DIRECCIÓN DE INTELIGENCIA POLICIAL

Bogotá D.C., 25 de marzo de 2022

I. ASPECTOS GENERALES DEL ESTUDIO PREVIO.

1. DEFINICIÓN O IDENTIFICACIÓN DE LA NECESIDAD Y ANÁLISIS DEL SECTOR

1.1 DESCRIPCIÓN GENERAL DEL OBJETO

ADQUISICIÓN SOFTWARE DE ANTIVIRUS, CONGELADOR DE DISCO, HIPERVISOR DE MÁQUINA VIRTUAL Y VPN

CLASIFICACIÓN UNSPSC	SEGMENTO	FAMILIA	CLASE
43231500	Difusión de tecnologías de la información y telecomunicaciones	Software	Software funcional
43232800	Difusión de tecnologías de la información y telecomunicaciones	Software	Software de administrador de redes
43232700	Difusión de tecnologías de la información y telecomunicaciones	Software	Software de aplicaciones de red
43233200	Difusión de tecnologías de la información y telecomunicaciones	Software	Software de seguridad y protección

1.2 VALOR ESTIMADO

El valor estimado del presente proceso es de NOVENTA Y OCHO MILLONES NOVECIENTOS CINCUENTA Y SEIS MIL SETECIENTOS CINCUENTA Y NUEVE PESOS CON SESENTA CENTAVOS M/CTE ($ 98.956.759,60) *

ÍTEM Y/O LOTE	RUBRO Y DESAGREGACIÓN PRESUPUESTAL	UNIDAD	DESCRIPCIÓN	RECURSO	CANTIDAD	VALOR UNITARIO ESTIMADO, EXENTO DE IVA	VALOR TOTAL ESTIMADO, EXENTO DE IVA
1	02-01-01-006-002-03	10	DIPOL	SOFTWARE PAQUETE ANTIVIRUS	70	$ 59.997,57	$ 4.199.829,90
2	02-01-01-006-002-03	10	DIPOL	SOFTWARE DE CONGELADOR DE DISCO	70	$ 179.992,71	$ 12.599.489,70
3	02-01-01-006-002-03	10	DIPOL	SOFTWARE VPN	70	$ 439.807,00	$ 30.786.490,00
4	02-01-01-006-002-03	10	DIPOL	SOFTWARE DE HIPERVISOR DE MÁQUINA VIRTUAL.	30	$ 1.712.365,00	$ 51.370.950,00
						VALOR TOTAL ESTIMADO	$ 98.956.759,60

NOTA: *El bien objeto de adquisición se encuentra catalogado como exento, de acuerdo a lo dispuesto en el artículo 188 del decreto 1819 de 2016, que modifica el artículo 477 del Estatuto Tributario. Bienes que se encuentran exentos del impuesto, literal n) Equipos, software y demás implementos de sistemas y comunicaciones para uso de las Fuerzas Militares y la Policía Nacional. Atendiendo su naturaleza y destinación estos bienes se encuentran gravados a la tarifa 0

1.3 CERTIFICACIÓN PLAN ANUAL DE ADQUISICIONES, GASTOS DE FUNCIONAMIENTO Y/O INVERSIÓN Y/O VIGENCIAS FUTURAS.

No.	Fecha	No. Plan de compras	Unidad	Recurso	Descripción	Cantidad	Valor unitario	Valor total
1	31/03/2022	53	DIPOL	10	SOFTWARE DE ANTIVIRUS DE MAQUINA VIRTUAL	30	$ 1.712.365,00	$ 51.370.950,00
2	31/03/2022	53	DIPOL	10	SOFTWARE VPN	70	$ 439.807,00	$ 30.786.490,00
3	31/03/2022	53	DIPOL	10	SOFTWARE DE CONGELADOR DE DISCO	70	$ 179.992,71	$ 12.599.489,70
4	31/03/2022	53	DIPOL	10	SOFTWARE PAQUETE ANTIVIRUS	70	$ 59.997,57	$ 4.199.829,90
					Total	240	$ 2.392.162,28	$ 98.956.759,60

1.4 CLASE DE CONTRATO

Compraventa

1.5 PERFIL Y CALIDAD DE LOS PROPONENTES

Se indica que a la necesidad del objeto del estudio previo el posible oferente podrá ser fabricante, distribuidor y/o comerciante.

Podrán participar todas las personas naturales o jurídicas, nacionales o extranjeras con representación o sucursal en Colombia, en forma individual o conjunta (Consorcio o Unión Temporal).

1.6 IDENTIFICACIÓN DE LA NECESIDAD Y JUSTIFICACIÓN

Uno de los principales retos para la Dirección de Inteligencia Policial es el mantenimiento de la información, lo que acarrea tomar medidas preventivas y reactivas en sistemas tecnológicos, que ayuden resguardar, proteger, mantener la confidencialidad, disponibilidad e integridad de los mismos. Con la actualización constante de los sistemas tecnológicos se facilita este proceso, porque se busca evitar alteraciones por circunstancias o factores externos; por lo cual al lograr el objetivo surge la necesidad de la adquisición de software que permita fortalecer el esquema de seguridad informática a través de técnicas y métodos de protección destinados a prevenir y resguardar la información que puede ser susceptible a daños o hurtos.

Alineados al contexto y atendiendo las responsabilidades establecidas en las políticas públicas, dentro del marco del CONPES 3995 "Confianza y Seguridad Digital" y el papel de la Inteligencia para recolectar información en pro de identificar, anticipar y contrarrestar las capacidades, intenciones y actividades de los ciberactores, la Policía Nacional, a través del Servicio de Inteligencia Policial y su grupo de Inteligencia de Señales y Geoespacial cuenta con capacidades de recolección y análisis de información, en el despliegue de actividades de cibermonitoreo, ciberpatrullaje y recolección técnica del ciberespacio. En donde actualmente la Dirección de Inteligencia Policial no cuenta con el software mencionado en el presente estudio previo. Por ende, no se está garantizando el anonimato y la seguridad en su navegación por la internet poniendo en riesgo la integridad, disponibilidad y confidencialidad de la información. Es por esto que es necesario con el fin de afianzar la importancia de generar canales seguros para la transferencia de información, incorporando tecnología de punta, protocolos seguros de comunicación y características de administración que garanticen altos niveles de seguridad de

cifrado para salvaguardar la información de la Dirección de Inteligencia. Es por ello que se va a adquirir los siguientes softwares, así:

Software de antivirus con el objetivo de poder blindar la seguridad de la información y control de virus, spam, malware, entre otras vulnerabilidades que puedan presentarse al momento de realizar la navegación en la red, así mismo proteger la infraestructura tecnológica y equipos de la Dirección de Inteligencia Policial.

Software congelador de disco el cual permita que la configuración de las estaciones de trabajo sea inalterable, así mismo garantiza la recuperación integral de las mismas, protege las configuraciones del equipo al igual que las múltiples particiones y unidades de disco duro, con el fin de garantizar la integralidad, confidencialidad y evitar afectaciones a la información que maneja el Grupo de Inteligencia de Señales y Geoespacial.

Software VPN de host (red privada virtual) que cifre los datos y no permita que estos sean obtenidos por delincuentes cibernéticos, quienes podrían obtener acceso a información de carácter confidencial que se maneja al interior del Grupo de Inteligencia de señales y Geoespacial, lo que permite trabajar de manera segura y protegida, sin importar dónde se encuentre el funcionario de inteligencia.

Software hipervisor de máquina virtual es una tecnología que utiliza software para emular el comportamiento del hardware creando un sistema operativo sobre una máquina virtual. Esto permite ejecutar múltiples sistemas operativos y aplicaciones, en un solo equipo de cómputo.

Así mismo, permite ejecutar las aplicaciones en una red virtual del mismo modo que en una red física, pero con mayores ventajas operativas y con la independencia del hardware que esta tecnología ofrece. Adicionalmente, permite gestionar y emular el comportamiento de los dispositivos y servicios de red lógicos (puertos, conmutadores, enrutadores, cortafuegos, equilibradores de carga, conexiones VPN, etc. con las cargas de trabajo que se hayan asociado.

La utilización de un hipervisor de escritorio permite ejecutar máquinas virtuales emulando recursos de la maquina anfitriona. Este ayudará que el funcionario recolector de información pueda navegar en un espacio protegido y seguro dentro del equipo de cómputo en la internet, no generando riesgos a la integralidad, disponibilidad y confidencialidad de la información por la contaminación generada por un malware, Ransomware o virus a la maquina física o red interna de la Dirección de Inteligencia Policial.

Dado lo anterior, la implementación de estos softwares permitirá mejorar la protección del sistema y la confidencialidad de la información, sumado a generar correlación y análisis desde el punto de vista de inteligencia policial; la cual permitirá dar respuesta a los diferentes requerimientos institucionales, mediante el desarrollo de productos en todos los campos y eventos, o amenazas de ciberseguridad, con calidad, oportunidad, impacto, confidencialidad y capacidad de asesoramiento al mando institucional.

ÍTEM	DESCRIPCIÓN	No. CANTIDAD ADQUIRIR	No. NECESIDAD	PORCENTAJE NECESIDAD
1	SOFTWARE PAQUETE ANTIVIRUS	70	70	100%
2	SOFTWARE DE CONGELADOR DE DISCO	70	70	100%
3	SOFTWARE VPN	70	70	100%
4	SOFTWARE DE HIPERVISOR DE MÁQUINA VIRTUAL	30	70	43%

Es de notar que para el ítem 4 de la anterior tabla, la necesidad es de setenta (70), pero por temas de presupuesto la capacidad a contratar es de treinta (30). Por tanto, se hace necesario la adquisición de cuarenta (40) software para suplir la necesidad, las cuales se tendrá en cuenta en una futura adición presupuestal.

Es importante indicar, que con la contratación de los bienes se cumple con lo establecido en la normatividad vigente frente a la austeridad del gasto.

Así mismo, los bienes son requeridos para el mes de mayo de la presente vigencia.

2. ANTECEDENTES ADMINISTRATIVOS DEL PROCESO

UNIDAD CONTRATANTE Y CONTRATISTA	NÚMERO DEL CONTRATO Y FECHA DE SUSCRIPCIÓN	OBJETO	NÚMERO DE PROCESO	ACIERTOS	PROBLEMAS
MINISTERIO DE HACIENDA Y CREDITO PUBLICO - PULXAR	3.257-2019 - 17/06/2019	CONTRATAR EL SERVICIO DE MANTENIMIENTO Y SOPORTE ESPECIALIZADO PARA LAS PLATAFORMAS DE REDHAT, ORACLE LINUX Y DE VIRTUALIZACIÓN ORACLE VM IMPLEMENTADOS EN EL MINISTERIO DE HACIENDA Y CRÉDITO PÚBLICO.	MHCP-PMC-12-2019	EL CONTRATO SE EJECUTÓ SIN CONTRATIEMPOS	NO SE PRESENTARON
INSTITUTO DISTRITAL DE LA PARTICIPACIÓN Y ACCIÓN COMUNAL - SAFETY IN DEEP SAS	972-2020 - 19/11/2020	MANTENIMIENTO Y RENOVACIÓN DE LICENCIAMIENTO DE LA SOLUCIÓN ENDPOINT SANDBLAST Y ADQUISICIÓN DE LICENCIAS VPN (PRESENTACIÓN DE OFERTA)	SASI-IDPAC-008-2020	EL CONTRATO SE EJECUTÓ SIN CONTRATIEMPOS	NO SE PRESENTARON
DIRECCIÓN DE INTELIGENCIA POLICIAL - ACONPIEXPRESS	04-2-10036-2021 - 10/08/2021	ADQUISICIÓN MEMORIA RAM, UNIDADES DE ESTADO SOLIDO Y LICENCIAS RED HAT ENTERPRISE VIRTUALIZATION PARA LA DIRECCIÓN DE INTELIGENCIA POLICIAL	PN DIPOL SA 037-2021	EL CONTRATO SE EJECUTÓ SIN CONTRATIEMPOS	NO SE PRESENTARON

- **Información verificada y aprobada por los funcionarios dueños de la necesidad que firman el presente estudio previo.**

3. FUNDAMENTOS JURÍDICOS QUE SOPORTAN LA MODALIDAD DE SELECCIÓN

Según lo expresado por el literal c) del numeral 1.1. Capítulo III de la resolución No. 03049 de 2014, *"Por medio de la cual se adopta el manual de contratación de la Policía Nacional"*:

> *"Se expresarán las razones que llevan a escoger la modalidad de selección de que se trate, indicando sobre el particular, los aspectos que se consideran determinantes para la aplicación de una u otra modalidad. (Podrán considerarse para los efectos enunciados las características del objeto a contratar, las circunstancias de la contratación, la cuantía o destinación de los bienes, servicios u obra, naturaleza de los contratantes, etc.)"*

Por lo anterior, se indica que la modalidad de selección, teniendo en cuenta lo dispuesto en las Leyes 80 de 1993, 1150 del 2007, 1882 de 2018 y el Decreto 1082 del 2015, es:

MÍNIMA CUANTÍA Previsto en el Capítulo 2, Sección 1, Subsección 5, Artículo 2.2.1.2.1.5.2 establece el procedimiento para la contratación de mínima cuantía, ya que el valor del estudio previo no excede el 10% de la menor cuantía de la Entidad Estatal e independientemente de su objeto.

4. CRITERIOS DE SELECCIÓN

4.1. ESPECIFICACIONES TÉCNICAS MÍNIMAS

4.2. Las especificaciones técnicas requeridas serán evaluadas como **CUMPLE** o **NO CUMPLE** y están descritas en el anexo Especificaciones Técnicas Mínimas del presente estudio previo.

4.2.1. EXPERIENCIA PROPONENTE

Con el fin de garantizar la calidad de los bienes a contratar y evitar incumplimientos en la ejecución del futuro contrato, se requiere acreditar experiencia en la venta software similares al objeto del presente estudio previo, tal acreditación será avalada con la presentación de certificaciones que acrediten la participación en contratos suscritos en los últimos tres (03) años (2019 y/o 2020 y/o 2021) con empresas públicas o privadas para lo cual el oferente deberá presentar máximo tres (03) certificaciones expedidas por la entidad que adquirió los software, con concepto favorable de la recepción de los servicios cuya suma o valor individual sea igual o superior al 100% del presupuesto oficial asignado.

Este aspecto se verificará en el anexo Especificaciones Técnicas Mínimas.

4.1.2 NIVEL DE EDUCACIÓN O NIVEL ACADÉMICO

El funcionario que realizará la instalación y configuración de los softwares, deberán ostentar el título de tecnólogo o ingeniero en Sistemas y/o Electrónico y/o a fines, para lo cual el oferente deberá presentar con la oferta, copia del diploma y/o acta de grado del título de dicho funcionario.

La Dirección de Inteligencia Policial de la Policía Nacional – DIPOL podrá solicitar el cambio del personal ofrecido en cualquier momento a partir de la suscripción del contrato y el mismo podrá ser sustituido por el proponente por uno con iguales o mejores capacidades, condiciones y calificaciones a las presentadas en la oferta.

NOTA: en caso de ser profesional extranjero deberá presentar certificado de homologación de su título profesional ante el Ministerio de Educación Nacional de Colombia.

4.1.3 EXPERIENCIA (No aplica)

4.1.4 EXPERIENCIA DEL PERSONAL

Con el fin de garantizar la idoneidad del funcionario encargado de las actividades de instalación, configuración de los software de antivirus, congelador de discos, hipervisor de máquina virtual, red privada virtual (VPN) e hipervisor de máquina virtual ofertada, el proponente deberá certificar que esta persona cuente con experiencia en Colombia de haber participado mínimo en un (1) proyecto relacionado con el objeto del presente contrato; para lo cual el oferente debe anexar a la propuesta, una (1) certificación de proyectos en los cuales haya participado, expedidas por el oferente, durante los últimos tres (3) años anteriores a la fecha de apertura del presente proceso.

Este aspecto se verificará en el Anexo Especificaciones Técnicas Mínimas.

4.1.5 CAPACIDAD OPERATIVA (No aplica)

4.1.6 OTRAS CONDICIONES TÉCNICAS VERIFICABLES (No aplica)

4.3. CONDICIONES TÉCNICAS ADICIONALES DE CALIFICACIÓN Y SU JUSTIFICACIÓN (No aplica):

4.3. EVALUACIÓN ECONÓMICA Y FINANCIERA

4.3.1. EVALUACIÓN ECONÓMICA

Se tendrá en cuenta la propuesta presentada con el menor valor a través de la plataforma del SECOP II.

4.3.2. FACTORES ADICIONALES DE CALIFICACIÓN Y SU JUSTIFICACIÓN:

No aplica

4.3.3. CRITERIOS DE DESEMPATE

En caso de empate se dará aplicabilidad a lo establecido en el artículo 35 de la ley 2069 del 2020 y demás normas vigentes.

5. CONDICIONES DEL CONTRATO

5.1. LUGAR DE ENTREGA O LUGAR DE PRESTACIÓN DEL SERVICIO

Los softwares a adquirir deberán ser entregados en el Almacén de Intendencia de la Dirección de Inteligencia Policial ubicada en la Avenida Boyacá No. 142 A 55, Barrio Colina Campestre, Bogotá D.C.

5.2. FORMA DE EJECUCIÓN

La ejecución del contrato será en forma total, previo acuerdo y coordinación con el supervisor del Contrato.

5.3. PLAZO DE EJECUCIÓN

El plazo de ejecución del contrato será a partir del día hábil siguiente a la aprobación de la garantía única y hasta el 15 de julio del 2022.

5.4. FORMA DE PAGO

El pago se realizará en moneda legal colombiana, en forma total, dentro de los sesenta (60) días calendario siguientes a la radicación de la factura, junto con el recibido a satisfacción suscrito por el supervisor del contrato, con los documentos requeridos por el Área Administrativa, de la Dirección de Inteligencia Policial, en caso de que los elementos sean de origen extranjero se deberá aportar la declaración de importación, de acuerdo al derecho a turno y la programación del plan anual de caja (PAC).

