos de despliegue y continuidad del servicio a) Configurar el despliegue en modo inline o de prevención, con capacidad de bloqueo activo de amenazas antes de que estas alcancen los sistemas internos. b) Configurar el despliegue en modo TAP o SPAN para monitoreo pasivo, sin afectar el flujo normal del tráfico de red. c) Configurar operación fail-open para asegurar la continuidad ininterrumpida del tráfico de red en caso de fallo del sensor o durante actividades de soporte, utilizando kits de bypass externos activos o pasivos para puertos de fibra. d) Configurar pares de sensores en alta disponibilidad (HA), con capacidad de failover completo y stateful, garantizando la continuidad de la protección incluso ante la falla de uno de los sensores. e) Actualizar y configurar el puerto de gestión dedicado RJ-45 de 1 Gbps. f) Actualizar y configurar el puerto de respuesta dedicado RJ-45 de 1 Gbps, destinado a la inyección de paquetes de respuesta, tales como TCP Resets, cuando la solución opere en modos SPAN o TAP. 2.4. Detección y prevención avanzada de amenazas

ITEM	RENOVACIÓN DE LAS SOLUCIONES.
	a) Configurar capacidades para la detección y prevención de intrusiones, ataques de denegación de servicio (DoS), denegación de servicio distribuido (DDoS) y descargas de malware. b) Configurar análisis profundo de protocolos, incluyendo reensamblaje de fragmentos IP, reconstrucción de flujos TCP y análisis exhaustivo hasta la capa de aplicación (Capa 7 / L7). c) Implementar protección en tiempo real contra descargas de archivos maliciosos, integrada con servicios de inteligencia de amenazas para el análisis de reputación de archivos. d) Implementar análisis dinámico sin firmas, con capacidad para identificar ataques de día cero (Zero-Day), malware multiflujo y técnicas evasivas, mediante un entorno virtual seguro tipo sandboxing, integrado con un servicio de análisis avanzado de malware. e) Configurar la detección de actividad asociada a servidores de Comando y Control (C&C/C2), incluyendo técnicas avanzadas basadas en DNS, tales como Fast-Flux Service Network (FFSN) y Domain Generation Algorithm (DGA). f) Activar el bloqueo de tráfico cuando se detecten firmas de alta confianza, utilizando adicionalmente la reputación de IP y puertos proporcionada por los servicios de inteligencia del fabricante, con el fin de apoyar la toma de decisiones de bloqueo y minimizar falsos positivos. g) Configurar la funcionalidad de normalización de tráfico (Traffic Normalization o Packet Scrubbing) en modo inline, con el fin de eliminar ambigüedades en los protocolos, descartar paquetes mal formados o ilegales, mitigar intentos de evasión y mejorar la precisión de la detección. h) Configurar capacidades Anti-Spoofing en modo inline, permitiendo descartar paquetes con direcciones IP de origen inválidas mediante su comparación con una lista configurada de redes internas. i) Configurar protección granular contra ataques DoS a nivel de host individual, manteniendo perfiles DoS independientes por interfaz y subinterfaz, con soporte para hasta 5.000 perfiles DoS. j) Configurar soporte para protección SYN Cookie, orientada a la mitigación de ataques de inundación SYN.
	2.5. Visibilidad y protección de movimientos laterales / redes de servidores. a) Configurar virtualización de puertos de monitoreo (VIPS/VIDS) y subinterfaces, con el fin de aplicar políticas de seguridad específicas y granulares a distintos grupos de tráfico dentro de un mismo puerto físico del sensor. b) Definir la segmentación del tráfico para la aplicación de políticas basadas en VLAN ID y bloques CIDR, con el propósito de proteger subredes de servidores y aislar movimientos laterales. c) Configurar la capacidad de aplicar políticas de seguridad personalizadas a nivel de dominios administrativos, interfaces y subinterfaces, permitiendo una adaptación precisa a los entornos de servidores, tales como servidores web, servidores de correo o segmentos internos. d) Integrar la consola de antimalware para el perfilamiento pasivo de dispositivos, permitiendo identificar el tipo de dispositivo y el sistema operativo de los hosts, con el fin de mejorar la relevancia de las alertas y la aplicación de políticas contextuales. e) Configurar la capacidad de exportar datos NetFlow hacia appliances o plataformas de análisis de comportamiento de amenazas, con el propósito de facilitar la detección de anomalías en la red. f) Definir e implementar reglas de Calidad de Servicio (QoS) que permitan garantizar el ancho de banda requerido para las aplicaciones críticas del negocio. g) Configurar la capacidad de restringir el acceso SSH al sensor únicamente a rangos de red o direcciones IP específicas, tanto IPv4 como IPv6, fortaleciendo la seguridad de la administración. h) Gestionar hasta 1.000 sistemas IPS virtuales. i) Gestionar hasta 254 etiquetas VLAN por interfaz. 2.6. Gestión centralizada y capacidades operacionales a) Configurar la consola de administración con una interfaz gráfica web (GUI) intuitiva, que permita la configuración, gestión, monitoreo de estado, generación de informes y administración de alertas en un entorno centralizado.