NOTA: El contratista en caso de estar obligado a facturar electrónicamente, deberá presentar en la ejecución la factura electrónica validada previamente por la DIAN, como requisito necesario para el pago de los bienes y/o servicios contratados. Lo anterior, teniendo en cuenta lo establecido en el Decreto 358 del 05 de marzo de 2020, Resolución No. 000042 del 05/05/2020 expedida por la DIAN y demás normas que reglamenten la facturación electrónica.

5.5. SUPERVISOR, INTERVENTOR Y/O COORDINADOR

La supervisión del contrato estará a cargo del Jefe Área Producción de Inteligencia o quien haga sus veces, o quien con posterioridad sea designado por parte del Director de Inteligencia, quien verificará la ejecución idónea y el cumplimiento del objeto del contrato de acuerdo con las funciones asignadas para el efecto en el numeral 1° del artículo 26 de la ley 80 del 1993, los artículos 83 y 84 de la ley 1474 del 2011, la resolución 00090 del 2018 y demás normas que regulen la materia.

5.6. OBLIGACIONES DEL CONTRATISTA

No aplica

5.7. OBLIGACIONES DE LA POLICÍA NACIONAL

No aplica

6. FORMA Y PROCEDIMIENTO DE ADJUDICACIÓN

No aplica

7. ESTIMACIÓN, TIPIFICACIÓN, ASIGNACIÓN DE RIESGOS Y DETERMINACIÓN DE GARANTÍAS.

Están descritas en el anexo estimación, tipificación, asignación de riesgos y determinación de garantías del presente estudio previo.

II. ESTUDIO DEL SECTOR

1. ANÁLISIS DE LA DEMANDA

Uno de los principales retos para la Dirección de Inteligencia Policial es el mantenimiento de la información, lo que acarrea tomar medidas preventivas y reactivas en sistemas tecnológicos, que ayuden resguardar, proteger, mantener la confidencialidad, disponibilidad e integridad de los mismos. Con la actualización constante de los sistemas tecnológicos se facilita este proceso, porque se busca evitar alteraciones por circunstancias o factores externos; por lo cual al lograr el objetivo surge la necesidad de la adquisición de software que permita fortalecer el esquema de seguridad informática a través de técnicas y métodos de protección destinados a prevenir y resguardar la información que puede ser susceptible a daños o hurtos.

Alineados al contexto y atendiendo las responsabilidades establecidas en las políticas públicas, dentro del marco del CONPES 3995 "Confianza y Seguridad Digital" y el papel de la Inteligencia para recolectar información en pro de identificar, anticipar y contrarrestar las capacidades, intenciones y actividades de los ciberactores, la Policía Nacional, a través del Servicio de Inteligencia Policial y su grupo de Inteligencia de Señales y Geoespacial cuenta con capacidades de recolección y análisis de información, en el despliegue de actividades de cibermonitoreo, ciberpatrullaje y recolección técnica del ciberespacio. En donde actualmente la Dirección de Inteligencia Policial no cuenta con el software mencionado en el presente estudio previo. Por ende, no se está garantizando el anonimato y la seguridad en su navegación por la internet poniendo en riesgo la integridad, disponibilidad y confidencialidad de la información. Es por esto que es necesario con el fin de afianzar la importancia de generar canales seguros para la transferencia de

información, incorporando tecnología de punta, protocolos seguros de comunicación y características de administración que garanticen altos niveles de seguridad de cifrado para salvaguardar la información de la Dirección de Inteligencia. Es por ello que se va a adquirir los siguientes softwares, así:

Software de antivirus con el objetivo de poder blindar la seguridad de la información y control de virus, spam, malware, entre otras vulnerabilidades que puedan presentarse al momento de realizar la navegación en la red, así mismo,proteger la infraestructura tecnológica y equipos de la Dirección de Inteligencia Policial.

Software congelador de disco el cual permita que la configuración de las estaciones de trabajo sea inalterable, así mismo garantiza la recuperación integral de las mismas, protege las configuraciones del equipo al igual que las múltiples particiones y unidades de disco duro, con el fin de garantizar la integralidad, confidencialidad y evitar afectaciones a la información que maneja el Grupo de Inteligencia de Señales y Geoespacial.

Software VPN de host (red privada virtual) que cifre los datos y no permita que estos sean obtenidos por delincuentes cibernéticos, quienes podrían obtener acceso a información de carácter confidencial que se maneja al interior del Grupo de Inteligencia de señales y Geoespacial, lo que permite trabajar de manera segura y protegida, sin importar dónde se encuentre el funcionario de inteligencia.

Software hipervisor de máquina virtual es una tecnología que utiliza software para emular el comportamiento del hardware creando un sistema operativo sobre una máquina virtual. Esto permite ejecutar múltiples sistemas operativos y aplicaciones, en un solo equipo de cómputo.

Así mismo, permite ejecutar las aplicaciones en una red virtual del mismo modo que en una red física, pero con mayores ventajas operativas y con la independencia del hardware que esta tecnología ofrece. Adicionalmente, permite gestionar y emular el comportamiento de los dispositivos y servicios de red lógicos (puertos, conmutadores, enrutadores, cortafuegos, equilibradores de carga, conexiones VPN, etc. con las cargas de trabajo que se hayan asociado.

La utilización de un hipervisor de escritorio permite ejecutar máquinas virtuales emulando recursos de la maquina anfitriona. Este ayudará que el funcionario recolector de información pueda navegar en un espacio protegido y seguro dentro del equipo de cómputo en la internet, no generando riesgos a la integralidad, disponibilidad y confidencialidad de la información por la contaminación generada por un malware, Ransomware o virus a la maquina física o red interna de la Dirección de Inteligencia Policial.

Dado lo anterior la implementación de estos softwares permitirá mejorar la protección del sistema y la confidencialidad de la información, sumado a generar correlación y análisis desde el punto de vista de inteligencia policial; la cual permitirá dar respuesta a los diferentes requerimientos institucionales, mediante el desarrollo de productos en todos los campos y eventos, o amenazas de

ciberseguridad, con calidad, oportunidad, impacto, confidencialidad y capacidad de asesoramiento al mando institucional.

ÍTEM	DESCRIPCIÓN	No. CANTIDAD ADQUIRIR	No. NECESIDAD	PORCENTAJE NECESIDAD
1	SOFTWARE ANTIVIRUS	70	70	100%
2	SOFTWARE CONGELADOR DE DISCO	70	70	100%
3	SOFTWARE VPN	70	70	100%
4	SOFTWARE HIPERVISOR DE MÁQUINA VIRTUAL	30	70	43%

Es de notar que para el ítem 4 de la anterior tabla, la necesidad es de setenta (70), pero por temas de presupuesto la capacidad a contratar es de treinta (30). Por tanto, se hace necesario la adquisición de cuarenta (40) software para suplir la necesidad, las cuales se tendrá en cuenta en una futura adición presupuestal.

2. ANÁLISIS DEL MERCADO

DESCRIPCIÓN DEL MERCADO

Los riesgos de la infraestructura computacional y de la información de las organizaciones les exigen a las empresas controlar impactos potenciales respecto a incidentes que deben neutralizar. Las políticas de seguridad abren oportunidades de negocio a las empresas de software que ofrecen un portafolio de servicios de expertos en gestión y monitoreo de seguridad, que utilizan herramientas avanzadas de protección de las aplicaciones, soluciones especializadas, investigación y personal con conocimientos de los entornos de las amenazas. El mercado nacional cuenta con empresas de reconocida trayectoria con la capacidad de ofrecer los softwares del presente estudio previo.

Según (Pastorino C. 2022). En su artículo "tendencias en ciberseguridad 2022: entre la evolución de las amenazas y los desafíos del trabajo híbrido". Cuando el mundo entero tuvo que quedarse en casa en el 2020, la mayoría de las empresas debieron implementar el teletrabajo y se enfocaron en brindar soluciones a sus empleados para que puedan realizar sus tareas mediante herramientas en línea. Este modelo de trabajo nuevo para muchos resultó muy eficaz, ya que los empleados encontraron en esta modalidad un mayor equilibrio entre la vida personal y laboral al ahorrar tiempo y dinero en desplazarse a una oficina. Además, muchos gerentes se sorprendieron al ver no solo que la productividad no se desplomó, sino que en muchos casos aumentó.

En el 2021 ha quedado claro que el trabajo remoto llegó para quedarse. Según una encuesta realizada por ESET en América Latina, el 70,5% de los trabajadores el tema de la ciberseguridad le preocupa más que antes y el 91% de las empresas ha tenido que digitalizar procesos críticos. Sin embargo, el 30% de los encuestados considera que su empresa no está mejor preparada para enfrentar las amenazas actuales. De hecho, el 77% de los encuestados utiliza su equipo personal

para trabajar y el 57% no fue provisto de las herramientas de seguridad necesarias para desarrollar su labor desde su hogar.

Si revisamos qué herramientas han adoptado las empresas, apenas el 30% utiliza soluciones que son básicas para la protección del acceso remoto, antivirus, congeladores de disco y conexión VPN y sólo el 52% ha realizado capacitaciones de seguridad informática para los teletrabajadores.

https://www.welivesecurity.com/la-es/2021/11/18/tendencias-ciberseguridad-2022/

El incremento en el uso del entorno digital aumenta las amenazas cibernéticas, las vulnerabilidades y los incidentes digitales. Situación que afecta la seguridad de los ciudadanos, de las organizaciones públicas y privadas, e incluso de la infraestructura que hace parte de los intereses de la nación, durante los últimos años, la industria de tecnologías de la información en el entorno de seguridad de la información ha construido herramientas tecnológicas basadas en recolección masiva, inteligencia artificial y big data, que permiten acortar tiempos de respuesta en la identificación, perfilación y análisis de redes de los actores que interactúan en el ciberespacio.

Estas técnicas y herramientas para la recopilación y análisis de información son cada vez más populares y son un aspecto clave de la seguridad de la información. En este sentido en la 15va edición de Ekoparty, el equipo de OSINT Latam Group presentó un taller de herramientas de OSINT e Ingeniería Social aplicadas a las investigaciones.

https://www.welivesecurity.com/la-es/2019/10/07/tecnicas-herramientas-osint-investigacion-internet/

Perspectiva regional y análisis de tendencias:

El mercado está impulsado por Israel, América del Norte por Asia Pacífico. Esto se debe principalmente a los ataques digitales expandidos en los EE.UU. También debido al avance dinámico y al desarrollo en investigación y desarrollo, las organizaciones en los EE.UU. y Canadá han adoptado la innovación más rápido que otras. No obstante, se espera que el desarrollo del mercado en Asia-Pacífico se desarrolle tremendamente.

Información competitiva:

Los principales actores en el mercado son CybelAngel, KB Crawl SAS, Palantir Technologies, SAIL LABS Technology, Digimind, Verint Systems, Intrinsic Technologies LLC, sistema experto, Thales Group y Exalead Dassault Systemes. Los principales actores del mercado se perfilan en detalle en vista de las cualidades, por ejemplo, cartera de la empresa, estrategias comerciales, visión general financiera, desarrollos recientes y participación de la industria en general.

Perspectiva de la industria y análisis de tendencias:

El mercado de inteligencia de fuente abierta (OSINT) ha experimentado un crecimiento significativo en los últimos años y se prevé un crecimiento enorme durante el período de pronóstico. El conocimiento de código abierto (OSINT) es información recopilada de fuentes de acceso libre para ser utilizada como parte de un contexto de inteligencia.

Segmentación de mercado:

El mercado de inteligencia de código abierto está segmentado en función del tipo, la tecnología y la aplicación. Según el tipo, el mercado se segmenta en inteligencia humana, análisis web oscuro, análisis de enlaces / redes, inteligencia de contenido, análisis de texto, análisis de datos, inteligencia artificial y big data. De estos, big data, análisis de texto y análisis de enlaces / redes dominan el mercado. Esto se debe a las progresiones tecnológicas y los análisis en el espacio cibernético que provocan una mayor amenaza de ciberataques, piratería y otros ejercicios ilegales. Basado en la tecnología, el mercado está segmentado en análisis de Big Data, análisis web, análisis de texto, seguridad cibernética, análisis de video y análisis de redes sociales. El software Big Data permite a OSINT proporcionar soporte productivo e importante para las técnicas e inteligencia empresarial de una organización.

https://steemit.com/utopian-io/@difelice/segmentos-de-mercado-de-open-source-intelligence-osint-estrategias-de-jugadores-clave-y-mas-hasta-2023-esto-aporta-el-informa

El mercado de inteligencia de código abierto está segmentado de la siguiente manera:

Por tipo:

Inteligencia humana, Análisis web oscuroLink / network analysis, Inteligencia de contenido, Análisis de texto, Analítica de datos, Inteligencia artificial, Grandes datos.

Por tecnología:

Text AnalyticsVideo, AnalyticsWeb, Analysis BigData, Software Análisis de redes sociales, Cyber Security, Otras

Por aplicación:

Sector público, Military & Defence, Sector privado, Homeland Security, Seguridad nacional y Otros.

Para realizar un análisis del mercado de los antivirus, congeladores de discos y VPN se han tenido en cuenta dos importantes artículos de reciente publicación en internet, las cuales nos dan una visión actual del sector de la seguridad de la información y en especial del nivel de protección que se debe lograr en los equipos de cómputo. También nos muestran los artículos antes mencionados, algunos detalles sobre las diferentes compañías mundiales dedicadas a la protección de la seguridad del equipo de cómputo del usuario final contra control de aplicaciones, códigos maliciosos y virus informáticos.

Según el Instituto de Educación Superior Tecnológico Público de Argentina (ISTPARGENTINA, 2020). Un controlador del núcleo o congelador de disco protege la integridad del de la unidad de almacenamiento redirigiendo la información que se va a escribir en el disco duro o partición protegida, dejando la información original intacta. Las escrituras redirigidas desaparecen cuando el sistema es reiniciado, restaurando el equipo a su estado original. Esto permite a los usuarios realizar cambios originales en el equipo, por ejemplo, para probar cambios potencialmente estables o benignos, sabiendo que al reiniciar el sistema volverán a desaparecer.

De igual forma, puede restaurar ciertos daños provocado por el malware y virus ya que tras el reinicio cualquier cambio hecho por el software malicioso puede quedar eliminado del sistema al ser revertido al estado original (junto con cualquier otro tipo de modificaciones que se hayan hecho). Sin embargo, esto no impide que un virus o malware se desarrolle mientras que no se reinicie el sistema, o que el virus afecte a una partición que no esté protegida, o que se coloque en el registro del congelador como archivo que estaba previamente en el sistema.

https://sites.google.com/a/istpargentina.edu.pe/integracion-a-las-tics/software/seguridad/importancia-del-deep-fre

La primera publicación denominada "El mejor antivirus del Mundo de 2016: Prueba y Comparativas Antivirus", artículo publicado el 25 de enero de 2020 en el sitio web https://mejorantivirusahora.com/el-mejor-antivirus-prueba-y-comparativas/.

"Los virus se hicieron muy comunes a finales de los 80 y principios de los 90. En esa época fue también cuando se lanzaron algunos de los primeros programas antivirus, como VirusScan de John McAfee y FluShot Plus, de Ross Greenberg. Como ya hemos señalado, otro que apareció en 1991 fue Norton Antivirus. Todos estos programas eran muy básicos, y su objetivo era eliminar virus también muy básicos. Algunos de estos virus robaban espacio en disco (todavía lo hacen hoy en día, pero en discos con mucha más capacidad), ralentizaban la CPU, accedían a información privada, dañaban archivos y mucho más. A día de hoy los virus hacen lo mismo, pero entonces no alcanzaban la gran escala que tienen los de ahora.

Con los años, los virus se han expandido hasta incluir spyware, adware, troyanos, ramsonware y muchos más. El objetivo de estos virus no ha cambiado desde su origen durante los días pre-Internet, sin embargo. Sigue siendo, principalmente, robar información privada o identidades, corromper información y otras cosas dañinas. Solo que se han vuelto mucho más sofisticados, y como resultado, los antivirus también son ahora mucho más sofisticados.

Un creciente número de suites de seguridad ahora disponen de herramientas especiales para ayudar a protegerte en tus redes sociales una creciente objetivo para spammers, scammers y otros grupos que quieren hacerse con tu información personal. Por ejemplo, la suite de Bit defender Internet Security viene con una herramienta que resalta cualquier posible problema que concierna a tu configuración de privacidad en Facebook. Varias suites de seguridad también incluyen herramientas que escanean enlaces en las redes sociales para evitar que seas forzado a hacer clic en enlaces malintencionados ocultos tras un acortador de enlace".

3. ANÁLISIS DE LA OFERTA

IDENTIFICACIÓN DEL PROVEEDOR: Para el presente proceso se contará con empresas que cumplan con los criterios de evaluación exigidos por la entidad; las cuales deberán contar con la disponibilidad y experiencia en la compra y venta de softwares inmersos en el presente estudio previo que les permita brindar calidad y garantía de estas; para la identificación de proveedores se tomó contacto con las empresas que se relacionan a continuación:

PRECIOS DE MERCADO: Para el presente proceso se contará con las empresas que cumplan con los criterios de evaluación exigidos por la entidad; para la identificación de proveedores se tomó contacto con las empresas que se relacionan a continuación:

- MULTISOFTWARE TRANSACCIONAL S.A.S (MULTISOFT S.A.S) Nit: 800210453-6
  Deicy Bibiana Rodríguez Roa
  Teléfonos: 317 6397126
  Correo: multisoft@multisoft.com.co; mario.alarcon@multisoft.com.co

- SOLUCIONES TECNOLOGIA Y SERVICIOS S.A Nit: 830.505521-5
  Mauricio Amaya
  Teléfonos: 320 3805020
  Correo: raiza.benitez@stssa-com.co

- GAMMA INGENIEROS S.A.S NIT: 891.501.783-1
  Gabriel de Jesus Mazo Mayorquin
  Teléfonos: 571 4076000 Ext 152 3012192501- 3107694014
  Correo: marilyn.restrepo@gammaingenieros.com

4. MONEDA A CONTRATAR

El pago se realizará en moneda colombiana (Pesos).