ITEM	RENOVACIÓN DE LAS SOLUCIONES.
	b) Configurar la gestión centralizada de licencias de capacidad y funcionalidades avanzadas, incluyendo sensores virtuales. c) Configurar la capacidad para asignar y administrar licencias a los sensores de forma eficiente a través de la consola de gestión. d) Implementar visibilidad detallada del rendimiento del sensor, incluyendo uso de throughput del dispositivo y de los puertos, consumo de memoria y utilización de CPU, a través de la consola de gestión. e) Configurar la actualización centralizada y programada de firmas y software del IPS. f) Garantizar que la comunicación entre el Manager y los sensores sea segura, con soporte mínimo para TLS 1.2. g) Configurar la gestión de dominios administrativos para permitir una organización jerárquica de recursos y la delegación de privilegios de administración. h) Configurar funcionalidades robustas de registro y análisis de eventos, incluyendo Attack Log, Threat Explorer, análisis de archivos de malware, actividades de callback, hosts de alto riesgo y una vista detallada de ataques basada en MITRE ATT&CK™. i) Configurar la capacidad de exportar logs de eventos para su integración con sistemas SIEM. j) Configurar la gestión de hasta 400.000 entradas de hashes de archivos, permitidos y bloqueados, para procesos de reputación de archivos. k) Actualizar la plataforma Manager instalada.
	2.7. Capacidades de análisis y detección de amenazas a) Configurar los dispositivos de seguridad de red, tales como IPS o soluciones de análisis avanzado de malware con sandboxing, para extraer objetos y URL del tráfico de red monitoreado, con el fin de someterlos a inspección y análisis. b) Integrar funcionalidades de sandboxing mediante el uso de imágenes de sistemas operativos de diferentes versiones de Windows y Linux, permitiendo la detonación segura y el análisis de comportamiento de amenazas en un entorno controlado y aislado. c) Aplicar reglas YARA personalizadas y predefinidas para la identificación de patrones, firmas y características asociadas a malware conocido, desconocido y de día cero, fortaleciendo la detección de amenazas avanzadas. d) Actualizar las herramientas de análisis estático para realizar inspección profunda de archivos y ejecutables, permitiendo identificar posibles amenazas sin requerir su ejecución dinámica. e) Configurar capacidades de detección equivalentes a las esperadas en un dispositivo físico de seguridad, delegando la complejidad del análisis avanzado de amenazas al servicio en la nube. f) Proveer un servicio alojado en una nube pública que reciba las submisiones enviadas por los sensores para su análisis. g) Recibir las submisiones enviadas por los sensores, realizar un análisis exhaustivo y remitir un veredicto de seguridad como resultado del análisis hacia los sensores correspondientes. h) Configurar los sensores para generar alertas de seguridad con base en el veredicto recibido desde el servicio en la nube. i) Implementar en los sensores la capacidad de generar alertas de seguridad basadas en el veredicto de análisis avanzado recibido desde el clúster IVX en la nube o servicio equivalente.
	2.8. Compatibilidad y modo de operación a) Configurar e implementar que los dispositivos físicos de seguridad de red funcionen como sensores mediante la integración con el servicio en la nube, permitiendo el envío de submisiones al servicio de análisis avanzado de malware. b) Configurar la habilitación del modo de sensor en la nube en los dispositivos de seguridad de red integrados, tanto desde la interfaz web de gestión como desde la interfaz de línea de comandos (CLI) del dispositivo.
	2.9. Conectividad y comunicación con la nube

ITEM	RENOVACIÓN DE LAS SOLUCIONES.
	a) Configurar una conexión segura y bidireccional con la red de inteligencia del fabricante, a través de la interfaz de gestión y mediante HTTPS por el puerto 443, para acceder a servicios esenciales como inteligencia de amenazas, licenciamiento, registro y actualizaciones de software. b) Configurar una comunicación segura entre los sensores y el broker en la nube, a través de la interfaz de submisión del dispositivo físico, utilizando SSH sobre SSL por el puerto 443, para el envío de objetos y la recepción de resultados de análisis. c) Configurar una interfaz de gestión dedicada para el tráfico de submisión, recomendando la separación entre el tráfico de gestión y el tráfico de datos mediante el uso de una interfaz de administración y una interfaz independiente para submisiones. d) Configurar una puerta de enlace predeterminada para la interfaz de submisión cuando los sensores y el servicio en la nube se encuentren en subredes diferentes. 2.10. Gestión y monitoreo de sensores a) Configurar la gestión centralizada de los sensores, agregando las alertas generadas por todos ellos y presentándolas en una única interfaz de administración. b) Monitorear de forma continua el estado de conexión y registro de los sensores con el servicio en la nube. c) Generar notificaciones por correo electrónico y mostrar advertencias visibles en el panel de control (Dashboard) de la solución IPS, así como en la salida de comandos de la CLI, en caso de fallos de conexión o registro. d) Implementar la capacidad de configurar notificaciones de alerta estándar desde la solución IPS. e) Configurar el envío de SNMP Traps para comunicar condiciones anómalas, incluyendo fallos de registro MVX, detección de dispositivos duplicados y problemas de conectividad con el servidor de tokens de la solución. f) Configurar notificaciones de eventos por correo electrónico relacionadas con el registro y las licencias, con capacidad para definir niveles de notificación, tales como falla o informativo. g) Configurar la visualización y filtrado de archivos de registro locales desde la interfaz web de la plataforma IPS o desde la CLI, permitiendo la búsqueda de mensajes específicos relacionados con la conexión al servicio en la nube. h) Configurar el envío de mensajes de registro hacia servidores syslog remotos, con opciones para definir formato, nivel de detalle, frecuencia y severidad del evento. i) Configurar la capacidad de restaurar automáticamente la configuración de registro del sensor en caso de que esta sea deshabilitada por cualquier motivo.
3.	CARACTERÍSTICAS DE LA RENOVACIÓN DE SOLUCIONES ENDPOINT- MDR El contratista deberá garantizar la operación de una solución integral de Protección de Endpoints (EPP), Detección y Respuesta de Endpoints (EDR) y Detección y Respuesta Gestionada (MDR), que permita fortalecer la postura de ciberseguridad de la Entidad mediante capacidades avanzadas de prevención, detección, investigación, contención y respuesta ante amenazas. La solución deberá cumplir, como mínimo, con los siguientes requisitos técnicos: 3.1. Capacidades generales de la solución a) La solución deberá proporcionar protección integral para los endpoints de la Entidad, garantizando visibilidad continua sobre amenazas, actividades sospechosas e incidentes de seguridad. b) Integrar en una única plataforma las capacidades de Protección de Endpoints (EPP), Detección y Respuesta de Endpoints (EDR) y funcionalidades forenses avanzadas. c) Disponer de administración centralizada mediante una plataforma On-Premise, SaaS o híbrida, utilizando un único agente para la gestión de todas las funcionalidades requeridas en un entorno de aproximadamente 1.300 dispositivos.

ITEM	RENOVACIÓN DE LAS SOLUCIONES.
	d) Implementar capacidades de adquisición y análisis de archivos, datos y colecciones de triage desde los endpoints, permitiendo validar alertas, realizar investigaciones y ejecutar acciones de contención sobre dispositivos comprometidos. 3.2. Protección avanzada contra amenazas a) Proporcionar protección contra malware mediante técnicas basadas en firmas, análisis heurístico y mecanismos avanzados de detección. b) Implementar integración con la interfaz AMSI (Antimalware Scan Interface) para monitorear, detectar y bloquear scripts maliciosos o sospechosos, generando alertas cuando se identifiquen eventos de riesgo. c) Permitir la comparación de scripts mediante reglas YARA obtenidas desde la plataforma de inteligencia de amenazas del fabricante. d) Implementar listas de bloqueo (Deny List) con capacidad para alertar, bloquear o poner en cuarentena archivos mediante hashes MD5, SHA-1 y SHA-256, rutas de archivos o información de inteligencia proveniente de fuentes externas. e) Incorporar motores avanzados de análisis de contenido capaces de contener, bloquear o remediar archivos según su reputación, reglas definidas o umbrales de riesgo configurables. f) Proporcionar servicios de intercambio bidireccional de información de archivos y amenazas en tiempo real, tanto en modalidades On-Premise como en la nube. g) Incorporar mecanismos de detección basados en Machine Learning (ML) en el agente de seguridad, permitiendo configurar diferentes niveles de sensibilidad para la identificación de malware conocido y desconocido. a) Integrar capacidades de Inteligencia Artificial Generativa (IA Generativa) para fortalecer las funcionalidades EDR, facilitar el análisis contextual de eventos y optimizar la toma de decisiones basada en datos. b) Permitir el aislamiento o cuarentena de dispositivos Windows y macOS, incluyendo la personalización de mensajes informativos mostrados a los usuarios. 3.3. Visibilidad, búsqueda e investigación a) Proporcionar capacidades avanzadas de búsqueda en tiempo real y retrospectiva sobre todos los endpoints protegidos, con el fin de apoyar actividades de investigación y caza de amenazas. b) Permitir búsquedas sobre atributos como procesos, aplicaciones, hashes, rutas de archivos, direcciones IP, eventos del sistema y registros de seguridad en entornos Windows, macOS y Linux. c) Permitir la importación masiva de Indicadores de Compromiso (IOC) en formatos de texto o CSV, soportando como mínimo 10.000 indicadores por archivo. d) Incorporar funcionalidades de IA Generativa en módulos de monitoreo, búsqueda de dispositivos e investigación histórica, mediante modos de análisis interactivo y generación de dossiers. e) Permitir la creación de investigaciones avanzadas que consoliden evidencias relacionadas con amenazas, incluyendo procesos, conexiones de red, archivos, llamadas API y líneas de comandos. f) Permitir la creación de colectores personalizados para la recopilación de información específica desde los endpoints, con soporte para scripts y contenidos desarrollados en Python u otros intérpretes compatibles. g) Generar representaciones gráficas del ciclo de ataque y la evolución de amenazas avanzadas, incluyendo información contextual sobre reputación, procesos y activos afectados. h) Incorporar ayuda contextual dentro de la interfaz de administración. i) Permitir la exportación e impresión de investigaciones y análisis detallados en formato PDF. 3.4. Detección avanzada basada en IA y Machine Learning a) Detectar y bloquear amenazas avanzadas, incluyendo malware de día cero, exploits y ataques realizados mediante PowerShell, JavaScript, VBScript u otros motores de scripting.

ITEM	RENOVACIÓN DE LAS SOLUCIONES.
	b) Incorporar motores de investigación asistidos por IA capaces de correlacionar eventos, contextualizar alertas y reducir falsos positivos utilizando inteligencia propia y de terceros. c) Permitir el envío automático de archivos sospechosos a servicios de sandboxing del mismo fabricante, ya sea en modalidad On-Premise o Cloud, para ampliar la capacidad de análisis. d) Integrar servicios de reputación y enriquecimiento de amenazas que permitan consultar información detallada y reportes asociados a eventos de seguridad. 3.5. Gestión y administración a) Permitir la creación de excepciones basadas en atributos específicos de dispositivos, fabricantes, productos o números de serie. b) Gestionar políticas de seguridad desde una consola centralizada única. c) Administrar los registros de la solución, incluyendo personalización, generación y descarga de logs para actividades de diagnóstico y soporte. d) Implementar mecanismos de autoprotección que impidan la alteración, desactivación o eliminación de componentes críticos de la solución. e) Permitir la protección de la interfaz de usuario mediante autenticación adicional o contraseña para evitar modificaciones no autorizadas. f) Mantener comunicación segura con los servicios de inteligencia del fabricante para procesos de licenciamiento, actualización de agentes, descarga de contenido IOC y servicios asociados, soportando IPv4 e IPv6. g) Permitir la creación de reglas personalizadas para la protección de procesos, archivos, servicios y registros del sistema, así como para la mitigación de ataques de explotación y uso indebido de APIs. h) Permitir la migración, exportación e importación de políticas y configuraciones entre entornos On-Premise, Cloud e híbridos. 3.6. Escalabilidad y compatibilidad a) Soportar arquitecturas On-Premise, Cloud e híbridas con capacidad de crecimiento de acuerdo con las necesidades de la Entidad. b) Permitir la configuración del número máximo de resultados devueltos por búsquedas en tiempo real, en rangos configurables. c) Garantizar compatibilidad con sistemas operativos Windows, macOS y Linux, incluyendo versiones heredadas o de soporte extendido requeridas por la Entidad. 3.7. Servicio de Detección y Respuesta Gestionada (MDR) a) Proporcionar monitoreo continuo 24x7x365 sobre la plataforma de seguridad implementada. b) Contar con capacidades de detección y análisis de amenazas soportadas por especialistas en ciberseguridad e inteligencia de amenazas. c) Analizar telemetría avanzada de endpoint para identificar actividades maliciosas que puedan evadir los mecanismos tradicionales de protección. d) Proporcionar recomendaciones para la optimización de políticas y mejora continua de la postura de seguridad. e) Incorporar servicios de inteligencia de amenazas para anticipar riesgos emergentes y priorizar actividades de remediación. f) Utilizar capacidades de Inteligencia Artificial para acelerar la investigación y correlación de alertas. g) Identificar amenazas basadas en archivos, amenazas sin archivos (Fileless) y mapear automáticamente técnicas asociadas al marco MITRE ATT&CK™. h) Realizar evaluaciones periódicas de configuración y estado de los endpoints protegidos. i) Administrar y optimizar todos los motores de seguridad disponibles en la solución. 3.8. Notificación y gestión de incidentes a) Garantizar tiempos de notificación conforme a los siguientes niveles mínimos de servicio (SLA): • Crítico: menos de 1 hora. • Alto: menos de 2 horas.