5. ANÁLISIS DE PRECIOS

5.1. PRECIOS REFERENCIA SECOP (OTRAS ENTIDADES)

SOFTWARE ANTIVIRUS

ENTIDAD CONTRATANTE Y CONTRATISTA	OBJETO	NÚMERO DEL CONTRATO Y FECHA DE SUSCRIPCIÓN	NÚMERO DE PROCESO	VALOR
FONDO ROTATORIO DE LA POLICIA – ACCESAR S.A.S	"SERVICIO RENOVACIÓN LICENCIAMIENTO ANTIVIRUS PARA EL FONDO ROTATORIO DE LA POLICÍA"	MC-072-2019 - 17/12/20219	CO1.PCCNTR.1234019	$ 52.816.365
https://community.secop.gov.co/Public/Tendering/ContractDetailView/Index?UniqueIdentifier=CO1.PCCNTR.1234019&AwardContractDetailId=355680&IsFromMarketplace=False&IsFromContractNotice=True&isModal=true&asPopupView=true#GenericContractInformation				
POLICÍA NACIONAL - DIRECCIÓN ADMINISTRATIVA Y FINANCIERA - Ona Systems	SOLUCIÓN SOFTWARE ANTIVIRUS, DATA LOST PREVENTION, CONTROL DE APLICACIONES, CIFRADO Y ANTISPAM (Presentación de oferta)	06-2-10124-20 - 19/10/2020	CO1.PCCNTR.1882433	$ 1.242.000.000
https://community.secop.gov.co/Public/Tendering/ContractDetailView/Index?UniqueIdentifier=CO1.PCCNTR.1882433&AwardContractDetailId=777801&IsFromMarketplace=False&IsFromContractNotice=True&isModal=true&asPopupView=true#GenericContractInformation				
CAJA DE SUELDOS DE RETIRO DE LA POLICIA NACIONAL - Grupo Microsistemas Colombia SAS	ADQUISICION DE LICENCIAS ANTIVIRUS	CO21000197-GAC – 28/05/2021	CO1.PCCNTR.2546213	$ 30.000.000

https://community.secop.gov.co/Public/Tendering/ContractDetailView/Index?UniqueIdentifier=CO1.PCCNTR.2546213&AwardContractDetailId=1286485&IsFromMarketplace=False&IsFromContractNotice=True&isModal=true&asPopupView=true#GenericContractInformation

SOFTWARE VPN

ENTIDAD	OBJETO	NÚMERO DE CONTRATO	FECHA	VALOR
MINISTERIO DE HACIENDA Y CREDITO PUBLICO - Q&C	SOLUCIÓN VPN SSL (Presentación de oferta)	3.270-2020	14/08/2020	$ 386.035.000
https://community.secop.gov.co/Public/Tendering/ContractDetailView/Index?UniqueIdentifier=CO1.PCCNTR.1711727&AwardContractDetailId=689832&IsFromMarketplace=False&IsFromContractNotice=True&isModal=true&asPopupView=true#GenericContractInformation				
INSTITUTO DISTRITAL DE LA PARTICIPACIÓN Y ACCIÓN COMUNAL	MANTENIMIENTO Y RENOVACIÓN DE LICENCIAMIENTO DE LA SOLUCIÓN ENDPOINT SANDBLAST Y ADQUISICIÓN DE LICENCIAS VPN (PRESENTACIÓN DE OFERTA)	972-2020	20/11/2020	$ 44.772.500
https://community.secop.gov.co/Public/Tendering/ContractDetailView/Index?UniqueIdentifier=CO1.PCCNTR.1989609&AwardContractDetailId=842744&IsFromMarketplace=False&IsFromContractNotice=True&isModal=true&asPopupView=true#GenericContractInformation				
AGENCIA PARA LA INFRAESTRUCTURA DEL META	ADQUIRIR UN FW CON CAPACIDAD DE REALIZAR TÚNELES VPN SITIO A SITIO Y QUE SEA COMPLETAMENTE COMPATIBLE CON LA INFRAESTRUCTURA TECNOLÓGICA DE LA GOBERNACIÓN DEL META	0764 DE 2021	29/12/2021	$ 56.999.000
https://community.secop.gov.co/Public/Tendering/ContractDetailView/Index?UniqueIdentifier=CO1.PCCNTR.3140629&AwardContractDetailId=1711619&IsFromMarketplace=False&IsFromContractNotice=True&isModal=true&asPopupView=true#GenericContractInformation				

SOFTWARE HIPERVISOR DE MAQUINA VIRTUAL

ENTIDAD	OBJETO	NÚMERO DE CONTRATO	FECHA	VALOR
MINISTERIO DE HACIENDA Y CREDITO PUBLICO	Contratar el servicio de mantenimiento y soporte especializado para las plataformas de RedHat, Oracle Linux y de virtualización ORACLE VM implementados en el Ministerio de Hacienda y Crédito Público.	3.257-2019	17/06/2019	$ 26.316.096
https://community.secop.gov.co/Public/Tendering/ContractDetailView/Index?UniqueIdentifier=CO1.PCCNTR.995308&AwardContractDetailId=326122&IsFromMarketplace=False&IsFromContractNotice=True&isModal=true&asPopupView=true#GenericContractInformation				
POLICÍA NACIONAL - DIRECCIÓN ADMINISTRATIVA Y FINANCIERA	ADQUIRIR Y/O RENOVAR LICENCIA DE USO VMWARE PARA LA CONTRALORIA DE CUNDINAMARCA	025-2020	23/11/2020	$ 8.925.000
https://community.secop.gov.co/Public/Tendering/ContractDetailView/Index?UniqueIdentifier=CO1.PCCNTR.1990212&AwardContractDetailId=842541&IsFromMarketplace=False&IsFromContractNotice=True&isModal=true&asPopupView=true#GenericContractInformation				
DIRECCIÓN DE INTELIGENCIA POLICIAL	ADQUISICIÓN MEMORIA RAM, UNIDADES DE ESTADO SOLIDO Y LICENCIAS RED HAT ENTERPRISE VIRTUALIZATION PARA LA DIRECCIÓN DE INTELIGENCIA POLICIAL	PN DIPOL SA 037-2021	10/08/2021	$ 360.900.000
https://community.secop.gov.co/Public/Tendering/ContractDetailView/Index?UniqueIdentifier=CO1.PCCNTR.2706525&AwardContractDetailId=1408444&IsFromMarketplace=False&IsFromContractNotice=True&isModal=true&asPopupView=true#GenericContractInformation				

- **Información verificada y aprobada por los funcionarios dueños de la necesidad que firman el presente estudio previo.**

NOTA: para el presente estudio previo no se tendrá en cuenta los precios de referencia SECOP I y SECOP II, ya que difieren ostensiblemente del precio proyectado y condiciones técnicas.

5.2. PRECIOS HISTÓRICOS

ÍTEM	ENTIDAD CONTRATANTE Y CONTRATISTA	NÚMERO DE CONTRATO	DESCRIPCIÓN	VALOR UNITARIO	VALOR UNITARIO PROYECTADO CON IPC 3.80% 2019
1	FONDO ROTATORIO DE LA POLICA - ACCESAR SAS	CTO-262-6-2019	SERVICIO RENOVACIÓN LICENCIAMIENTO ANTIVIRUS PARA EL FONDO ROTATORIO DE LA POLICÍA	$ 52.816.365	$ 54.823.386,87
2	N/A	N/A	N/A	N/A	N/A
3	MINISTERIO DE HACIENDA Y CREDITO PUBLICO - PULXAR	3.257-2019	CONTRATAR EL SERVICIO DE MANTENIMIENTO Y SOPORTE ESPECIALIZADO PARA LAS PLATAFORMAS DE REDHAT, ORACLE LINUX Y DE VIRTUALIZACIÓN ORACLE VM IMPLEMENTADOS EN EL MINISTERIO DE HACIENDA Y CRÉDITO PÚBLICO.	$ 26.316.096	$ 27.316.107,65

ÍTEM	ENTIDAD CONTRATANTE Y CONTRATISTA	NÚMERO DE CONTRATO	DESCRIPCIÓN	VALOR UNITARIO	VALOR UNITARIO PROYECTADO CON IPC 1.61% 2020
1	CONTRALORIA DE CUNDINAMARCA - KAVANTIC SAS	021-2020	SOLUCIÓN SOFTWARE ANTIVIRUS, DATA LOST PREVENTION, CONTROL DE APLICACIONES, CIFRADO Y ANTISPAM	$ 20.935.075	$ 21.272.129,71
2	INSTITUTO DISTRITAL DE LA PARTICIPACIÓN Y ACCIÓN COMUNAL - SAFETY IN DEEP SAS	972-2020	MANTENIMIENTO Y RENOVACIÓN DE LICENCIAMIENTO DE LA SOLUCIÓN ENDPOINT SANDBLAST Y ADQUISICIÓN DE LICENCIAS VPN (PRESENTACIÓN DE OFERTA)	$ 44.772.500	$ 45.493.337,25
3	CONTRALORIA DE CUNDINAMARCA - REALTIME CONSULTING & SERVICES S.A.S	025-2020	ADQUIRIR Y/O RENOVAR LICENCIA DE USO VMWARE PARA LA CONTRALORIA DE CUNDINAMARCA	$ 8.925.000	$ 9.068.692,50

ÍTEM	ENTIDAD CONTRATANTE Y CONTRATISTA	NÚMERO DE CONTRATO	DESCRIPCIÓN	VALOR UNITARIO	VALOR UNITARIO PROYECTADO CON IPC 5.62% 2021
1	FONDO ROTATORIO DE LA POLICA - GRUPO MICROSISTEMAS COLOMBIA SAS	CO21000197-GAC	ADQUISICION DE LICENCIAS ANTIVIRUS	$ 30.000.000	$ 31.686.000,00
2	AIM - ADSUM SOLUCIONES TECNOLÓGICAS SAS	0764 DE 2021	ADQUIRIR UN FW CON CAPACIDAD DE REALIZAR TÚNELES VPN SITIO A SITIO Y QUE SEA COMPLETAMENTE COMPATIBLE CON LA INFRAESTRUCTURA TECNOLÓGICA DE LA GOBERNACIÓN DEL META	$ 56.999.000	$ 60.202.343,80
3	DIRECCIÓN DE INTELIGENCIA POLICIAL - ACONPIEXPRESS	04-2-10036-2021	ADQUISICIÓN MEMORIA RAM, UNIDADES DE ESTADO SOLIDO Y LICENCIAS RED HAT ENTERPRISE VIRTUALIZATION PARA LA DIRECCIÓN DE INTELIGENCIA POLICIAL	$ 360.900.000	$ 381.182.580,00

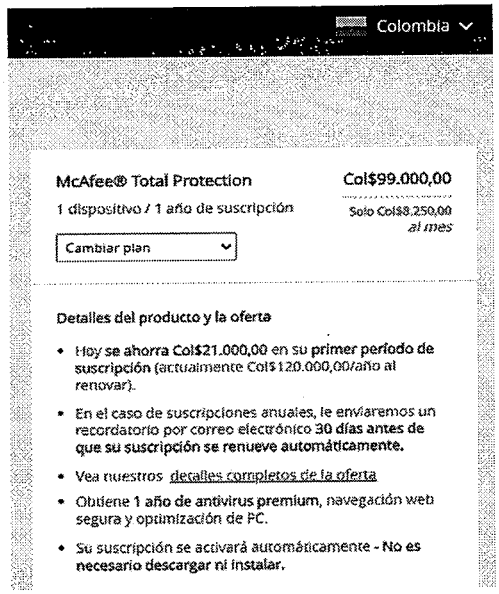
NOTA: para el presente estudio previo no se tendrá en cuenta los precios históricos proyectados, teniendo en cuenta que difieren en cuento a las especificaciones técnicas contratadas y las requeridas por la Dirección de Inteligencia Policial para el presente proceso.

- **Información verificada y aprobada por los funcionarios dueños de la necesidad que firman el presente estudio previo.**

5.3. PRECIOS DE CATÁLOGO O PORTALES WEB

Fue consultado por parte del estructurador del estudio previo el sitio o portal web de la empresa McAfee quien provee el software antivirus como se relaciona en la siguiente URL, así:

https://www.mcafee.com/consumer/es-co/landing-page/direct/sem/mtp-family/desktop/brand-ad.html?csrc=google&csrcl2=brand&cctype=[ES-CO][Search][Brand]%20McAfee&ccstype=&ccoe=direct&ccoel2=sem&pkg_id=521&affid=1485&culture=ES-CO&utm_source=google&utm_medium=SEM&utm_campaign=[ES-CO][Search][Brand]%20McAfee&utm_content=[brand][exact]%20mcafee&utm_term=mcafee&gclid=EAIaIQobChMI7-D1-bPh9gIV1O2zCh154g9VEAAYASAAEgKy6_D_BwE



BIEN O SERVICIO	FECHA	EMPRESA	VALOR
SOFTWARE ANTIVIRUS	24/03/2022	MCAFEE	$ 99.000

NOTA: teniendo en cuenta lo anterior, y atendiendo el valor por cada unidad de software antivirus, no se tendrán en cuenta para el análisis del valor estimado, toda vez que difieren de forma considerablemente respecto a los precios de mercado y supera el valor unitario presupuestado en el plan anual de adquisiciones para satisfacer la necesidad.

De igual forma se deja constancia que fue verificada la página de la Tienda Virtual del Estado Colombiano encontrando únicamente el hipervisor de máquina virtual con especificaciones técnicas diferentes y el valor de acuerdo al catálogo del acuerdo marco de precios CCE-139-IAD-2020 SOFTWARE POR CATÁLOGO, expone los precios en moneda extranjera, así mismo verificadas las páginas web de los fabricantes o comercializadores de los software objeto del presente estudio previo, la opción de compra es ofrecida en moneda extranjera, entonces por estas razones no serán relacionados ni tenidos en cuenta para el análisis del valor estimado.

- **Información verificada y aprobada por los funcionarios dueños de la necesidad que firman el presente estudio previo.**

5.4. PRECIOS DE MERCADO

El 17/03/2022 se publicó en el SECOP II el proceso SOLICITUD DE COTIZACION DIPOL-ARPIN-003, con el fin de estructurar el estudio de mercado para el presente proceso, el 23/03/2022 a las 10:30 a.m., fue la fecha límite para responder a la solicitud de información presentando respuesta tres empresas, como se relaciona a continuación, así:

ÍTEM	DESCRIPCIÓN	SOLUCUIONES – TECNOLOGÍA Y SERVICIO S. A	ONA SYSTEMS	MULTISOFT S.A.S	MENOR VALOR COTIZADO
1	SOFTWARE DE PAQUETE ANTIVIRUS	$ 4.200.000,00	$ 26.013.680,00	$ 4.199.829,90	$ 4.199.829,90
2	SOFTWARE CONGELADOR DE DISCO	$ 12.600.000,00	$ 31.699.150,00	$ 12.599.489,70	$ 12.599.489,70
3	SOFTWARE VPN	$ 31.500.000,00	$ 30.786.490,00	$ 31.498.724,60	$ 30.786.490,00
4	SOFTWARE DE HIPERVISOR DE MÁQUINA VIRTUAL	$ 51.600.000,00	$ 51.370.950,00	$ 51.697.906,20	$ 51.370.950,00
VALOR TOTAL		**$ 99.900.000,00**	**$ 139.870.270,00**	**$ 99.995.950,40**	**$ 98.956.759,60**

NOTA 1: *El bien objeto de adquisición se encuentra catalogado como exento, de acuerdo a lo dispuesto en el artículo 188 del decreto 1819 de 2016, que modifica el artículo 477 del Estatuto Tributario. Bienes que se encuentran exentos del impuesto, literal n) Equipos, software y demás implementos de sistemas y comunicaciones para uso de las Fuerzas Militares y la Policía Nacional. Atendiendo su naturaleza y destinación estos bienes se encuentran gravados a la tarifa 0

Nota 2: las cotizaciones relacionadas en el análisis de mercado se obtuvieron a través de una invitación a cotizar publicada en SECOP II.

- **Información verificada y aprobada por los funcionarios dueños de la necesidad que firman el presente estudio previo.**

5.5 ANÁLISIS DEL VALOR ESTIMADO

ÍTEM	DESCRIPCIÓN	PRECIO SECOP	PRECIOS DE CATÁLOGO	PRECIOS HISTÓRICOS PROYECTADOS	PRECIOS DE MERCADO	VALOR ESTIMADO
1	SOFTWARE PAQUETE ANTIVIRUS	NO APLICA	NO APLICA	NO APLICA	$ 4.199.829,90	$ 4.199.829,90
2	SOFTWARE DE CONGELADOR DE DISCO	NO APLICA	NO APLICA	NO APLICA	$ 12.599.489,70	$ 12.599.489,70

3	SOFTWARE VPN	NO APLICA	NO APLICA	NO APLICA	$ 30.786.490,00	$ 30.786.490,00
4	SOFTWARE DE HIPERVISOR DE MÁQUINA VIRTUAL	NO APLICA	NO APLICA	NO APLICA	$ 51.370.950,00	$ 51.370.950,00
VALOR TOTAL					$ 98.956.759,60	$ 98.956.759,60

- **Información verificada y aprobada por los funcionarios dueños de la necesidad que firman el presente estudio previo.**

5.6 VALOR ESTIMADO DE LA CONTRATACIÓN

El valor estimado del presente proceso es de NOVENTA Y OCHO MILLONES NOVECIENTOS CINCUENTA Y SEIS MIL SETECIENTOS CINCUENTA Y NUEVE MIL PESOS CON SESENTA CENTAVOS M/CTE ($ 98.956.759,60)

ITEM Y/O LOTE	RUBRO Y DESAGREGACIÓN PRESUPUESTAL	RECURSO	UNIDAD DE DESTINO	DESCRIPCIÓN	CANTIDAD	VALOR UNITARIO ESTIMADO EXENTO DE IVA	VALOR TOTAL ESTIMADO EXENTO DE IVA
1	02-01-01-006-002-03	10	DIPOL	SOFTWARE PAQUETE ANTIVIRUS	70	$ 59.997,57	$ 4.199.829,90
2	02-01-01-006-002-03	10	DIPOL	SOFTWARE DE CONGELADOR DE DISCO	70	$ 179.992,71	$ 12.599.489,70
3	02-01-01-006-002-03	10	DIPOL	SOFTWARE VPN	70	$ 439.807,00	$ 30.786.490,00
4	02-01-01-006-002-03	10	DIPOL	SOFTWARE DE HIPERVISOR DE MÁQUINA VIRTUAL.	30	$ 1.712.365,00	$ 51.370.950,00
						VALOR TOTAL ESTIMADO	$ 98.956.759,60

NOTA: *El bien objeto de adquisición se encuentra catalogado como exento, de acuerdo a lo dispuesto en el artículo 188 del decreto 1819 de 2016, que modifica el artículo 477 del Estatuto Tributario. Bienes que se encuentran exentos del impuesto, literal n) Equipos, software y demás implementos de sistemas y comunicaciones para uso de las Fuerzas Militares y la Policía Nacional. Atendiendo su naturaleza y destinación estos bienes se encuentran gravados a la tarifa 0

Teniente Coronel **Fernando Guzmán Ramos**
Jefe Área de Producción

Capitán **John Guevara Pulido**
Recolector de Información
Área Producción de Inteligencia

Documentos Anexos al Estudio Previo:

Los documentos seleccionados en la siguiente lista, aplican para el proceso de Mínima Cuantía cuyo objeto es "ADQUISICIÓN SOFTWARE DE ANTIVIRUS, CONGELADOR DE DISCO, HIPERVISOR DE MÁQUINA VIRTUAL Y VPN"

Aplica	**Anexos**
☐	Certificación de la necesidad
☐	Especificaciones técnicas mínimas
☐	Constancia de idoneidad y experiencia (No Aplica)
☐	Estimación, tipificación, asignación de riesgos y determinación de garantías
☐	Análisis del riesgo y forma de mitigarlo.
☐	Ficha técnica (No Aplica)
☐	Obligaciones de la policía nacional (No Aplica)
☐	Obligaciones del contratista (No Aplica)

Aplica	**Formularios adjuntos al estudio previo**
☐	Factores de verificación y ponderación. (No aplica)
☐	Apoyo a la industria nacional (No aplica)
☐	Indicación de trato nacional (No aplica)
☐	Experiencia del proponente (No aplica)
☐	Certificación de contratos para acreditación de experiencia proponente extranjero sin sucursal o domicilio en Colombia (No aplica)
☐	Clasificación proponente extranjero (No aplica)
☐	Acuerdo de confidencialidad (obligatorio)

- ☐ Capacidad financiera (No aplica)
- ☐ Certificación de compromiso del fabricante y/o oferente (No aplica)
- ☐ Certificación de la capacidad técnica (No aplica)
- ☐ Personal, experiencia y tiempos de dedicación mínimos (No aplica)
- ☐ Carta de compromiso postventa (No aplica)

Otros documentos adjuntos al Estudio Previo

Otros

- Acta comité Ambiental
- Acta comité Seguridad y Salud en el trabajo
- Acta comité tecnológico Oficina de Telemática DIPOL
- Concepto de Viabilidad por parte de la Oficina de Telemática DIPON
- Certificado Plan de Compras
- Cotizaciones

ELABORACION DE ESTUDIOS PREVIOS PARA CONTRATOS	POLICÍA NACIONAL
CERTIFICACIÓN DE LA NECESIDAD	

En mi calidad de Almacenista de Intendencia de la Dirección de Inteligencia Policial, manifiesto con la suscripción de esta CERTIFICACIÓN que consultado el Inventario de Bienes del almacén de la DIRECCIÓN DE INTELIGENCIA POLICAL no se cuenta con los softwares de antivirus, congelador de disco, hipervisor de máquina virtual y VPN, por lo cual se hace necesario adquirir los softwares en mención

Por tal razón la única forma de resolver la necesidad es mediante la contratación de los elementos relacionados en este estudio.

ÍTEM	CÓDIGO SAP SILOG	TALLA	DESCRIPCIÓN	NECESIDAD REAL	EXISTENCIA ALMACÉN VESTUARIO	CANTIDAD ADQUIRIR	DÉFICIT %
1	1023300	No aplica	SOFTWARE DE ANTIVIRUS	70	0	70	100%
2	1023300	No aplica	SOFTWARE CONGELADOR DE DISCO	70	0	70	100%
3	1023300	No aplica	SOFTWARE VPN	70	0	70	100%
4	1023300	No aplica	SOFTWARE HIPERVISOR DE MÁQUINA VIRTUAL	70	0	30	100%

Intendente Jefe **JORGE ARMANDO JURADO PAREDES**
Almacenista de Intendencia Policial

ELABORACION DE ESTUDIOS PREVIOS PARA CONTRATOS	POLICÍA NACIONAL
ESPECIFICACIONES TÉCNICAS MÍNIMAS	

ÍTEM	CONDICIONES TÉCNICAS MÍNIMAS	CUMPLE	NO CUMPLE
1	**SOFTWARE DE ANTIVIRUS** **Marca: especificar por el oferente** **Referencia: especificar por el oferente**		
1.1	Se requieren el software de antivirus para setenta (70) equipos de cómputo, con las siguientes funcionalidades:		
1.2	El antivirus debe contar con un mecanismo de actualización frecuente de antimalware que garantice la integridad y minimice la manipulación o alteración de las definiciones de virus por medio de cifrado y firmas digitales.		
1.3	El antivirus debe permitir el acceso en demanda, en segundo plano, proactivo, sub-sistema de prevención de brotes de virus, análisis de phishing y filtrado de contenido, protección sobre los protocolos HTTP, HTTPS, FTP.		
1.4	La solución debe analizar tipo de archivo verdadero y eliminar si da el caso, archivos ejecutables con extensiones como: *.EXE, *.APP, *.VB, *.VBS, *.SCR, *.BAT, *.DLL, *.COM, *.BIN, *.EBS., entre otros que aprovechan los diferentes tipos de extensiones de un sistema operativo, camuflándose para afectar a los sistemas.		
1.5	La solución debe ejecutar detección de archivos con base al tipo y no solo a la extensión.		
1.6	Debe anticiparse a los virus desconocidos e intrusos mediante herramientas que supervisen los procesos en ejecución en busca de comportamientos maliciosos.		
1.7	Escanee sitios Web en busca de código malicioso; Control y Protección Web.		
1.8	Compruebe la reputación de los vínculos antes de navegar en ellos.		
1.9	Detecte y bloquee los vínculos de phishing que intentan robar información confidencial y datos financieros.		
1.10	Reconocimiento de anomalías, detección y bloqueo de ataques de tipo Host Sweep, TCP o UDP port Scan, CGI Holes.		
1.11	Utiliza técnicas de análisis avanzadas para comprobar si un sitio presenta las características típicas de las operaciones de phishing.		
1.12	La solución de antivirus debe soportar la instalación de los agentes en estaciones de trabajo, portátiles y equipos de cómputo. Así como garantizar la compatibilidad en los dispositivos mencionados.		
1.13	La protección antivirus debe tener compatibilidad con sistemas operativos Windows y Mac.		
1.14	La solución permite el monitoreo en tiempo real de los procesos en memoria para capturar los virus que son ejecutados en memoria sin necesidad de escribir el archivo.		
1.15	El módulo de comportamiento debe ser capaz de detectar amenazas de día cero tipo Ransomware		
1.16	Detección y reacción contra Ransomware que inicie el cifrado de información, así no se tenga firma de detección de malware para detenerlo. Este módulo debe terminar el proceso de cifrado malicioso de forma automática.		
1.17	Protección contra la explotación permitiendo finalizar programas que se identifiquen con comportamiento anormal asociado a ataques de Exploit.		
1.18	Evitar o monitorear que un programa con comportamiento sospechoso pueda duplicar o inyectar archivos.		
1.19	Evitar o monitorear que un programa con comportamiento sospechoso pueda incrustar complementos en los navegadores.		
1.20	Evitar o monitorear que un programa con comportamiento sospechoso pueda instalar librería del programa malicioso.		
1.21	Para aquellos programas válidos y que por su comportamiento el Antimalware no permita su ejecución, deberá de permitirlos agregándolos a una lista blanca.		
1.22	Detección del malware en pre-ejecución y comprobar el comportamiento malicioso para detectar malware desconocido.		
1.23	Debe realizar la verificación de todos los archivos accedidos en tiempo real, incluso durante el proceso de arranque.		
1.24	Debe realizar la limpieza del sistema automáticamente, eliminando elementos maliciosos detectados y aplicaciones potencialmente indeseables (PUA).		
1.25	Debe proteger las funciones críticas en los navegadores de Internet (Safe Browsing).		
1.26	Debe permitir la autorización de detecciones maliciosas y excluir de la exploración de directorios y archivos específicos.		
1.27	Se requiere protección integrada, es decir, en un solo agente, contra amenazas de seguridad, incluyendo las potencialmente no deseadas (PUA).		
1.28	Permitir la utilización de contraseña de protección para posibilitar la reconfiguración local en el cliente y desinstalación de los componentes de protección.		
1.29	Debe poseer la capacidad de bloqueo de ataques basado en la explotación de vulnerabilidad conocida.		

1.30	Debe ser capaz de aplicar un análisis adicional, inspeccionando finamente el comportamiento de los códigos durante la ejecución, para detectar el comportamiento sospechoso de las aplicaciones, tales como desbordamiento de búfer.		
1.31	Debe prevenir el ataque de vulnerabilidades de navegador a través de web exploits.		
1.32	Debe brindar protección de amenazas de día cero (0) a través de tecnología de deep learning (signature less).		
1.33	Debe tener la funcionalidad de detección de amenazas desconocidas que están en memoria con tecnología de Deep Learning.		
1.34	Debe tener la capacidad de detección y bloqueo proactivo de keyloggers y otros malwares no conocidos (ataques de día cero) a través del análisis de comportamiento de procesos en memoria.		
1.35	Debe tener la capacidad de detección y bloqueo de Trojans y Worms, entre otros malwares, por comportamiento de los procesos en memoria.		
1.36	Debe detectar el malware en pre-ejecución un tiempo aproximado de no más de 20 milisegundos.		
1.37	No debe requerir descarga de firmas de ningún tipo para la parte de protección por comportamiento.		
1.38	Debe tener la capacidad de analizar el comportamiento de nuevos procesos al ser ejecutados, en complemento a la exploración programada.		
1.39	Debe contar con bloqueo y protección contra amenazas desconocidas potencialmente sospechosas (PUA).		
1.40	Se debe garantizar la generación de excepciones ante falsos positivos.		
1.41	El software debe tener la capacidad de protección AMSI contra scripts maliciosos.		
1.42	El software debe poseer un IPS de Host.		
1.43	El software debe disponer de capacidad de protección contra ransomware no basada exclusivamente en la detección por firmas.		
1.44	El software debe disponer de capacidad de remediación de la acción de encriptación maliciosa del ransomware.		
1.45	El software a instalar en equipos de cómputo debe disponer de capacidad de prevención contra la acción de cifrado malicioso ejecutado por ransomware, posibilitando el bloqueo de las computadoras de donde parte tal acción.		
1.46	El software debe contar con protección anti-ransomware para el sector de booteo.		
1.47	El software debe restaurar automáticamente los archivos cifrados por un proceso malicioso de ransomware.		
1.48	Detección y protección de técnicas de explotación: Enforce Data Execution Prevention; Mandatory Address Space Layout Randomization; Bottom-up ASLR; Null Page (Null Deference Protection); Heap Spray Allocation; Dynamic Heap Spray; Stack Pivot; Stack Exec (MemProt); Stack-based ROP Mitigations (Caller); Branch-based ROP Mitigations (Hardware Assisted); Structured Exception Handler Overwrite (SEHOP); Import Address Table Filtering (IAF); Load Library; Reflective DLL Injection; Shellcode; VBScript God Mode; Wow64; Syscall; Hollow Process; DLL Hijacking; Squiblydoo Applocker Bypass; APC Protection (Double Pulsar / AtomBombing);		
1.49	El software debe garantizar la mitigación de inyección de códigos en procesos.		
1.50	El software debe garantizar la protección contra robo de credenciales.		
1.51	El software debe garantizar la protección contra malware escondido en aplicaciones legitimas (code cave).		
1.52	El software debe evitar la migración de procesos maliciosos, evitando que un proceso malicioso migre a otro.		
1.53	El software debe evitar la escalada de privilegios y acceso elevado a recursos.		

1.54	El software debe evitar la modificación de las claves de registro para la ejecución de código arbitrario.		
1.55	El software debe cumplir con todos los ítems anteriores que apliquen a estaciones de trabajo bajo S.O. Windows.		
1.56	El antivirus debe tener la capacidad de analizar Scripts de Java y VBScript antes de que se ejecuten.		
1.57	El software debe controlar las actividades realizadas por aplicaciones vulnerables.		
1.58	El antivirus debe contar con tecnología de remoción y detección de virus, macros infecciosas, troyanos, gusanos informáticos, Keyloggers, Spyware y adware, Rootkits, Bots y otras amenazas. Mitigar ataques y neutralizar los objetos maliciosos por medio de tecnologías de desinfección a niveles bajos del sistema operativo de un equipo.		
1.59	El antivirus deberá ser estable, de tal manera que no afecte ni perjudique el rendimiento de las máquinas y/o aplicativos que estén instalados en las mismas.		
1.60	El antivirus debe contar y quedar configurado con un módulo de exploración en tiempo real, que ofrezca protección continúa frente a los virus que llegan a través de dispositivos de almacenamiento extraíbles, en la red y de las diversas fuentes en Internet.		
1.61	El antivirus debe tener la capacidad de explorar los procesos maliciosos que se encuentren corriendo en memoria.		
1.62	El antivirus debe correr con un recurso de CPU bajo para tareas de exploración en demanda		
1.63	El antivirus debe permitir y quedar configurado para tareas calendarizadas de revisión y limpieza del sistema de archivos.		
1.64	El software de antivirus debe poseer mecanismos o técnicas como buffer overflows que sirven como protección contra vulnerabilidades en memoria.		
1.65	El software debe consumir recursos mínimos de máquina.		
1.66	El software debe permitir en su configuración la exclusión del análisis de extensiones o ficheros no deseados. Esto desde su configuración local protegida por una contraseña.		
1.67	El antivirus debe explorar archivos descargados desde todas las plataformas de correo, análisis de Onedrive y/o de almacenamiento en la nube instalados por aplicaciones como Dropbox, Drive Gmail a las cuales se tiene acceso desde las estaciones de trabajo.		
1.68	El antivirus debe contar con un módulo de exploración bajo demanda que, permita iniciar una exploración en cualquier momento, especificar los objetivos (discos duros, carpetas, memoria, unidades extraíbles) y las exclusiones de la exploración, así como también determinar cómo debe responder el explorador cuando detecte un virus mostrando el informe detallado.		
1.69	El software debe garantizar un análisis por demanda en los dispositivos extraíbles y almacenamiento en línea, antes de tener acceso a ellos una vez conectados a los equipos de cómputo.		
1.70	El software debe garantizar la detección de ataques de tipo Exploits hacia vulnerabilidades de sistema operativo como también de aplicaciones diferentes de Microsoft.		
1.71	El software debe proporcionar un módulo de bloqueo de aplicaciones para proporcionar un mayor nivel de protección, seguridad y control a los usuarios.		
1.72	El antivirus deberá permitir la desactivación del agente por medio de una contraseña, en caso de que se requiera o necesite.		
1.73	El software deberá entregar contexto de la amenaza detectada mediante la visualización de todo el ataque, como inicio y como se comportó. Debe proveer detalle de los equipos involucrados en el ataque tales como llaves de registro, procesos y conexiones de red.		
1.74	El software debe proveer respuesta automática a incidentes como actividades de limpieza del endpoint hasta obtener su estado de salud original.		
1.75	El software debe explorar múltiples formatos de compresión de archivos como: (zip, rar, tar, gzip entre otros).		
1.76	El software debe tener la capacidad de explorar los procesos que se encuentren corriendo en memoria.		
1.77	El software debe ser capaz de detectar y bloquear ataques de fileless basados en PowerShell, Windows Management Instrumentations (WMI), VBScript y System Exploits para las plataformas cliente y servidores soportadas por Microsoft.		
1.78	El software debe ser capaz de retornar el sistema a un estado saludable, mediante técnicas de remediación de archivos que eventualmente puedan llegar a ser modificados durante la ejecución de una amenaza.		
1.79	El motor de exploración del software deberá utilizar distintas tecnologías de detección de virus: Exploración de firmas y exploración heurística "busca patrones de comportamiento de virus conocidos para la detección de virus desconocidos".		
1.80	El software debe permitir la toma de decisiones correctas sobre la ejecución de archivos y personalizar las directivas o políticas, en función del nivel de tolerancia al riesgo.		
1.81	El software debe tener soporte para comunicaciones bajo IPv6		
1.82	El software debe avisar sobre los posibles conflictos que existan con otros de antivirus y firewall instalados previamente en la máquina.		