ITEM	RENOVACIÓN DE LAS SOLUCIONES.
	• Medio: menos de 24 horas. b) Definir planes de escalamiento adaptados a la estructura organizacional de la Entidad. c) Implementar procedimientos formales de escalamiento para incidentes críticos, altos y medios, utilizando múltiples canales de comunicación. d) Entregar reportes de incidentes con hallazgos, acciones ejecutadas y recomendaciones de mejora. e) Notificar de forma proactiva sobre campañas activas, brechas identificadas y amenazas emergentes detectadas por el fabricante. 3.9. Apoyo en respuesta a incidentes a) Proporcionar servicios de respuesta coordinada ante incidentes, incluyendo acciones de contención y remediación previamente acordadas con la Entidad. b) Ejecutar acciones de contención como aislamiento de equipos, cuarentena de archivos y control dinámico de aplicaciones. c) Permitir la personalización de las acciones de respuesta de acuerdo con el nivel de criticidad de los activos y la tolerancia al riesgo de la Entidad. d) Realizar análisis de causa raíz e investigaciones de incidentes utilizando información de EDR y fuentes complementarias. e) Facilitar la transición entre actividades de detección, triage e investigaciones formales de respuesta a incidentes. f) Mantener capacidades de retención y análisis forense para apoyar investigaciones posteriores. g) Proporcionar recomendaciones especializadas para fortalecer la postura de seguridad tras cada incidente. 3.10 Equipo especializado y soporte a) Garantizar la operación del servicio mediante un equipo de expertos disponible 24x7x365. b) Apoyar de manera continua la mejora de la postura de seguridad, la optimización de controles y la reducción de la carga operativa del personal de la Entidad. c) Garantizar compatibilidad con entornos cloud públicos, privados e híbridos. d) Entregar informes mensuales de gestión durante la vigencia de la renovación de la garantía y brindar soporte para actividades de cumplimiento normativo y auditoría de seguridad. e) El oferente deberá presentar con su propuesta un documento en el que relacione el perfil de los ingenieros que prestarán los servicios, dichos recursos deben pertenecer al fabricante de la solución ofertada o a un tercero autorizado por este.
4.	EL CONTRATISTA DEBE PRESTAR LOS SIGUIENTES SERVICIOS DE SOPORTE:
4.1.	El proponente deberá prestar el servicio mediante cinco (5) profesionales en ingeniería o tecnología, sin que ello genere para la entidad contratante vínculo laboral alguno, con el fin de garantizar la vigencia de la garantía del fabricante y la prestación del soporte técnico durante el tiempo requerido para el licenciamiento contratado. Se deben adjuntar con la presentación de la propuesta todos los documentos solicitados al equipo de profesionales. (hoja de vida, experiencia, certificaciones etc.) Un (1) profesional en ingeniería en áreas de sistemas, electrónica, eléctrica, telecomunicaciones, ingeniería industrial, telemática o afines, el cual deberá contar con las siguientes condiciones mínimas: - Experiencia mínima como gerente y/o consultor en tres (3) proyectos de seguridad de la información y/o seguridad informática. - El personal asignado deberá contar con las siguientes certificaciones y formación académica: - Especialización en gerencia de proyectos - Project Management Professional - PMP (Vigente) - Scrum Fundamentals Certified Un (1) profesional en ingeniería en áreas de sistemas, electrónica, eléctrica, telecomunicaciones, ingeniería industrial, telemática o afines, el cual deberá contar con las siguientes condiciones mínimas:

ITEM	RENOVACIÓN DE LAS SOLUCIONES.
	- Experiencia en mínimo 3 proyectos como líder técnico en los productos de seguridad solicitados en las especificaciones técnicas. - El personal asignado deberá contar con las siguientes certificaciones y formación académica: - Especialista en Seguridad Informática - ISO 27001 versión 2013 - CISM (Vigente) - Certified Ethical Hacker (CEH) Un (1) profesional en ingeniería en áreas de sistemas, electrónica, eléctrica, telecomunicaciones, ingeniería industrial, telemática o afines, el cual deberá contar con las siguientes condiciones mínimas: - Experiencia mínimo 2 certificaciones de experiencia en mínimo 2 entidades en donde haya realizado, soportado consecutivamente durante 5 años esta labor de análisis de vulnerabilidades. - El personal asignado deberá contar con las siguientes certificaciones y formación académica: - Especialización en seguridad informática - ISO/IEC 27001 - InsightAppSec Certified Administrator Un (1) profesional en ingeniería o tecnólogo en áreas de sistemas, electrónica, eléctrica, telecomunicaciones, ingeniería industrial, telemática o afines, el cual deberá contar con las siguientes condiciones mínimas: - Experiencia mínima de tres (3) años en actividades relacionadas con soporte y administración de plataformas tecnológicas Trellix. - Soporte técnico en sitio, el contratista deberá disponer de un (01) ingeniero que deberá estar en sitio en las instalaciones de la Entidad sede principal (ciudad de Bogotá) dos días a la semana (lunes y jueves) cuando exista algún día festivo este se deberá reponer por otro día de común acuerdo con el supervisor del contrato, durante la vigencia de la renovación del licenciamiento adquirido por la Entidad, para la revisión del estado de las consolas, ajustes, afinamientos y reportes que le sean solicitados a través del supervisor del contrato. - El personal asignado deberá contar con certificación vigente: - Endpoint Security Technical Specialist (Vigente) - ePolicy Orchestrator (ePO) SaaS Technical Professional (Vigente) - Endpoint Detection and Response Administration (Vigente) Un (1) profesional en ingeniería o tecnólogo en áreas de sistemas, electrónica, eléctrica, telecomunicaciones, ingeniería industrial, telemática o afines, el cual deberá contar con las siguientes condiciones mínimas: - Experiencia mínima de tres (3) años en actividades relacionadas con soporte y administración de plataformas tecnológicas Trellix. - El personal asignado deberá contar con certificación vigente: - Data Security Technical Specialist(Vigente) - Intrusion Prevention System (IPS) Technical Professional (Vigente) Para los efectos de este proceso de selección se entiende como: NOTA 1: Los documentos que acrediten la experiencia profesional y específica de obligatorio cumplimiento del equipo de trabajo, son los siguientes: 1. Hoja de vida 2. Fotocopia de la cédula de ciudadanía 3. Fotocopia del diploma o acta de grado otorgado por una Institución Educativa oficialmente reconocida. 4. Fotocopia de la tarjeta profesional vigente 5. Certificación vigente expedida por el Consejo Profesional respectivo, cuando aplique. 6. Certificaciones laborales que deben indicar: • Razón Social o nombre de la entidad o empresa, dirección y número de contacto. • Nombres, apellidos e identificación respecto de la persona certificada.