1.83	El software debe poder restringir completa o parcialmente el acceso a la consola cliente para configurar parámetros individuales sobre el host.		
1.84	El software debe permitir configurar idioma dentro de la aplicación, entre ellos idioma español.		
1.85	El software debe poder configurar acciones sobre infecciones identificadas: Denegar acceso / limpiar / Eliminar / Ninguna.		
1.86	El software debe ofrecer opciones de envío de infecciones a cuarentena y ejecutar acciones sobre ítems enviados allí.		
1.87	El software debe poder habilitar la opción de escaneo de clic-derecho sobre carpetas específicas en sistemas operativos soportados.		
1.88	El software debe contar con características de protección para navegadores web (Active X) o detecciones que se realicen por comportamiento.		
1.89	El software debe permitir la detección basada en el comportamiento anómalo en el punto final.		
1.90	El software debe emplear una arquitectura multicapa, para defenderse de ataques basados en comportamientos, evitando cambios a nivel de sistema, restringiendo el acceso a procesos, archivos, recursos compartidos, valores y claves de registro específicos.		
1.91	El software debe poder identificar patrones similares de comportamiento dentro de diferentes variantes, usando reglas que pueden configurarse para evitar la instalación y / o la carga de nuevas variantes históricas, actuales y en evolución de amenazas de día cero.		
1.92	El software debe ser compatible con todas las versiones de los navegadores Internet Explorer, Google Chrome, Mozilla Firefox.		
1.93	El software debe garantizar en las estaciones de trabajo protección contra infecciones a través descargas de internet, archivos adjuntos de e-mail, redes, archivos compartidos, CD-ROM, USB, dispositivos extraíbles, carpetas públicas y carpetas personales de todo tipo de correo, almacenadas localmente, mensajes de correo electrónico entrante y saliente, servicios en línea, entre otros tipos de almacenamiento.		
1.94	El software debe ser capaz de detectar el 100% de los virus conocidos (reportados en listas), contra programas malignos especificados.		
1.95	El software debe contar con mecanismos de borrado seguro de malware residentes en memorias que sean difíciles de erradicar, evitando el reinicio, en caso de no contar con la herramienta, deberá prever que el técnico experto en antimalware esté presente en el reinicio del equipo de cómputo verificando y garantizando la erradicación del mismo.		
1.96	El software debe contar con tecnología de mitigación de EXPLOITS, que ataquen soluciones comúnmente usadas y que pueden no estar actualizadas, como Acrobat, Flash Player, entre otras.		
1.97	El software debe contar con mecanismos de detección de ausencia de configuraciones y/o parches específicos de sistema operativo.		
1.98	El software debe ofrecer una solución para controlar dispositivos en sistemas operativos Windows (32/64 bits).		
1.99	El software debe permitir la limpieza de amenazas dentro archivos adjuntos (JavaScript dentro de archivos PDF o Microsoft Word, por ejemplo).		
2	**SOFTWARE CONGELADOR DE DISCO** **Marca: especificar por el oferente** **Referencia: especificar por el oferente**		
2.1	Se requieren software de congelar discos para setenta (70) equipos de cómputo, con las siguientes funcionalidades:		
2.2	El contratista debe proveer el software permita protección avanzada para estaciones de trabajo de sistema operativo Windows 7, 8 a 10 en sus últimas versiones estables. La cual debe garantizar que se preserve la configuración, actualizaciones del sistema operativo (Update) y base de datos de antivirus.		
2.3	El software debe garantizar que cada vez que se reinicie el equipo el software debe restaurar la configuración.		
2.4	El software debe proporcionar a los usuarios un acceso ilimitado a los cambios de configuración permanentes.		
2.5	El software debe evitar los cambios de configuración, permitiendo a los usuarios guardar su trabajo sin que se altere la configuración de base de los equipos.		
2.6	El software debe garantizar la eliminación de las amenazas de día cero, garantizando reversar todos los cambios maliciosos realizados en el sistema, incluidas las amenazas día cero.		
2.7	El contratista debe garantizar que el software no degrade el rendimiento de los equipos.		
2.8	El software debe garantizar la eliminación de todo el software instalado sin autorización, al momento de reiniciar el equipo.		
2.9	El software debe permitir el reinicio sin borrado de la configuración y un reinicio borrando la configuración del equipo.		
2.10	El software debe garantizar el 100 % de recuperación de las estaciones de trabajo al reiniciar.		
2.11	El software debe proporcionar la protección con contraseña y seguridad completa para el acceso a la configuración.		

2.12	El software debe proteger el registro de arranque maestro (MBR), los múltiples discos duros y particiones del equipo.		
2.13	El software debe admitir discos duros SCSI, ATA, SATA e IDE.		
2.14	El software debe admitir discos FAT, FAT32, NTFS, básicos y dinámicos.		
2.15	El software debe permitir preseleccionar unidades a congelar y, de forma selectiva, cuáles deben ser congeladas o descongeladas unidades fijas.		
2.16	El software debe tener la opción de instalación silenciosa para una conexión rápida como parte de una imagen maestra o implementación por demanda.		
2.17	Creación de ThawSpaces visibles u ocultos en una estación de trabajo para almacenar programas, guardar archivos o realizar cambios permanentes.		
3	**SOFTWARE VPN** **Marca: especificar por el oferente** **Referencia: especificar por el oferente**		
3.1	Se requieren el software VPN de EndPoint para setenta (70) equipos de cómputo, con las siguientes funcionalidades:		
3.2	El software debe proporcionar a los usuarios la conexión a sus dispositivos a través de ubicaciones de servidores iguales o mayores a 60 países.		
3.3	El software de VPN no debe recopilar ni compartir datos privados, y por ningún motivo hacer seguimiento de ellos. De igual forma no debe registrar datos de tráfico o solicitudes a DNS		
3.4	El software de VPN no debe realizar control del ancho de banda. Este debe garantizar un ancho de banda ilimitado.		
3.5	El software de VPN debe garantizar el enmascaramiento de la dirección IP en todo momento.		
3.6	El software de VPN debe contar con Kill Switch automático. Lo que significa que, si se bloquea accidentalmente una conexión VPN, la función Kill Switch impide que tu dispositivo acceda a la web., mediante el bloqueo de tráfico en internet hasta su restauración.		
3.7	El software de VPN actuará como un proxy, para su actividad web: en lugar de la dirección IP y ubicaciones reales, las páginas web que se vayan a visitar solo verán la dirección IP y la ubicación del servidor VPN.		
3.8	El software de VPN garantizará la protección a la conexión entre el cliente y el servidor utilizando tunelización y cifrado (protocolo AES- 256 bits)		
3.9	El software de VPN debe garantizar como mínimo los siguientes protocolos: IKEv2, L2TP/IPsec, OpenVPN, Lightway.		
3.10	El software de VPN debe contar con soporte 7x24 con chat en vivo.		
3.11	El software de VPN debe permitir el cambio ilimitado de servidores de conexión.		
3.12	El software de VPN debe operar son sus propios DNS, los cuales deben manejar tráfico cifrado.		
3.13	El software de VPN debe brindar protección de fugas de DNS y WebRTC.		
3.14	El software debe brindar un informe de errores, test de velocidad y la opción de escoger el más rápido.		
3.15	El software de VPN debe poseer la opción de evitar la detección de la dirección IPv6 mientras se esté conectado.		
4	**SOFTWARE DE HIPERVISOR DE MAQUINA VIRTUAL** **Marca: especificar por el oferente** **Referencia: especificar por el oferente**		
4.1	Se requieren el software hipervisor de máquina virtual para treinta (30) equipos de cómputo, con las siguientes funcionalidades:		
4.2	Soporte básico por un año de suscripción.		
4.3	El software hipervisor deberá permitir crear máquinas virtuales hasta de 16 CPU, 64 GB de RAM, 3 GB de vRAM).		
4.4	Posibilidad de crear VM restringidas con fecha y hora de caducidad predefinidas.		
4.5	El software hipervisor de máquina virtual deberá tener compatibilidad con DirectX 11 y gráficos 3D acelerados con OpenGL 4.1, una nueva interfaz de usuario con modo oscuro, compatibilidad con el modo Hyper-V de Windows en hosts Windows 7, Windows 10, y las últimas versiones estables en el mercado.		
4.6	El software hipervisor de máquina virtual deberá permitir: Crear nuevas máquinas virtuales. Convertir PC en máquina virtual.		
4.7	El software hipervisor de máquina virtual deberá tener integración de host/invitado: Uso compartido de archivos de host/invitado. Carpetas compartidas/reflejadas. SSH de un solo clic a máquina virtual Linux. Ejecutar máquinas virtuales con distintos modos de visualización. Modo de visualización unificado (solo para sistemas Windows invitados).		
4.8	El software hipervisor de máquina virtual deberá tener compatibilidad con:		

	Compatibilidad con una amplia gama de dispositivos virtuales. Compatibilidad con lector de tarjetas inteligentes USB. Compatibilidad con dispositivos USB 3.1 Compatibilidad con dispositivos de asistencia. Dispositivo de módulo de plataforma segura virtual. Dispositivo NVMe virtual.		
4.9	El software hipervisor de máquina virtual deberá tener funciones de seguridad como: Compatibilidad con seguridad basada en la virtualización de Microsoft (invitado). Módulo de plataforma segura virtual (vTPM). Compatibilidad con arranque UEFI. Compatibilidad con arranque seguro UEFI. Procesador de gráficos en el entorno de pruebas de la GPU Instantánea. Crear y gestionar máquinas virtuales cifradas.		
4.10	El software hipervisor de máquina virtual deberá tener funciones específicas de host Windows: Host de Windows 10. Motor de representación DX12. Compatibilidad con el modo Hyper-V (Device Guard, WSL). Compartir máquina virtual (servidor de Workstation).		
4.11	El software hipervisor de máquina virtual deberá tener Funciones avanzadas: Operación desde la línea de comandos: vmrun y VIX. Personalización de redes virtuales (NAT, cambio de nombre de red). Simulación de redes virtuales (pérdida de paquetes, latencia, ancho de banda). Conectar con el servidor ESXi. Creación de clones asociados. Creación de clones completos. Cifrar máquinas virtuales.		
4.12	El software hipervisor de máquina virtual deberá tener version comercial y de prueba.		
4.13	El sistema debe contar con un soporte y actualizaciones por un periodo mínimo de 1 año.		
4.14	El software hipervisor de máquina virtual deberá ser la última versión disponible por el fabricante y en el evento que el fabricante genere nuevas actualizaciones o versiones, el proveedor deberá suministrar el licenciamiento para ejecutar la última versión disponible y estable del hipervisor de máquina virtual.		
4.15	El contratista deberá entregar una certificación directamente emitida por el fabricante, en donde conste que el software adquirido por la entidad tiene suscripción de uso por el término de (1) año contado a partir de la entrega del software al supervisor del contrato.		
4.16	El contratista deberá garantizar que las mejoras de software a nuevas versiones (más recientes), releases y parches, entre otros, son de una versión igual o superior a las últimas versiones liberadas por la casa matriz en el mercado colombiano.		
4.17	El contratista deberá hacer entrega del software objeto del contrato, previa suscripción del acta de inicio y durante el plazo de ejecución del contrato.		
5	SERVICIOS DE IMPLEMENTACIÓN		
5.1	Los softwares ofertados deberán ser instalados, configurados y puestos en funcionamiento en las instalaciones de la Dirección de Inteligencia Policía ubicada en la Av. Boyacá 142ª 55 por el contratista		
6	ASISTENCIA TÉCNICA Y GARANTÍA		
6.1	El contratista deberá brindar soporte técnico de los softwares por un periodo de un año, contado a partir de la firma del recibido a satisfacción del supervisor del contrato por concepto de los softwares, donde se certifique la entrega de los softwares adquiridos mediante el presente proceso contractual.		
6.2	El servicio de soporte debe ser telefónico/sitio web y darse directamente por el contratista para todos los niveles de prioridad de los incidentes, problemas, inquietudes, dudas que se reporten durante el término de vigencia del contrato.		
6.3	En caso de existir urgencia respecto a incidentes que involucren las soluciones ofertadas, el contratista deberá proporcionar en caso de necesitarlo apoyo de casa matriz (presencial) hasta solucionar el incidente.		
6.4	El soporte de los softwares será 7x24 con un tiempo de respuesta no superior a 2 horas por parte del contratista. Los softwares deben contar con un soporte que permita accesos directos a los especialistas de producto cuando sea requerido por los diferentes medios de atención por parte de la dirección de inteligencia policial.		
7	TRANSFERENCIA DE CONOCIMIENTOS		
7.1	El contratista deberá incluir una transferencia de conocimientos de cuatro (4) horas virtuales, para dos (2) funcionarios, en el manejo, instalación y operación del software de antivirus, congelador de disco, hipervisor de máquina virtual y red privada virtual (VPN).		
8	ASPECTOS DE CONFIDENCIALIDAD		

8.1	El personal que realice la instalación y configuración de los productos ofertados deberá someterse a un estudio de seguridad realizado por la Dirección de Inteligencia de la Policía Nacional, durante la vigencia del contrato.		
8.2	En virtud del presente estudio previo, el contratista se obliga a no suministrar información que obtenga o conozca con ocasión de la ejecución del presente contrato; así como sobre los lugares a los cuales tenga acceso con ocasión de su desarrollo. El oferente deberá diligenciar el formulario acuerdo de confidencialidad.		
8.3	La Dirección de Inteligencia Policial de la Policía Nacional - DIPOL se reserva el derecho de hacer las verificaciones que considere necesarias en la documentación presentada, con el fin de garantizar la transparencia del proceso de contratación.		
9	**NIVEL EDUCATIVO**		
9.1	El funcionario que realizará la instalación y configuración de los softwares, deberán ostentar el título de tecnólogo o ingeniero en Sistemas y/o Electrónico y/o a fines, para lo cual el oferente deberá presentar con la oferta, copia del diploma y/o acta de grado del título de dicho funcionario		
9.2	La Dirección de Inteligencia Policial de la Policía Nacional – DIPOL podrá solicitar el cambio del personal ofrecido en cualquier momento a partir de la suscripción del contrato y el mismo podrá ser sustituido por el proponente por uno con iguales o mejores capacidades, condiciones y calificaciones a las presentadas en la oferta.		
10	**EXPERIENCIA DEL PERSONAL**		
10.1	Con el fin de garantizar la idoneidad del funcionario encargado de las actividades de instalación, configuración de los software de antivirus, congelador de discos, hipervisor de máquina virtual, red privada virtual (VPN) e hipervisor de máquina virtual ofertada, el proponente deberá certificar que esta persona cuente con experiencia en Colombia de haber participado mínimo en un (1) proyecto relacionado con el objeto del presente contrato; para lo cual el oferente debe anexar a la propuesta, una (1) certificación de proyectos en los cuales haya participado, expedidas por el oferente, durante los últimos tres (3) años anteriores a la fecha de apertura del presente proceso.		
11	**DOCUMENTACIÓN TÉCNICA – ENTREGABLES**		
11.1	El contratista debe entregar los manuales de uso en idioma español.		
11.2	Toda la documentación debe entregarse en idioma español.		
12	**EXPERIENCIA DEL OFERENTE**		
12.1	Con el fin de garantizar la calidad de los bienes a contratar y evitar incumplimientos en la ejecución del futuro contrato, se requiere acreditar experiencia en la venta software similares al objeto del presente estudio previo, tal acreditación será avalada con la presentación de certificaciones que acrediten la participación en contratos suscritos en los últimos tres (03) años (2019 y/o 2020 y/o 2021) con empresas públicas o privadas para lo cual el oferente deberá presentar máximo tres (03) certificaciones expedidas por la entidad que adquirió los software, con concepto favorable de la recepción de los servicios cuya suma o valor individual sea igual o superior al 100% del presupuesto oficial asignado.		
13	**REQUERIMIENTOS AMBIENTALES**		
13.1	El contratista deberá entregar los manuales de manera digital con el fin de aportar a la política de cero papeles establecida en directiva presidencial 04/2012.		
14	**SISTEMA DE GESTIÓN DE SEGURIDAD Y SALUD EN EL TRABAJO**		
14.1	El contratista aplicará el protocolo de bioseguridad establecido en la Dirección de Inteligencia Policial, teniendo en cuenta lo establecido por el Ministerio de Salud y Protección Social, a través de la Resolución 0000223 del 25/02/2021 "Por medio de la cual se modifica la Resolución 000666 del 24l04/2020 en sentido de sustituir el anexo técnico" y la Resolución 777 del 02/07/.2021 "Por la cual se definen los criterios y condiciones para el desarrollo de las actividades económicas, sociales y del estado y se adopta el protocolo de bioseguridad para la ejecución de estas".		
14.2	El contratista deberá entregar los documentos que evidencien objetivamente, la afiliación a la Seguridad Social Integral del personal que ejecutará el objeto contractual, (E.P.S., A.F.P., A.R.L., C.C.F.), obligándose a mantener dicha afiliación, durante la totalidad del tiempo necesario para la ejecución de la actividad contratada.		
14.3	El contratista correrá con los gastos médicos, de hospitalización y procedimientos médicos a que haya a lugar, en caso de que uno de sus funcionarios sufra un accidente laboral durante la ejecución del presente contrato.		
14.4	En caso de presentarse un accidente de trabajo dentro de las instalaciones de la Dirección de Inteligencia, le corresponde al contratista realizar el respectivo reporte e investigación dentro del tiempo reglamentario, presentará una copia de la documentación al Grupo de Seguridad y Salud en el Trabajo de la Dirección de Inteligencia Policial, según lo establecido en la Resolución 1401 del 14 mayo de 2007 o cualquiera que la modifique, reemplace o sustituya.		
14.5	El contratista deberá colaborar en las auditorias de cumplimiento al Sistema de Gestión de Seguridad y Salud en el Trabajo, que se realicen en el centro de trabajo donde se encuentre desempeñando las actividades		

Teniente Coronel **Fernando Guzmán Ramos**
Jefe Área de Producción

Capitán **John Guevara Pulido**
Recolector de Información
Área Producción de Inteligencia

GARANTÍAS DEL PROCESO

ETAPA PRECONTRACTUAL

MECANISMO DE COBERTURA	CLASE DE RIESGO	TIPIFICACIÓN DE LOS RIESGOS	ESTIMACIÓN DEL RIESGO	ASIGNACIÓN DEL RIESGO	VIGENCIA	JUSTIFICACIÓN COBERTURA / VIGENCIA
GARANTIA DE SERIEDAD	RIESGO JURIDICO	LA NO SUSCRIPCION DEL CONTRATO SIN JUSTA CAUSA	DIEZ POR CIENTO (10%) DEL MONTO DEL PRESUPUESTO OFICIAL.	PROPONENTE SELECCIONADO	DESDE LA PRESENTACION DE LA OFERTA Y POR CUATRO (4) MESES MAS.	AMPARA LA NO SUSCRIPCIÓN DEL CONTRATO SIN JUSTA CAUSA POR EL DIEZ POR CIENTO (10%) DEL PRESUPUESTO OFICIAL DESDE LA PRESENTACIÓN DE LA OFERTA Y POR CUATRO (4) MESES MÁS.
	RIESGO JURIDICO	LA NO AMPLIACION DE LA VIGENCIA DE LA GARANTIA DE SERIEDAD DE OFERTA CUANDO EL TERMINO PREVISTO EN LA INVITACION PARA LA ADJUDICACION DEL CONTRATO SE PRORROGUE O CUANDO EL TERMINO PREVISTO PARA LA SUSCRIPCION DEL CONTRATO SE PRORROGUE SIEMPRE Y CUANDO ESAS PRORROGAS NO EXCEDAN UN TERMINO DE CUATRO MESES.				
	RIESGO JURIDICO	LA FALTA DE OTORGAMIENTO POR PARTE DEL PROPONENTE SELECCIONADO DE GARANTIA DE CUMPLIMIENTO EXIGIDA POR LA ENTIDAD PARA AMPARAR EL INCUMPLIMIENTO DE LAS OBLIGACIONES DEL CONTRATO.				
	RIESGO JURIDICO	EL RETIRO DE LA OFERTA DESPUES DE VENCIDO EL TERMINO FIJADO PARA LA PRESENTACION DE LAS OFERTAS.				

ETAPA CONTRACTUAL

MECANISMO DE COBERTURA	CLASE DE RIESGO	TIPIFICACIÓN DE LOS RIESGOS	ESTIMACIÓN DEL RIESGO	ASIGNACIÓN DEL RIESGO	VIGENCIA	JUSTIFICACIÓN COBERTURA / VIGENCIA
GARANTIA UNICA	RIESGO JURIDICO	INCUMPLIMIENTO DEL CONTRATO	VEINTE POR CIENTO (20%) DEL VALOR DEL CONTRATO	CONTRATISTA	VIGENTE POR UN TERMINO IGUAL AL PLAZO DE EJECUCIÓN DEL CONTRATO Y (4) CUATRO MESES MAS.	AMPARA EL RIESGO DE INCUMPLIMIENTO DURANTE EL PLAZO DE EJECUCIÓN Y LIQUIDACION DEL CONTRATO LA ESTIMACION DEL RIESGO CUBRE EL 20% DEL VALOR DEL CONTRATO COMO QUIERA QUE SE PRETENDE EL PAGO PARCIAL O DEFINITIVO DE LOS PERJUICIOS QUE CAUSE A LA ENTIDAD EN LOS MISMOS TERMINOS DE LA CLAUSULA PENAL PECUNIARIA.
GARANTÍA ÚNICA	RIESGO OPERATIVO	CALIDAD DE LOS ELEMENTOS	CINCUENTA POR CIENTO (50%) DEL VALOR DEL CONTRATO	CONTRATISTA	VIGENTE POR UN TERMINO IGUAL AL PLAZO DE EJECUCIÓN DEL CONTRATO Y UN (01) AÑO MÁS	AMPARA EL RIESGO DE MALA CALIDAD DE LOS BIENES DURANTE EL PLAZO DE EJECUCIÓN Y EL TIEMPO QUE CUBRE LA GARANTÍA TÉCNICA. LA ESTIMACIÓN DEL RIESGO CUBRE EL CINCUENTA POR CIENTO (50%) DEL VALOR DEL CONTRATO LO QUE CUBRIRÍA EL PERJUICIO ADMINISTRATIVO POR LA POSIBLE PÉRDIDA DE LOS RECURSOS, LOS GASTOS OCASIONADOS POR EL PROCESO Y LA NO ENTREGA DE LOS BIENES REQUERIDOS.

CLAUSULAS SANCIONATORIAS

MECANISMO DE COBERTURA	CLASE DE RIESGO	TIPIFICACIÓN DE LOS RIESGOS	ESTIMACIÓN DEL RIESGO	ASIGNACIÓN DEL RIESGO	VIGENCIA	JUSTIFICACIÓN COBERTURA / VIGENCIA
MULTA	RIESGO JURIDICO	LA NO CONSTITUCION DENTRO DEL TERMINO Y EN LA FORMA PREVISTA EN EL CONTRATO O EN ALGUNO DE SUS MODIFICATORIOS LA POLIZA DE GARANTIA UNICA	MULTA CUYO VALOR SE LIQUIDARÁ CON BASE EN UN CERO PUNTO DOS (0.2%) DEL VALOR DEL CONTRATO	CONTRATISTA	LA MULTA SE APLICARÁ POR CADA DIA DE RETARDO Y HASTA POR DIEZ (10) DIAS	CUANDO EL CONTRATISTA NO CONSTITUYA DENTRO DEL TERMINO Y EN LA FORMA PREVISTA EN EL CONTRATO O EN ALGUNO DE SUS MODIFICATORIOS, A POLIZA DE GARANTIA UNICA
MULTA	RIESGO JURIDICO	INCUMPLIMIENTO PARCIAL	MULTAS CUYO VALOR SE LIQUIDARÁ CON BASE EN UN CERO PUNTO CINCO (0.5%) DEL VALOR DEJADO DE CUMPLIR O ENTREGAR	CONTRATISTA	LA MULTA SE APLICARÁ POR CADA DIA DE RETARDO HASTA POR UN PLAZO DE QUINCE (15) DIAS CALENDARIO QUE SE DESCONTARÁ DEL SALDO QUE LE ADEUDE LA ENTIDAD. ESTA SANCION SE IMPONDRA MEDIANTE ACTO ADMINISTRATIVO MOTIVADO EN EL QUE SE EXPRESARA LAS CAUSAS QUE DIERON LUGAR A ELLA	AMPARA LA MORA O INCUMPLIMIENTO PARCIAL DE ALGUNA OBLIGACION DERIVADA DEL CONTRATO POR CAUSAS IMPUTABLES AL CONTRATISTA
CLAUSULA PENAL PECUNIARIA	RIESGO JURIDICO	INCUMPLIMIENTO TOTAL DECLARATORIA DE CADUCIDAD	VEINTE POR CIENTO (20%) DEL VALOR TOTAL DEL CONTRATO	CONTRATISTA	EL VEINTE POR CIENTO (20%) DEL VALOR TOTAL DEL CONTRATO CUANDO SE TRATE DE INCUMPLIMIENTO TOTAL DEL CONTRATO Y PROPORCIONAL AL INCUMPLIMIENTO PARCIAL DEL CONTRATO	AMPARA EL INCUMPLIMIENTO PARCIAL O DEFINITIVO DEL CONTRATO POR PARTE DEL CONTRATISTA, SE BUSCA EL PAGO PARCIAL Y DEFINITIVO DE LOS PERJUICIOS QUE SE CAUSEN A LA ENTIDAD

ANALISIS DE RIESGO DEL PROCESO

GARANTÍA TÉCNICA	RIESGO OPERATIVO	DAÑOS DE LOS ELEMENTOS Y DESPERFECTOS CON LOS MISMOS	VALOR DESPERFECTOS Y/O COMPONENTES DE LOS ELEMENTOS	CONTRATISTA	EL CONTRATISTA DEBERÁ BRINDAR SOPORTE TÉCNICO DE LOS SOFTWARES POR UN PERIODO DE UN AÑO, CONTADO A PARTIR DE LA FIRMA DEL RECIBIDO A SATISFACCIÓN DEL SUPERVISOR DEL CONTRATO POR CONCEPTO DE LOS SOFTWARES, DONDE SE CERTIFIQUE LA ENTREGA DE LOS SOFTWARES ADQUIRIDOS MEDIANTE EL PRESENTE PROCESO CONTRACTUAL.	AMPARA EL CORRECTO FUNCIONAMIENTO DEL MOBILIARIO, LOS MUEBLES, SUS PARTES Y ACCESORIOS DESDE EL MOMENTO DE SU ENTREGA Y HASTA POR EL PERIODO ESTIPULADO EN LAS ESPECIFICACIONES TÉCNICAS.

Teniente Coronel **Fernando Guzmán Ramos**
Jefe Área de Producción

Capitán **John Guevara Pulido**
Recolector de Información
Área Producción de Inteligencia

POLICÍA NACIONAL

ELABORACION DE ESTUDIOS PREVIOS PARA CONTRATOS

ANÁLISIS DEL RIESGO Y LA FORMA DE MITIGARLO

No.	Clase	Fuente	Etapa	Tipo	Descripción	Consecuencia de la Ocurrencia del Evento	Probabilidad	Impacto	Calificación Total	Prioridad	¿A quién se le asigna el riesgo?	Tratamiento controles a ser implementados	Impacto después del tratamiento			Afecta la ejecución del contrato	¿Afecta el equilibrio económico del contrato?	Persona responsable por implementar el tratamiento	Fecha estimada en que se inicia el tratamiento	Fecha estimada en que se complementa el tratamiento	Monitoreo y Revisión	
													Probabilidad	Impacto	Calificación total						¿Como se realiza el monitoreo?	Periodicidad ¿Cuándo?
1	General	Externo	Ejecución	Social o político	No suscripción del contrato sin justa causa	Que no se firme el contrato y se tenga que iniciar un nuevo proceso	1	5	6	Alto	Entidad Estatal	Garantía única	1	1	Bajo	No	No	Supervisor del Contrato	Desde la firma del contrato	3 meses después de la presentación de la oferta	Verificación de la calidad de los productos, producto por muestreo	Una vez
2	General	Externo	Contratación	Social o político	La no ampliación de la vigencia de la garantía	Que los software adquiridos queden sin cobertura de garantía	1	2	3	Medio	Entidad Estatal	Garantía única	1	1	Bajo	No	No	Supervisor del Contrato	Desde la firma del contrato	3 meses después de la presentación de la oferta	Seguimiento a los productos que serán entregado s e instalados	Una vez
3	General	Externo	Contratación	Social o político	Garantía que ampare el incumplimiento de las obligaciones del contrato	No se cumple lo contratado	1	2	5	Medio	Entidad Estatal	Garantía de seriedad	1	1	Bajo	No	No	Entidad Estatal	Desde la presentación de la oferta	3 meses después de la presentación de la oferta	Revistas periódicas	Una vez
4	General	Externo	Ejecución	Contratación	Retiro de la oferta después del término para presentación	No se firme el contrato	1	3	4	Medio	Entidad Estatal	Garantía de seriedad	1	1	Bajo	No	No	Entidad Estatal	Desde la presentación de la oferta	3 meses después de la presentación de la oferta	Verificar firma del contrato	Una vez
5	General	Externo	Ejecución	Social o político	Incumplimiento del contrato	No se cumple lo contratado	2	4	6	Alto	Contratista	Garantía única	2	2	Bajo	No	No	Entidad Estatal	Desde la firma del contrato	2 meses	Revistas periódicas	Frecuente
6	General	Externo	Ejecución	Social o político	Incumplimiento del contrato	Demoras en la entrega de los software	2	3	5	Alto	Contratista	Garantía única	2	2	Bajo	No	No	Supervisor del Contrato	Desde la firma del contrato	3 meses después de la presentación de la oferta	Seguimiento Proceso Contractual	Una vez
7	General	Externo	Ejecución	Social o político	Incumplimiento del contrato	No se cumple con lo contratado	2	2	6	Medio	Contratista	Garantía única	2	2	Bajo	No	No	Supervisor del Contrato	Desde la firma del contrato	3 meses después de la presentación de la oferta	Verificación de la calidad de los productos, producto por muestreo del seguimiento o contractual	Una vez
8	General	Externo	Ejecución	Social o político	Calidad del Producto	Calidad deficiente de los software	3	4	6	Alto	Contratista	Garantía técnica	2	2	Bajo	No	No	Supervisor del Contrato	Desde la firma del contrato	3 meses después de la presentación de la oferta	Seguimiento a la calidad de los productos, producto por muestreo del seguimiento o contractual I	Una vez

Teniente Coronel **Fernando Guzmán Ramos**
Jefe Área de Producción

Capitán **John Guevara Pulido**
Recolector de Información
Área Producción de Inteligencia

ELABORACION DE ESTUDIOS PREVIOS PARA CONTRATOS	POLICÍA NACIONAL
FORMULARIO COMPROMISO ANTICORRUPCIÓN	

Bogotá D.C., seleccionar la fecha.

Señores.
POLICÍA NACIONAL – DIRECCIÓN DE INTELIGENCIA POLICIAL
Ciudad.

Referencia: Compromiso anticorrupción del proceso de Mínima Cuantía , Número Diligenciar el número del proceso cuyo objeto es: ADQUISICIÓN SOFTWARE DE ANTIVIRUS, CONGELADOR DE DISCO, HIPERVISOR DE MÁQUINA VIRTUAL Y VPN

El (los) suscrito(s) a saber Nombre del representante legal de la sociedad, asociación, persona jurídica, consorcio, unión temporal .: domiciliado en Domicio de la persona firmante., identificado con Documentos de identificación y lugar de expedición, quien obra en calidad de (representante legal de la sociedad, del consorcio, de la unión temporal, o de la asociación proponente, si se trata de persona jurídica, caso en el cual debe identificarse de manera completa dicha sociedad, consorcio, unión temporal, o asociación, indicando instrumento de constitución y haciendo mención a su registro en la cámara de comercio del domicilio de la persona jurídica), que en adelante se denominará el proponente, manifiesta(n) su voluntad de asumir, de manera unilateral, teniendo en cuenta las siguientes consideraciones:

PRIMERO: que la POLICÍA NACIONAL – DIRECCIÓN DE INTELIGENCIA POLICIAL, adelanta un proceso de selección para la celebración de un contrato estatal.

SEGUNDO: que es interés del proponente apoyar la acción del estado colombiano, y de la POLICÍA NACIONAL – DIRECCIÓN DE INTELIGENCIA POLICIAL para fortalecer la transparencia en los procesos de contratación, y la responsabilidad de rendir cuentas;

TERCERO: que siendo del interés del proponente participar en el proceso de selección aludido en el considerando primero precedente, se encuentra dispuesto a suministrar la información propia que resulte necesaria para aportar transparencia al proceso, y en tal sentido suscribe el presente compromiso unilateral anticorrupción, que se regirá por los siguientes compromisos:

COMPROMISOS ASUMIDOS.

El proponente, mediante suscripción del presente documento, asume los siguientes compromisos:

Nos comprometemos a no ofrecer y no dar dádivas, sobornos o cualquier forma de halago, retribuciones o prebenda a servidores públicos o asesores de la Entidad Contratante, directamente o a través de sus empleados, contratistas o tercero.

Nos comprometemos a no efectuar acuerdos, o realizar actos o conductas que tengan por objeto o efecto la colusión en el presente Proceso de Contratación.

Nos comprometemos a revelar la información que sobre el presente Proceso de Contratación nos soliciten los organismos de control de la República de Colombia.

Nos comprometemos a comunicar a nuestros empleados y asesores el contenido del presente Compromiso Anticorrupción, explicar su importancia y las consecuencias de su incumplimiento por nuestra parte, y la de nuestros empleados o asesores.

Conocemos las consecuencias derivadas del incumplimiento del presente compromiso anticorrupción.

El proponente no ofrecerá ni dará sobornos ni ninguna otra forma de halago a ningún funcionario público en relación con su propuesta, con el proceso de contratación, ni con la ejecución del contrato que pueda celebrarse como resultado de su propuesta,

El proponente se compromete a no permitir que nadie, bien sea empleado de la compañía o un agente comisionista independiente, o un asesor o consultor lo haga en su nombre;

El proponente se compromete formalmente a impartir instrucciones a todos sus empleados, agentes y asesores, y a cualesquiera otros representantes suyos, exigiéndoles el cumplimiento en todo momento de las leyes de la República de Colombia, especialmente de aquellas que rigen el presente proceso de selección y la relación contractual que podría derivarse de ella, y les impondrá las obligaciones de:

No ofrecer o pagar sobornos o cualquier halago a los funcionarios de LA UNIDAD EJECUTORA, ni a cualquier otro servidor público o privado que pueda influir en la adjudicación de la propuesta, bien sea directa o indirectamente, ni a terceras personas que, por su influencia sobre funcionarios públicos, puedan influir sobre la aceptación de la propuesta.

No ofrecer pagos o halagos a los funcionarios de la POLICÍA NACIONAL - UNIDAD EJECUTORA durante el desarrollo del contrato que se suscriba si llegase a ser aceptada su propuesta.

Asimismo, debe tener en cuenta que los acuerdos contrarios a la libre competencia, es decir, aquellos que tengan por objeto la colusión (convenio o contrato hecho en forma fraudulenta o engañosa) en los procesos o los que tengan como efecto la distribución de adjudicaciones de contratos, distribución de concursos o fijación de términos de las propuestas,[1] son sancionables por la Superintendencia de Industria y Comercio.

El proponente se compromete a que los recursos utilizados para las gestiones pre-contractuales o contractuales derivadas del presente proceso no provendrán de actividades ilícitas tales como el lavado de activos, testaferrato, tráfico de estupefacientes o delitos contra el orden constitucional, o que de alguna manera contraríen las leyes de la República, la moral o las buenas costumbres.

El proponente asume a través de la suscripción del presente compromiso, las consecuencias previstas en la solicitud de oferta del proceso de contratación, si se verificare el incumplimiento de los compromisos anticorrupción.

En constancia de lo anterior, y como manifestación de la aceptación de los compromisos unilaterales incorporados en el presente documento, se firma el mismo en la ciudad de (ciudad donde se firma el presente documento) a los (día del mes en letras y números, días del mes de del año).