ITEM	RENOVACIÓN DE LAS SOLUCIONES.
	• Cargo y funciones desempeñadas u objeto y obligaciones del contrato, debidamente especificados. • Fecha de inicio de labores o del contrato (día, mes y año) • Fecha de terminación de labores o del contrato o plazo de ejecución (día, mes y año) Para los efectos de este proceso de selección se entiende como: Experiencia profesional: Se cuenta a partir de la fecha de expedición de la matrícula profesional, para el caso de ingenieros en virtud del artículo 6º de la Ley 842 de 2003. Requisitos para ejercer la profesión. Para poder ejercer legalmente la Ingeniería, sus profesiones afines o sus profesiones auxiliares en el territorio nacional, en las ramas o especialidades regidas por la presente ley, se requiere estar matriculado o inscrito en el Registro Profesional respectivo, que seguirá llevando el COPNIA, lo cual se acreditará con la presentación de la tarjeta o documento adoptado por este para tal fin El artículo 12 de la Ley 842 de 2003, EXPERIENCIA PROFESIONAL. Para los efectos del ejercicio de la ingeniería o de alguna de sus profesiones afines o auxiliares, la experiencia profesional solo se computará a partir de la fecha de expedición de la matrícula profesional o del certificado de inscripción profesional, respectivamente. Todas las matrículas profesionales, certificadas de inscripción profesional y certificados de matrícula otorgados con anterioridad a la vigencia de la presente ley conservan su validez y se presumen auténticas. NOTA 2: Para el cómputo de la experiencia no se tendrá en cuenta la experiencia simultánea del profesional que se traslape temporalmente frente a actividades específicas referidas, la cual solo se agregará una vez dentro de la suma de experiencia de cada integrante. Para el caso de personas que hayan obtenido su título profesional en ingeniería y la experiencia en el extranjero, dicha experiencia profesional se contabilizará a partir de la obtención del título. NOTA 3: Si el proponente es quien certifica al equipo de trabajo, deberá aportar copia del contrato suscrito entre el proponente y el profesional correspondiente, en el cual consigne la identificación del contrato entre el proponente y el cliente final, que respalde dicha experiencia, registrada en el RUP; en caso de no existir contrato suscrito, deberá allegar certificación de la Junta Directiva o Junta de Socios (la que corresponda) con el visto bueno del Revisor Fiscal o Contador (en caso de no existir Revisor Fiscal), para certificar la experiencia del profesional propuesto. Las certificaciones emitidas por el mismo personal propuesto, es decir, la auto certificación, no serán tenida cuenta. NOTA 4: La Experiencia Profesional se contará a partir de la terminación de materias de acuerdo con lo señalado en el artículo 229 del Decreto Ley 019 de 2012, excepto para el caso de los ingenieros que conforme con lo establecido en el artículo 12 de la Ley 842 del 14 de octubre de 2003, la experiencia profesional de los ingenieros o alguna de sus profesiones afines o auxiliares, solo se contará a partir de la fecha de expedición de la matrícula profesional; si el título fue obtenido antes de la expedición de la Ley 842 de 2003, la experiencia se contará a partir del título profesional. En todo caso la experiencia deberá acreditarse siempre en los términos establecidos en el presente documento. En el evento en que algún miembro del equipo de trabajo presente título obtenido en el exterior de pregrado o postgrado, deberá aportar el acto administrativo por el cual se convalida dicho título en nuestro país, ante el Ministerio de Educación Nacional de Colombia, para que sea tenido en cuenta, y de conformidad con los requerimientos establecidos por las resoluciones vigentes y aplicables expedidas por dicho Ministerio, para su regulación, en el momento de la convalidación. Las convalidaciones que estén en curso ante el Ministerio de Educación Nacional no servirán para acreditar los títulos académicos. Conforme a lo señalado en la Guía Práctica para la Convalidación de Títulos Profesionales en Colombia, publicada en la página web del Ministerio de Educación Nacional, "la existencia de convenios internacionales no exonera al interesado del trámite correspondiente." NOTA 5: El proponente que presente dentro de su equipo de trabajo profesionales extranjeros, con su oferta deberá aportar el permiso de trabajo que trata el artículo 23 de

ITEM	RENOVACIÓN DE LAS SOLUCIONES.
	la Ley 842 de 2003, y en todo caso el permiso deberá estar otorgado para ejercer cualquiera de los programas en ingeniería objeto de la habilitación. El proponente para la presentación de su equipo de trabajo deberá dar estricto cumplimiento a lo exigido en el artículo 22 de la Ley 842 de 2003, "(...) la participación de los profesionales extranjeros no podrá ser superior a un veinte por ciento (20%) de su personal de ingenieros o profesionales auxiliares o afines colombianos (...)". NOTA 6: Las certificaciones deberán establecer la fecha de inicio y finalización, en caso de no diligenciarse o no encontrarse en los documentos aportados las fechas de inicio, terminación del contrato con día, mes y año y la certificación se emita únicamente nombrando los meses, La UNIDAD tomará el último día de cada mes como fecha de inicio y el primer día de cada mes como fecha de terminación; cuando la certificación se expida mencionado únicamente los años, se aplicará la regla anterior al último mes del año como mes de inicio y el primer mes del año como mes de finalización. NOTA 7: La UNIDAD podrá verificar los soportes de hoja de vida de los miembros del equipo y toda la documentación aportada de cada proponente con el fin de corroborar su veracidad. NOTA 8: Las experiencias reportadas podrán estar vigentes, caso en el cual se contabilizarán hasta la fecha de expedición de la certificación. NOTA 9: Cada profesional propuesto deberá ser postulado SOLO para un cargo, so pena de ser calificada la oferta como no cumple. NOTA 10: No se aceptará que más de un oferente presente la misma hoja de vida dentro del equipo de trabajo propuesto. NOTA 11: No se aceptarán certificaciones expedidas por quienes hayan sido socios o integrantes de empresas que están canceladas o extintas a la vida jurídica. NOTA 12: Si la empresa está en liquidación se aceptarán certificaciones expedidas por el agente liquidador y en tal caso, se requiere que el proponente allegue copia del certificado de existencia y representación legal de la cámara de comercio de la empresa en liquidación, en la que se pueda verificar la identidad del agente liquidador. Las certificaciones de experiencia se consideran expedidas bajo la gravedad del juramento. La UNIDAD se reserva el derecho de verificar durante la evaluación y hasta la adjudicación la información aportada por el proponente y solicitar los soportes que considere convenientes tales como: copias de los contratos, actas de liquidación, estados financieros, copia de pago de impuestos etc., sin que por ello el proponente esté facultado para complementar, adicionar o mejorar su propuesta.
4.2.	El contratista deberá prestar a la Unidad Administrativa Especial de la Justicia Penal Militar y Policial los servicios de soporte, administración, mantenimiento, actualización y optimización de las soluciones TRELIX objeto del contrato, incluyendo, sin costo adicional para la Entidad, las siguientes actividades y prestaciones: a) Realizar la configuración, administración, respaldo y soporte inmediato ante incidentes o fallas de las soluciones implementadas, así como la instalación, actualización y aplicación de parches, prestación de soporte preventivo y correctivo, y la generación de informes, métricas y analíticas de desempeño, disponibilidad y capacidad de la infraestructura monitoreada. b) Prestar los servicios de diagnóstico, análisis y solución de incidentes, problemas y fallas operativas, con el propósito de optimizar el desempeño, disponibilidad y rendimiento de los servicios y componentes que operan sobre la plataforma TRELIX. c) Realizar visitas de soporte y mantenimiento correctivo de manera ilimitada, cuando el supervisor lo requiera durante la renovación del licenciamiento de la solución. d) Actualizar los productos instalados en las consolas de administración, servidores, appliances físicos o virtuales, plataformas on-premise y servicios en la nube de LA UNIDAD o del fabricante, según corresponda. Soporte técnico y afinamiento especializado

ITEM	RENOVACIÓN DE LAS SOLUCIONES.
	El contratista deberá prestar los servicios de soporte técnico y afinamiento de la solución bajo las siguientes condiciones: a) La consola principal de administración de LA UNIDAD se encuentra ubicada en Bogotá D.C.; sin embargo, su ubicación podrá ser trasladada a otra sede dentro de la ciudad o sus municipios aledaños. b) El soporte para los equipos ubicados en Bogotá D.C. deberá prestarse de manera presencial cuando sea requerido por la Entidad. Para los equipos ubicados fuera de Bogotá D.C., el servicio podrá prestarse mediante acceso remoto, siempre que exista conectividad a Internet o cualquier otro mecanismo de acceso suministrado por la Entidad. c) El contratista deberá configurar, verificar y optimizar los servicios instalados en los equipos de cómputo que cuenten con funcionalidades de antimalware, prevención de intrusiones, detección de ataques y análisis de comportamientos sospechosos. Lo anterior incluye la validación de la comunicación entre agentes y consola, la instalación de las versiones más recientes soportadas por el fabricante, la verificación de actualizaciones, la ejecución de análisis, la atención de incidentes reportados por los usuarios y la validación permanente del correcto funcionamiento, compatibilidad y rendimiento de los productos. d) Instalar, activar, configurar y poner en funcionamiento las licencias adquiridas, renovadas o actualizadas en los servidores, estaciones de trabajo y demás activos tecnológicos de LA UNIDAD a nivel nacional. e) Instalar, configurar y optimizar todos los productos de software renovados y sus componentes asociados, garantizando el aprovechamiento integral de las funcionalidades contratadas en servidores, segmentos de red, estaciones de trabajo, equipos portátiles y demás sistemas tecnológicos. Asimismo, deberá actualizar los sistemas operativos y componentes de software a versiones soportadas y certificadas por el fabricante, e implementar las herramientas de gestión necesarias para la administración centralizada de la solución. f) Garantizar la compatibilidad de la solución con la infraestructura tecnológica existente, evitando afectaciones en el desempeño de estaciones de trabajo, servidores, aplicaciones, bases de datos y componentes de red. En caso de presentarse incompatibilidades o degradación del servicio, el contratista deberá ejecutar las pruebas, ajustes y actividades de soporte necesarias para su corrección. g) Suministrar periódicamente a la Oficina de Tecnologías de la Información y las Comunicaciones información relacionada con nuevas amenazas, malware, actividades maliciosas, intentos de intrusión y comportamientos sospechosos, incluyendo recomendaciones, medidas preventivas y acciones de mitigación. h) Entregar en formato digital los manuales técnicos, guías de administración, documentación de usuario y cualquier otro material oficial emitido por el fabricante, en su versión más reciente disponible y en idioma español o inglés. i) Ejecutar las actividades de renovación, instalación, actualización y afinamiento de las licencias y componentes de la solución, verificando permanentemente su correcto funcionamiento. Asimismo, deberá revisar y apoyar la desinfección de equipos que presenten incidentes de malware, intrusiones o comportamientos sospechosos, y formular recomendaciones relacionadas con parches de seguridad, endurecimiento de plataformas y mejores prácticas de protección. j) Cuando sea requerido por la Entidad, el Contratista deberá prestar soporte en sitio sobre estaciones de trabajo, servidores, consolas de administración, appliances físicos o virtuales y demás componentes de la solución. Para usuarios ubicados fuera de Bogotá D.C., el soporte se prestará de manera remota o presencial cuando la situación técnica así lo amerite. k) Disponer de los recursos humanos, técnicos y tecnológicos necesarios para atender incidentes relacionados con malware, intrusiones, ataques informáticos, spyware, spam, comportamientos sospechosos o cualquier otra amenaza que afecte la solución implementada, hasta lograr el restablecimiento completo del servicio. l) Incluir dentro del soporte especializado actividades de instalación de releases, actualizaciones, parches, fixes, bloqueos de puertos, corrección de errores, optimización de configuraciones y actualización de firmas y motores de protección necesarios para mantener la solución protegida frente a amenazas emergentes. Servicios complementarios