El proponente:

_____

Firma del representante legal del proponente
Nombre o razón social del oferente: Diligenciar el nombre completo del proponente
Identificación (NIT ☐ C.C ☐ C.E ☐): Diligenciar la identificación del proponente
Nombre Representante Legal: Diligenciar el nombre completo del representante legal
Identificación (C.C ☐ C.E. ☐) Diligenciar el documento de identificación del representante legal
Dirección: Diligenciar la dirección del proveedor
Teléfono: Diligenciar teléfonos de contacto del proveedor
Email: Diligenciar correo electrónico de notificaciones

NOTA: para el caso de ofertas conjuntas, suscribirán el presente documento todas los que conforman el consorcio o unión temporal a través del integrante, representante legal o apoderado.

[1] Decreto 2153 de 1992, Arts. 44 y 47.

Bogotá D.C., seleccionar la fecha.

Señores.
POLICÍA NACIONAL – DIRECCIÓN DE INTELIGENCIA POLICIAL
Ciudad.

Referencia: presentación sistema de gestión de la seguridad y salud en el trabajo para el proceso de Mínima Cuantía Número Diligenciar el número del proceso cuyo objeto es: "ADQUISICIÓN SOFTWARE DE ANTIVIRUS, CONGELADOR DE DISCO, HIPERVISOR DE MÁQUINA VIRTUAL Y VPN"

El(los) suscrito(s) a saber: Nombre del representante legal de la sociedad, asociación, persona jurídica, consorcio, unión temporal , domiciliado en Domicio de la persona firmante., identificado con Documentos de identificación y lugar de expedición, quien obra en calidad de (representante legal de la sociedad, del consorcio, de la unión temporal, o de la asociación proponente, si se trata de persona jurídica, caso en el cual debe identificarse de manera completa dicha sociedad, consorcio, unión temporal, o asociación, indicando instrumento de constitución y haciendo mención a su registro en la cámara de comercio del domicilio de la persona jurídica), quien en adelante se denominará el PROPONENTE, manifiesta(n) su voluntad de asumir, de manera unilateral, el presente compromiso, teniendo en cuenta las siguientes consideraciones:

La Policía Nacional, mediante la Resolución 03843 del 09/09/2019, prevé en el Artículo 2º, lo relacionado con la ***"Política del Sistema de Gestión de la Seguridad y Salud en el Trabajo de la Policía Nacional"***, en lo siguiente:

> *"La Policía Nacional de Colombia, en el ejercicio de su función de mantenimiento de seguridad y convivencia ciudadana, manifiesta su compromiso con la protección de la seguridad y salud en el trabajo de todos los funcionarios uniformados, no uniformados, contratistas y trabajadores en misión, mediante la identificación de peligros, evaluación y valoración de los riesgos laborales en todos los niveles de la Institución; para ello destinará el capital humano, financiero y tecnológico, que permita el cumplimiento de los requerimientos legales y las acciones de mejora continua".*

PERSONA JURÍDICA

Una vez leída y conocida la Política que define la Policía Nacional para el Sistema de Gestión de Seguridad y Salud en el Trabajo certifico que cumplo con los requisitos legales aplicables a mi actividad económica, clase de riesgo y tamaño de la empresa, actualizando los documentos técnicos y cumplimientos asociados al objeto del presente contrato.

PERSONA NATURAL

Una vez leída y conocida la Política que define la Policía Nacional para el Sistema de Gestión de Seguridad y Salud en el Trabajo, certifico que cumplo con los requisitos legales aplicables a la actividad económica y clase de riesgo para la cual fui contratado, así mismo me comprometo a cumplir con las actividades y recomendaciones establecidas por el Sistema de Gestión de Seguridad y Salud en el Trabajo en el marco del objeto del presente contrato y de las instalaciones policiales en donde preste mis servicios.

Nota: seleccionar, según corresponda.

De igual manera en la ejecución del contrato adicional a los requerimientos exigidos para su ejecución, la persona natural o jurídica deberá:

- Cumplir con las obligaciones del SGSST, que las normas legales vigentes y/o la Policía Nacional haya considerado en el contrato y acorde a la exposición del contratista o subcontratista a los riesgos encontrados en el centro de trabajo donde desarrolla la actividad.
- Participar en las actividades que la Policía Nacional desarrolle en materia de promoción y prevención de riesgos laborales.

- Cumplir con el uso continuo y permanente de los elementos de protección personal, durante la ejecución contractual, acorde a los peligros y riesgos relacionados la tarea contratada.
- Conocer y participar en todas las actividades del plan de emergencia que se programen por parte de la Policía Nacional y los brigadistas de los centros de trabajo en donde desarrollará las actividades.
- Notificar a la mayor brevedad, al supervisor del contrato, la ocurrencia de incidentes, accidentes de trabajo o el diagnóstico de enfermedades laborales, así como las condiciones de peligro que detecte durante la ejecución de la actividad contratada.
- Practicarse o practicar a sus trabajadores (según sea el caso), los exámenes médico ocupacionales y complementarios que correspondan, de acuerdo a la actividad contratada y objeto del contrato.
- Diligenciar los formatos del SGSST de la Policía Nacional o el contratante, que le sean aplicables a la ejecución de la tarea contratada.
- Entregar los documentos que evidencien objetivamente los aportes al Sistema de Seguridad Social Integral, según los requisitos legales y las obligaciones como contratista, efectuando los pagos a la ARL de acuerdo a la clase de riesgo de la actividad desarrollada.

Las personas **jurídicas** deben diligenciar la lista de chequeo que evidencie el cumplimiento a la Resolución 0312 del 2019 "*Por la cual se definen los Estándares Mínimos del Sistema de Gestión de Seguridad y Salud en el Trabajo SG-SST*, considerando lo siguiente:

1. Estándares mínimos para empresas, empleadores y contratantes con diez (10) o menos trabajadores, clasificadas con riesgo I, II ó III
2. Estándares mínimos para empresas de once (11) a cincuenta (50) trabajadores clasificadas con riesgo I, II ó III.
3. Estándares mínimos para empresas de más de cincuenta (50) trabajadores clasificadas con riesgo I, II, III, IV ó V y de cincuenta (50) ó menos trabajadores con riesgo IV ó V.

La verificación al cumplimiento de lo antes descrito será efectuada por el supervisor del contrato.

El proponente:

_____

Firma del representante legal del proponente
Nombre o razón social del oferente: Diligenciar el nombre completo del proponente
Identificación (NIT ☐ C.C ☐ C.E ☐): Diligenciar la identificación del proponente
Nombre Representante Legal: Diligenciar el nombre completo del representante legal
Identificación (C.C ☐ C.E. ☐) Diligenciar el documento de identificación del representante legal
Dirección: Diligenciar la dirección del proveedor
Teléfono: Diligenciar teléfonos de contacto del proveedor
Email: Diligenciar correo electrónico de notificaciones

Nota: Este formulario se actualizará por parte de las unidades dueñas de la necesidad en coordinación con el responsable del Sistema de Gestión de SST de la unidad, cada vez que se requiera, de acuerdo con la actualización de la normatividad, política y objetivos del SG-SST de la Policía Nacional

ELABORACION DE ESTUDIOS PREVIOS PARA CONTRATOS	POLICÍA NACIONAL
FORMULARIO ACUERDO DE CONFIDENCIALIDAD	

Bogotá D.C., seleccionar la fecha.

Señores.
POLICÍA NACIONAL – DIRECCIÓN DE INTELIGENCIA POLICIAL
Ciudad.

Referencia: Acuerdo de confidencialidad del proceso de Mínima Cuantía , Número Diligenciar el número del proceso cuyo objeto es: "ADQUISICIÓN SOFTWARE DE ANTIVIRUS, CONGELADOR DE DISCO, HIPERVISOR DE MÁQUINA VIRTUAL Y VPN"

El(los) suscrito(s) a saber: Nombre del representante legal de la sociedad, asociación o persona jurídica proponente, o nombre del representante legal del consorcio o unión temporal proponente). domiciliado en Domicilio de la persona firmante , identificado con Documento de identificación de la persona firmante y lugar de expedición, quien obra en calidad de representante legal Seleccionar la opción correspondiente, si se trata de persona jurídica, caso en el cual debe identificarse de manera completa dicha sociedad, consorcio, unión temporal, o asociación, indicando instrumento de constitución y haciendo mención a su registro en la cámara de comercio del domicilio de la persona jurídica), que en adelante se denominará el proponente, manifiesta(n) su voluntad de asumir, de manera unilateral, el presente compromiso, teniendo en cuenta las siguientes consideraciones:

Primero: que la Policía Nacional adelanta un proceso de contratación a través de la modalidad de Mínima Cuantía, para la celebración de un contrato estatal para la "ADQUISICIÓN SOFTWARE DE ANTIVIRUS, CONGELADOR DE DISCO, HIPERVISOR DE MÁQUINA VIRTUAL Y VPN"

Segundo: que el **proponente** entiende que parte de la información a la cual tendrá acceso por causa o con ocasión de los procesos de contratación descritos en el numeral anterior se encuentra sujeta a reserva legal por tratarse de actividades relacionadas con la defensa y seguridad de la nación.

Cláusula primera. Compromisos asumidos.

El proponente, mediante suscripción del presente documento, asume los siguientes compromisos:

1. Mantener en reserva y no divulgar la **información confidencial** revelada por la **policía nacional** o por terceros formalmente designados para el efecto.

2. Mantener en reserva y no divulgar ni utilizar, en provecho propio o de terceros y para fines distintos a los previstos en el **contrato**, la información que le sea entregada directamente por la **policía nacional** y/o sus designados.

3. Mantener en reserva y no divulgar por ningún motivo la información que personalmente conozca o llegare a conocer en desarrollo y ejecución de las actividades que le competan por causa o con ocasión del **contrato**.

4. Mantener en reserva y no divulgar la información protegida por derechos de autor o por secreto industrial de acuerdo a la normatividad vigente y que haga parte de la **información confidencial.**

5. Reconocer que el recibo de la **información confidencial** no concede, ni expresa ni implícitamente, autorización, permiso o licencia de uso de marcas, patentes, derechos de autor, o de cualquier otro derecho de propiedad industrial o intelectual de la **Policía Nacional**.

6. Suscribir, con antelación a la revelación de la **información confidencial**, los acuerdos de confidencialidad que se ajustan a todo lo dispuesto en el presente acuerdo con todos sus empleados y/o familiares de los mismos, contratistas, subcontratistas, proveedores y demás personas naturales o jurídicas que haya involucrado, involucre o llegare a involucrar en la ejecución de las actividades que le correspondan para el cumplimiento del objeto del **contrato**.

7. El **proponente** mantendrá una lista de usuarios de la **información confidencial** que será entregada al **proponente** cuando lo solicite.

8. Utilizar única y exclusivamente la **información confidencial** que conozca o llegare a conocer, en desarrollo y ejecución de lo que le competa en relación con el contrato.

9. No utilizar la **información confidencial** que conozca o llegare a conocer, en desarrollo y ejecución del **contrato**, en provecho propio o de terceros y para fines distintos a los previstos en el mismo, prohibiéndose la divulgación inclusive para fines académicos.

10. Adoptar y mantener mecanismos internos de seguridad adecuados para proteger la confidencialidad de toda la información que conozca o llegare a conocer en desarrollo del **contrato**.

11. No usar la **información confidencial** de modo que pueda ser de alguna manera, directa o indirectamente, perjudicial para los intereses de la **policía nacional**.

12. No acceder, copiar, reproducir, distribuir o transmitir por ningún medio conocido o por conocer la **información confidencial**, en todo o en parte, sin previo y escrito consentimiento de la **Policía Nacional**.

13. Cumplir con la confidencialidad en las mismas condiciones y formas, y con el mismo cuidado con que realiza la protección de la información confidencial.

El proponente:

_____
Firma del representante legal del proponente
Nombre o razón social del oferente: Diligenciar el nombre completo del proponente
Identificación (NIT ☐ C.C ☐ C.E ☐): Diligenciar la identificación del proponente
Nombre Representante Legal: Diligenciar el nombre completo del representante legal
Identificación (C.C ☐ C.E. ☐) Diligenciar el documento de identificación del representante legal
Dirección: Diligenciar la dirección del proveedor
Teléfono: Diligenciar teléfonos de contacto del proveedor
Email: Diligenciar correo electrónico de notificaciones

SOLICITUD COTIZACIONES	
ADVERTENCIA	La cotización solicitada servirá únicamente de base para la elaboración de un estudio de mercado y, por tanto, **no constituye en sí misma una oferta y consecuentemente NO obliga a las partes.**
OBJETO	**ADQUISICIÓN SOFTWARE DE ANTIVIRUS, CONGELADOR DE DISCOS, HIPERVISOR DE MÁQUINA VIRTUAL Y RED PRIVADA VIRTUAL (VPN).**
VALIDEZ DE LA COTIZACIÓN	30 días
ESPECIFICACIONES TÉCNICAS	SOFTWARE DE ANTIVIRUS - Marca: especificar por el oferente - Referencia: especificar por el oferente - Se requieren el software de antivirus para setenta (70) equipos de cómputo - El antivirus debe contar con un mecanismo de actualización frecuente de antimalware que garantice la integridad y minimice la manipulación o alteración de las definiciones de virus por medio de cifrado y firmas digitales. - El antivirus debe permitir el acceso en demanda, en segundo plano, proactivo, sub-sistema de prevención de brotes de virus, análisis de phishing y filtrado de contenido, protección sobre los protocolos HTTP, HTTPS, FTP. - La solución debe analizar tipo de archivo verdadero y eliminar si da el caso, archivos ejecutables con extensiones como: *.EXE, *.APP, *.VB, *.VBS, *.SCR, *.BAT, *.DLL, *.COM, *.BIN, *.EBS., entre otros que aprovechan los diferentes tipos de extensiones de un sistema operativo, camuflándose para afectar a los sistemas. - La solución debe ejecutar detección de archivos con base al tipo y no solo a la extensión. - Debe anticiparse a los virus desconocidos e intrusos mediante herramientas que supervisen los procesos en ejecución en busca de comportamientos maliciosos. - Escanee sitios Web en busca de código malicioso; Control y Protección Web. - Compruebe la reputación de los vínculos antes de navegar en ellos. - Detecte y bloquee los vínculos de phishing que intentan robar información confidencial y datos financieros. - Reconocimiento de anomalías, detección y bloqueo de ataques de tipo Host Sweep, TCP o UDP port Scan, CGI Holes. - Utiliza técnicas de análisis avanzadas para comprobar si un sitio presenta las características típicas de las operaciones de phishing. - La solución de antivirus debe soportar la instalación de los agentes en estaciones de trabajo, portátiles y equipos de cómputo. Así como garantizar la compatibilidad en los dispositivos mencionados. - La protección antivirus debe tener compatibilidad con sistemas operativos Windows y Mac. - La solución permite el monitoreo en tiempo real de los procesos en memoria para capturar los virus que son ejecutados en memoria sin necesidad de escribir el archivo. - El módulo de comportamiento debe ser capaz de detectar amenazas de día cero tipo Ransomware - Detección y reacción contra Ransomware que inicie el cifrado de información, así no se tenga firma de detección de malware para

	detenerlo. Este módulo debe terminar el proceso de cifrado malicioso de forma automática. - Protección contra la explotación permitiendo finalizar programas que se identifiquen con comportamiento anormal asociado a ataques de Exploit. - Evitar o monitorear que un programa con comportamiento sospechoso pueda duplicar o inyectar archivos. - Evitar o monitorear que un programa con comportamiento sospechoso pueda incrustar complementos en los navegadores. - Evitar o monitorear que un programa con comportamiento sospechoso pueda instalar librería del programa malicioso. - Para aquellos programas válidos y que por su comportamiento el Antimalware no permita su ejecución, deberá de permitirlos agregándolos a una lista blanca. - Detección del malware en pre-ejecución y comprobar el comportamiento malicioso para detectar malware desconocido. - Debe realizar la verificación de todos los archivos accedidos en tiempo real, incluso durante el proceso de arranque. - Debe realizar la limpieza del sistema automáticamente, eliminando elementos maliciosos detectados y aplicaciones potencialmente indeseables (PUA). - Debe proteger las funciones críticas en los navegadores de Internet (Safe Browsing). - Debe permitir la autorización de detecciones maliciosas y excluir de la exploración de directorios y archivos específicos. - Se requiere protección integrada, es decir, en un solo agente, contra amenazas de seguridad, incluyendo las potencialmente no deseadas (PUA). - Permitir la utilización de contraseña de protección para posibilitar la reconfiguración local en el cliente y desinstalación de los componentes de protección. - Debe poseer la capacidad de bloqueo de ataques basado en la explotación de vulnerabilidad conocida. - Debe ser capaz de aplicar un análisis adicional, inspeccionando finamente el comportamiento de los códigos durante la ejecución, para detectar el comportamiento sospechoso de las aplicaciones, tales como desbordamiento de búfer. - Debe prevenir el ataque de vulnerabilidades de navegador a través de web exploits. - Debe brindar protección de amenazas de día cero (0) a través de tecnología de deep learning (signature less). - Debe tener la funcionalidad de detección de amenazas desconocidas que están en memoria con tecnología de Deep Learning. - Debe tener la capacidad de detección y bloqueo proactivo de keyloggers y otros malwares no conocidos (ataques de día cero) a través del análisis de comportamiento de procesos en memoria. - Debe tener la capacidad de detección y bloqueo de Trojans y Worms, entre otros malwares, por comportamiento de los procesos en memoria. - Debe detectar el malware en pre-ejecución un tiempo aproximado de no más de 20 milisegundos. - No debe requerir descarga de firmas de ningún tipo para la parte de protección por comportamiento. - Debe tener la capacidad de analizar el comportamiento de nuevos procesos al ser ejecutados, en complemento a la exploración programada.