ITEM	RENOVACIÓN DE LAS SOLUCIONES.

ITEM	RENOVACIÓN DE LAS SOLUCIONES.
	asistencia de cada una de las personas que participen de la misma. Se debe incluir material y laboratorios.
4.5.	ASPECTOS DE CONFIDENCIALIDAD, INTEGRIDAD Y SEGURIDAD DE LA INFORMACIÓN INSTITUCIONAL El contratista adjudicatario deberá considerar como información confidencial y de propiedad exclusiva de la Unidad Administrativa Especial de la Justicia Penal Militar y Policial toda la información relacionada con el diseño, configuración, implementación, pruebas, resultados, políticas, procedimientos, arquitecturas, documentación técnica y procesos asociados a la actualización, administración y soporte de la solución, así como de todos los productos y servicios objeto del contrato. En consecuencia, el contratista deberá adoptar y mantener las medidas técnicas, administrativas, operativas y de seguridad necesarias para garantizar la confidencialidad, integridad y disponibilidad de dicha información, evitando su copia, reproducción, sustracción, divulgación, modificación, alteración, ocultamiento, pérdida, uso indebido o acceso por parte de terceros no autorizados. Asimismo, durante las actividades de diseño, implementación, actualización, pruebas, soporte, mantenimiento y administración de la solución y de los productos suministrados, el contratista se obliga a utilizar la información, herramientas, credenciales, accesos y recursos tecnológicos únicamente para el cumplimiento del objeto contractual, absteniéndose de realizar cualquier uso indebido de los mismos. De igual forma, el contratista no podrá copiar, reproducir, almacenar, extraer, transferir, divulgar, modificar o utilizar para fines distintos a los establecidos en el contrato la información a la que tenga acceso con ocasión de la ejecución de sus obligaciones, salvo autorización previa y expresa de la Unidad o por requerimiento de autoridad competente. El deber de confidencialidad se mantendrá durante la ejecución del contrato y con posterioridad a su terminación, por el término establecido en la normatividad aplicable o mientras la información conserve su carácter reservado o confidencial.
4.6.	GARANTIA El proponente adjudicatario deberá garantizar que la calidad técnica de los bienes y servicios suministrados en el marco del contrato, incluyendo hardware, software, licenciamiento, configuraciones, implementaciones y servicios administrados, cumpla plenamente con las especificaciones técnicas definidas por el fabricante y con los requerimientos funcionales y operativos de la Unidad Administrativa Especial de la Justicia Penal Militar y Policial. Asimismo, el contratista deberá garantizar la actualización permanente de las soluciones suministradas durante la vigencia del licenciamiento, incluyendo la instalación, configuración y puesta en operación de nuevas versiones, mejoras funcionales, actualizaciones de seguridad, correcciones de errores (bug fixes), parches y demás componentes liberados oficialmente por el fabricante. Las actualizaciones deberán implementarse en todos los componentes de la solución, incluyendo consolas de administración, servidores, appliances, servicios en la nube, estaciones de trabajo, dispositivos finales y capas de seguridad perimetral de la red, previa realización de pruebas controladas que validen su compatibilidad, estabilidad y correcto funcionamiento dentro de la infraestructura tecnológica de la Entidad. El contratista deberá garantizar que las actualizaciones, correcciones y mejoras implementadas no afecten la disponibilidad, integridad, confidencialidad, interoperabilidad ni el desempeño de los servicios tecnológicos de la UAEJPMP. Las obligaciones descritas deberán ser prestadas durante el período acordado, contado a partir de la fecha de activación, entrega y puesta en funcionamiento de las licencias y derechos de uso renovados y adquiridos, conforme a las cantidades y especificaciones establecidas en el presente documento.

ANEXO No. 2

Los riesgos que podrían afectar el normal desarrollo de las actividades previstas en esta contratación son las siguientes:

O. N.	Clase	Fuente	Etapa	Tipo	Descripción (Qué puede pasar y, cómo puede ocurrir)	Consecuencias de la ocurrencia del evento	Probabilidad	Impacto	Valoración del riesgo	Categoría	¿A quién se le asigna?	Tratamiento /Controles a ser implementados	Impacto después de Tratamiento				¿Afecta la ejecución del contrato?	Persona responsable por	Fecha estimada en que se inicia el tratamiento	Fecha estimada en que se completa el tratamiento	Monitoreo y revisión	
													Probabilidad	Impacto	Valoración del riesgo	Categoría					¿Cómo se realiza el monitoreo?	Periodicidad ¿Cuánto?
1	GENERAL	EXTERNA	EJECUCIÓN	REGULATORIO	Cuando el contrato deba ser suspendido por causas ajenas a la voluntad, la entidad y/o cuando sea solicitado por parte del contratista, se le notificará a este el acto administrativo que suspende el contrato, el cual deberá indicar con claridad las causas exógenas o las razones expuestas por el contratista, así como la fecha de reanudación	Suspensión del contrato y notificación al contratista del acto administrativo que deberá indicar las causas y la fecha de reanudación del contrato	4	2	6	ALTO	CONTRATISTA Y ENTIDAD	Mitigar la causa de la suspensión.	3	2	5	MEDIO	SI	Entidad / Contratista	A partir de la firma del contrato	Hasta la terminación del contrato y/o su liquidación	Seguimiento a la causa de la suspensión a través de la gestión del supervisor	Ocurrencia del hecho
	GENERAL	EXTERNA	EJECUCIÓN	REGULATORIO	Se presenta por la expedición de normas que impongan nuevos tributos, impuestos, o cargas parafiscales, que puedan afectar el equilibrio económico del contrato.	Afecta el equilibrio contractual, aumento de costos no contemplados en el contrato	5	3	8	MEDIO	CONTRATISTA Y ENTIDAD	Una vez sea expedida una disposición legal que afecte el valor del contrato, el contratista debe solicitar y justificar si es necesario tramitar una modificación contractual	1	2		BAJO	NO	Entidad / Contratista	A partir del inicio del contrato	Hasta la terminación del contrato y/o su liquidación	Verificación permanente de cambios tributarios	De acuerdo con la posibilidad de ocurrencia
	General	Externo	Ejecución	Financiero	Cuando el contratista no cuente con la liquidez necesaria para la correcta ejecución del contrato	Ausencia de recursos para la ejecución y posible financiación, cesión de derechos económicos	3	4	7	RIESGO ALTO	Contratista	Establecer seguimiento al plan de inversión	2	3	5	RIESGO MEDIO	SI	Contratista	Desde los requisitos ejecución y legalización del contrato	Plazo de ejecución del contrato	Control Entidad	Al iniciar la ejecución contractual y mensualmente
	ESPECÍFICO	INTERNO	PLANEACIÓN	ECONÓMICOS	La inadecuada proyección de costos económicos incurridos por el contratista en la	Afectación en la ejecución del contrato	3	3	6	MEDIO	CONTRATISTA	Presentar las cotizaciones y ofertas en el proceso contractual basadas en estudios en pesos	2	2	4	BAJO	SI	CONTRATISTA	Desde los requisitos ejecución y legalización del contrato	Hasta la terminación del contrato y/o su liquidación	En la realización del estudio de mercado, se estudiarán las cotizaciones	Cuando se está realizando los estudios de Mercado y durante el término de presentación

9	ESPECÍFICO	GENERAL	6	5	ejecución del contrato al momento de presentar su propuesta económica a la Administración.
EXTERNAL	GENERAL	GENERAL	GENERAL	GENERAL	
EJECUCIÓN	EXTERNAL	EXTERNAL	EXTERNAL	EXTERNAL	
OPERACIONAL	EJECUCIÓN	PLANEACIÓN	PLANEACIÓN	ECONÓMICO	Presentación de ofertas con precios artificialmente bajos.
Riesgo de fuga de información	TECNOLOGÍCOS	ECONÓMICO	ECONÓMICO		Se pone en riesgo el proceso de selección y el cumplimiento de obligaciones contractuales en el caso que se adjudique.
Afectación Integridad, disponibilidad y confidencialidad de la información		Aumento de la propuesta económica y afectación al presupuesto de la entidad		2	
2		4		3	
2		4		5	
4		8			
BAJO	ALTO		MEDIO		
CONTRATISTA	CONTRATISTA	CONTRATISTA	CONTRATISTA		Realizar un estudio de mercado ajustado a la realidad comercial.
Exigir al contratista la suscripción del compromiso de confidencialidad como la vigilancia	Validar la posible incidencia que esta fluctuación pueda afectar la determinación del presupuesto o y tenerlo en cuenta en los estudios de mercado, se solicita las cotizaciones en pesos. Utilizar productos financieros para controlar el riesgo.	1	3	4	teniendo en cuenta los indicadores económicos en la coyuntura actual, para que no tenga incidencia directa en los valores y la ejecución del futuro contrato.
1		3			
1		3			
1		6			
BAJO	MEDIO		BAJO		
SI	SI		SI		
CONTRATISTA	CONTRATISTA		CONTRATISTA		
A partir del inicio del contrato	En el momento de la adjudicación	En el momento de la adjudicación	En el momento de la adjudicación		
Hasta la terminación del contrato	Hasta la creación del contrato	Hasta la creación del contrato	Hasta la creación del contrato		
Realizar la instalación y configuración del software del componente adquirido	Establecer el presupuesto teniendo en cuenta la fluctuación de la moneda cambiaria y hacer seguimiento continuo a la misma durante el término de ejecución del contrato	Supervisión y monitoreo, que eviten interrupciones en el servicio.	Solicitar o la sustentación de los precios artificialmente bajos al proponente.		es a fin de estimar el presupuesto estimado adecuado para el cumplimiento del objeto contractual
Durante toda la etapa contractual	Permanente	Ocurrencia del hecho	Quando se está realizando la evaluación de las ofertas.		de las ofertas y la ejecución del contrato

10	ESPECÍFICO	EXTERNO	EJECUCIÓN	OPERACIONAL	Retiro del contratista como canal distribuidor del fabricante	Hacer incurrir en costos adicionales al contratista y en posibles incumplimientos 2	2	2		BAJO	CONTRATISTA	que realiza el supervisor del contrato	1	1	1	BAJO	SI	CONTRATISTA	A partir del inicio del contrato	Hasta la terminación del contrato	de acuerdo con las mejores prácticas de seguridad del fabricante.	
												El contratista deberá garantizar que antes y durante la vigencia del contrato se mantendrá como canal distribuidor del fabricante								Evaluar la vigencia de la certificación como canal distribuidor del fabricante y exigir su renovación al vencimiento de esta	Cuando el fabricante retire al contratista como canal autorizado de distribución	