	- Debe contar con bloqueo y protección contra amenazas desconocidas potencialmente sospechosas (PUA). - Se debe garantizar la generación de excepciones ante falsos positivos. - El software debe tener la capacidad de protección AMSI contra scripts maliciosos. - El software debe poseer un IPS de Host. - El software debe disponer de capacidad de protección contra ransomware no basada exclusivamente en la detección por firmas. - El software debe disponer de capacidad de remediación de la acción de encriptación maliciosa del ransomware. - El software a instalar en equipos de cómputo debe disponer de capacidad de prevención contra la acción de cifrado malicioso ejecutado por ransomware, posibilitando el bloqueo de las computadoras de donde parte tal acción. - El software debe contar con protección anti-ransomware para el sector de booteo. - El software debe restaurar automáticamente los archivos cifrados por un proceso malicioso de ransomware. - Detección y protección de técnicas de explotación: o Enforce Data Execution Prevention; o Mandatory Address Space Layout Randomization; o Bottom-up ASLR; o Null Page (Null Deference Protection); o Heap Spray Allocation; o Dynamic Heap Spray; o Stack Pivot; o Stack Exec (MemProt); o Stack-based ROP Mitigations (Caller); o Branch-based ROP Mitigations (Hardware Assisted); o Structured Exception Handler Overwrite (SEHOP); o Import Address Table Filtering (IAF); o Load Library; o Reflective DLL Injection; o Shellcode; o VBScript God Mode; o Wow64; o Syscall; o Hollow Process; o DLL Hijacking; o Squiblydoo Applocker Bypass; - APC Protection (Double Pulsar / AtomBombing); - El software debe garantizar la mitigación de inyección de códigos en procesos. - El software debe garantizar la protección contra robo de credenciales. - El software debe garantizar la protección contra malware escondido en aplicaciones legitimas (code cave). - El software debe evitar la migración de procesos maliciosos, evitando que un proceso malicioso migre a otro. - El software debe evitar la escalada de privilegios y acceso elevado a recursos. - El software debe evitar la modificación de las claves de registro para la ejecución de código arbitrario. - El software debe cumplir con todos los Ítems anteriores que apliquen a estaciones de trabajo bajo S.O. Windows.

	- El antivirus debe tener la capacidad de analizar Scripts de Java y VBScript antes de que se ejecuten. - El software debe controlar las actividades realizadas por aplicaciones vulnerables. - El antivirus debe contar con tecnología de remoción y detección de virus, macros infecciosas, troyanos, gusanos informáticos, Keyloggers, Spyware y adware, Rootkits, Bots y otras amenazas. Mitigar ataques y neutralizar los objetos maliciosos por medio de tecnologías de desinfección a niveles bajos del sistema operativo de un equipo. - El antivirus deberá ser estable, de tal manera que no afecte ni perjudique el rendimiento de las máquinas y/o aplicativos que estén instalados en las mismas. - El antivirus debe contar y quedar configurado con un módulo de exploración en tiempo real, que ofrezca protección continúa frente a los virus que llegan a través de dispositivos de almacenamiento extraíbles, en la red y de las diversas fuentes en Internet. - El antivirus debe tener la capacidad de explorar los procesos maliciosos que se encuentren corriendo en memoria. - El antivirus debe correr con un recurso de CPU bajo para tareas de exploración en demanda - El antivirus debe permitir y quedar configurado para tareas calendarizadas de revisión y limpieza del sistema de archivos. - El software de antivirus debe poseer mecanismos o técnicas como buffer overflows que sirven como protección contra vulnerabilidades en memoria. - El software debe consumir recursos mínimos de máquina. - El software debe permitir en su configuración la exclusión del análisis de extensiones o ficheros no deseados. Esto desde su configuración local protegida por una contraseña. - El antivirus debe explorar archivos descargados desde todas las plataformas de correo, análisis de Onedrive y/o de almacenamiento en la nube instalados por aplicaciones como Dropbox, Drive Gmail a las cuales se tiene acceso desde las estaciones de trabajo. - El antivirus debe contar con un módulo de exploración bajo demanda que, permita iniciar una exploración en cualquier momento, especificar los objetivos (discos duros, carpetas, memoria, unidades extraíbles) y las exclusiones de la exploración, así como también determinar cómo debe responder el explorador cuando detecte un virus mostrando el informe detallado. - El software debe garantizar un análisis por demanda en los dispositivos extraíbles y almacenamiento en línea, antes de tener acceso a ellos una vez conectados a los equipos de cómputo. - El software debe garantizar la detección de ataques de tipo Exploits hacia vulnerabilidades de sistema operativo como también de aplicaciones diferentes de Microsoft. - El software debe proporcionar un módulo de bloqueo de aplicaciones para proporcionar un mayor nivel de protección, seguridad y control a los usuarios. - El antivirus deberá permitir la desactivación del agente por medio de una contraseña, en caso de que se requiera o necesite. - El software deberá entregar contexto de la amenaza detectada mediante la visualización de todo el ataque, como inicio y como se comportó. Debe proveer detalle de los equipos involucrados en el ataque tales como llaves de registro, procesos y conexiones de red.

	- El software debe proveer respuesta automática a incidentes como actividades de limpieza del endpoint hasta obtener su estado de salud original. - El software debe explorar múltiples formatos de compresión de archivos como: (zip, rar, tar, gzip entre otros). - El software debe tener la capacidad de explorar los procesos que se encuentren corriendo en memoria. - El software debe ser capaz de detectar y bloquear ataques de fileless basados en PowerShell, Windows Management Instrumentations (WMI), VBScript y System Exploits para las plataformas cliente y servidores soportadas por Microsoft. - El software debe ser capaz de retornar el sistema a un estado saludable, mediante técnicas de remediación de archivos que eventualmente puedan llegar a ser modificados durante la ejecución de una amenaza. - El motor de exploración del software deberá utilizar distintas tecnologías de detección de virus: Exploración de firmas y exploración heurística "busca patrones de comportamiento de virus conocidos para la detección de virus desconocidos". - El software debe permitir la toma de decisiones correctas sobre la ejecución de archivos y personalizar las directivas o políticas, en función del nivel de tolerancia al riesgo. - El software debe tener soporte para comunicaciones bajo IPv6 - El software debe avisar sobre los posibles conflictos que existan con otros de antivirus y firewall instalados previamente en la máquina. - El software debe poder restringir completa o parcialmente el acceso a la consola cliente para configurar parámetros individuales sobre el host. - El software debe permitir configurar idioma dentro de la aplicación, entre ellos idioma español. - El software debe poder configurar acciones sobre infecciones identificadas: Denegar acceso / limpiar / Eliminar / Ninguna. - El software debe ofrecer opciones de envío de infecciones a cuarentena y ejecutar acciones sobre ítems enviados allí. - El software debe poder habilitar la opción de escaneo de clic-derecho sobre carpetas específicas en sistemas operativos soportados. - El software debe contar con características de protección para navegadores web (Active X) o detecciones que se realicen por comportamiento. - El software debe permitir la detección basada en el comportamiento anómalo en el punto final. - El software debe emplear una arquitectura multicapa, para defenderse de ataques basados en comportamientos, evitando cambios a nivel de sistema, restringiendo el acceso a procesos, archivos, recursos compartidos, valores y claves de registro específicos. - El software debe poder identificar patrones similares de comportamiento dentro de diferentes variantes, usando reglas que pueden configurarse para evitar la instalación y / o la carga de nuevas variantes históricas, actuales y en evolución de amenazas de día cero. - El software debe ser compatible con todas las versiones de los navegadores Internet Explorer, Google Chrome, Mozilla Firefox. - El software debe garantizar en las estaciones de trabajo protección contra infecciones a través descargas de internet, archivos adjuntos de e-mail, redes, archivos compartidos, CD-ROM, USB, dispositivos

	extraíbles, carpetas públicas y carpetas personales de todo tipo de correo, almacenadas localmente, mensajes de correo electrónico entrante y saliente, servicios en línea, entre otros tipos de almacenamiento. - El software debe ser capaz de detectar el 100% de los virus conocidos (reportados en listas), contra programas malignos especificados. - El software debe contar con mecanismos de borrado seguro de malware residentes en memorias que sean difíciles de erradicar, evitando el reinicio, en caso de no contar con la herramienta, deberá prever que el técnico experto en antimalware esté presente en el reinicio del equipo de cómputo verificando y garantizando la erradicación del mismo. - El software debe contar con tecnología de mitigación de EXPLOITS, que ataquen soluciones comúnmente usadas y que pueden no estar actualizadas, como Acrobat, Flash Player, entre otras. - El software debe contar con mecanismos de detección de ausencia de configuraciones y/o parches específicos de sistema operativo. - El software debe ofrecer una solución para controlar dispositivos en sistemas operativos Windows (32/64 bits). - El software debe permitir la limpieza de amenazas dentro archivos adjuntos (JavaScript dentro de archivos PDF o Microsoft Word, por ejemplo). SOFTWARE CONGELADOR DE DISCO - Marca: especificar por el oferente - Referencia: especificar por el oferente - Se requieren software de congelar discos para setenta (70) equipos de cómputo, con las siguientes funcionalidades: - El oferente debe proveer el software permita protección avanzada para estaciones de trabajo de sistema operativo Windows 7, 8 a 10 en sus últimas versiones estables. La cual debe garantizar que se preserve la configuración, actualizaciones del sistema operativo (Update) y base de datos de antivirus. - El software debe garantizar que cada vez que se reinicie el equipo el software debe restaurar la configuración. - El software debe proporcionar a los usuarios un acceso ilimitado a los cambios de configuración permanentes. - El software debe evitar los cambios de configuración, permitiendo a los usuarios guardar su trabajo sin que se altere la configuración de base de los equipos. - El software debe garantizar la eliminación de las amenazas de día cero, garantizando reversar todos los cambios maliciosos realizados en el sistema, incluidas las amenazas día cero. - El oferente debe garantizar que el software no degrade el rendimiento de los equipos. - El software debe garantizar la eliminación de todo el software instalado sin autorización, al momento de reiniciar el equipo. - El software debe permitir el reinicio sin borrado de la configuración y un reinicio borrando la configuración del equipo. - El software debe garantizar el 100 % de recuperación de las estaciones de trabajo al reiniciar. - El software debe proporcionar la protección con contraseña y seguridad completa para el acceso a la configuración. - El software debe proteger el registro de arranque maestro (MBR), los múltiples discos duros y particiones del equipo.

	- El software debe admitir discos duros SCSI, ATA, SATA e IDE. - El software debe admitir discos FAT, FAT32, NTFS, básicos y dinámicos. - El software debe permitir preseleccionar unidades a congelar y, de forma selectiva, cuáles deben ser congeladas o descongeladas unidades fijas. - El software debe tener la opción de instalación silenciosa para una conexión rápida como parte de una imagen maestra o implementación por demanda. - Creación de ThawSpaces visibles u ocultos en una estación de trabajo para almacenar programas, guardar archivos o realizar cambios permanentes. SOFTWARE DE RED PRIVADA VIRTUAL - Marca: especificar por el oferente - Referencia: especificar por el oferente - Se requieren el software de red privada virtual VPN de EndPoint para setenta (70) equipos de cómputo. - El software debe proporcionar a los usuarios la conexión a sus dispositivos a través de ubicaciones de servidores iguales o mayores a 60 países. - El software de VPN no debe recopilar ni compartir datos privados, y por ningún motivo hacer seguimiento de ellos. De igual forma no debe registrar datos de tráfico o solicitudes a DNS - El software de VPN no debe realizar control del ancho de banda. Este debe garantizar un ancho de banda ilimitado. - El software de VPN debe garantizar el enmascaramiento de la dirección IP en todo momento. - El software de VPN debe contar con Kill Switch automático. Lo que significa que, si se bloquea accidentalmente una conexión VPN, la función Kill Switch impide que tu dispositivo acceda a la web., mediante el bloqueo de tráfico en internet hasta su restauración. - El software de VPN actuará como un proxy, para su actividad web: en lugar de la dirección IP y ubicaciones reales, las páginas web que se vayan a visitar solo verán la dirección IP y la ubicación del servidor VPN. - El software de VPN garantizará la protección a la conexión entre el cliente y el servidor utilizando tunelización y cifrado (protocolo AES-256 bits) - El software de VPN debe garantizar como mínimo los siguientes protocolos: IKEv2, L2TP/IPsec, OpenVPN, Lightway. - El software de VPN debe contar con soporte 7x24 con chat en vivo. - El software de VPN debe permitir el cambio ilimitado de servidores de conexión. - El software de VPN debe operar son sus propios DNS, los cuales deben manejar tráfico cifrado. - El software de VPN debe brindar protección de fugas de DNS y WebRTC. - El software debe brindar un informe de errores, test de velocidad y la opción de escoger el más rápido. - El software de VPN debe poseer la opción de evitar la detección de la dirección IPv6 mientras se esté conectado. SOFTWARE DE HIPERVISOR DE MÁQUINA VIRTUAL

	- Marca: especificar por el oferente - Referencia: especificar por el oferente - Se requieren el software hipervisor de máquina virtual para treinta (30) equipos de cómputo. - Soporte básico por un año de suscripción. - El software hipervisor deberá permitir crear máquinas virtuales hasta de 16 CPU, 64 GB de RAM, 3 GB de vRAM). - Posibilidad de crear VM restringidas con fecha y hora de caducidad predefinidas. - El software hipervisor de máquina virtual deberá tener compatibilidad con DirectX 11 y gráficos 3D acelerados con OpenGL 4.1, una nueva interfaz de usuario con modo oscuro, compatibilidad con el modo Hyper-V de Windows en hosts Windows 7, Windows 10, y las últimas versiones estables en el mercado. - El software hipervisor de máquina virtual deberá permitir: o Crear nuevas máquinas virtuales. o Convertir PC en máquina virtual. - El software hipervisor de máquina virtual deberá tener integración de host/invitado: o Uso compartido de archivos de host/invitado. o Carpetas compartidas/reflejadas. o SSH de un solo clic a máquina virtual Linux. o Ejecutar máquinas virtuales con distintos modos de visualización. o Modo de visualización unificado (solo para sistemas Windows invitados). - El software hipervisor de máquina virtual deberá tener compatibilidad con: o Compatibilidad con una amplia gama de dispositivos virtuales. o Compatibilidad con lector de tarjetas inteligentes USB. o Compatibilidad con dispositivos USB 3.1 o Compatibilidad con dispositivos de asistencia. o Dispositivo de módulo de plataforma segura virtual. o Dispositivo NVMe virtual. - El software hipervisor de máquina virtual deberá tener funciones de seguridad como: o Compatibilidad con seguridad basada en la virtualización de Microsoft (invitado). o Módulo de plataforma segura virtual (vTPM). o Compatibilidad con arranque UEFI. o Compatibilidad con arranque seguro UEFI. o Procesador de gráficos en el entorno de pruebas de la GPU Instantánea. o Crear y gestionar máquinas virtuales cifradas. - El software hipervisor de máquina virtual deberá tener funciones específicas de host Windows: o Host de Windows 10. o Motor de representación DX12. o Compatibilidad con el modo Hyper-V (Device Guard, WSL). o Compartir máquina virtual (servidor de Workstation). - El software hipervisor de máquina virtual deberá tener Funciones avanzadas: o Operación desde la línea de comandos: vmrun y VIX.

	o Personalización de redes virtuales (NAT, cambio de nombre de red). o Simulación de redes virtuales (pérdida de paquetes, latencia, ancho de banda). o Conectar con el servidor ESXi. o Creación de clones asociados. o Creación de clones completos. o Cifrar máquinas virtuales. - El software hipervisor de máquina virtual deberá tener version comercial y de prueba. - El sistema debe contar con un soporte y actualizaciones por un periodo mínimo de 1 año. - El software hipervisor de máquina virtual deberá ser la última versión disponible por el fabricante y en el evento que el fabricante genere nuevas actualizaciones o versiones, el proveedor deberá suministrar el software para ejecutar la última versión disponible y estable del hipervisor de máquina virtual. - El contratista deberá entregar una certificación directamente emitida por el fabricante, en donde conste que el software adquirido por la entidad tiene suscripción de uso por el término de (1) año contado a partir de la entrega del software al supervisor del contrato. - El contratista deberá garantizar que las mejoras de software a nuevas versiones (más recientes), releases y parches, entre otros, son de una versión igual o superior a las últimas versiones liberadas por la casa matriz en el mercado colombiano. - El contratista deberá hacer entrega del software objeto del contrato, previa suscripción del acta de inicio y durante el plazo de ejecución del contrato. - SERVICIOS DE IMPLEMENTACIÓN Los softwares ofertados deberán ser instalados, configurados y puestos en funcionamiento en las instalaciones de la Dirección de Inteligencia Policía ubicada en la Av. Boyacá 142ª 55 por el oferente. - ASISTENCIA TÉCNICA Y GARANTÍA - El oferente deberá brindar soporte técnico de los softwares por un periodo de un año, contados a partir de la firma del recibido a satisfacción del supervisor del contrato por concepto de los softwares, donde se certifique la entrega de los softwares adquiridos mediante el presente proceso contractual. - El servicio de soporte debe ser telefónico/sitio web y darse directamente por el oferente para todos los niveles de prioridad de los incidentes, problemas, inquietudes, dudas que se reporten durante el término de vigencia del contrato. - En caso de existir urgencia respecto a incidentes que involucren las soluciones ofertadas, el oferente deberá proporcionar en caso de necesitarlo apoyo de casa matriz (presencial) hasta solucionar el incidente. - El soporte de los softwares será 7x24 con un tiempo de respuesta no superior a 2 horas por parte del oferente. Los softwares deben contar con un soporte que permita accesos directos a los especialistas de producto cuando sea requerido por los diferentes medios de atención por parte de la dirección de inteligencia policial.

	- TRANSFERENCIA DE CONOCIMIENTOS El oferente deberá incluir una transferencia de conocimientos de cuatro (4) horas virtuales, para dos (2) funcionarios, en el manejo, instalación y operación del software de antivirus, congelador de disco, hipervisor de máquina virtual y red privada virtual (VPN). - ASPECTOS DE CONFIDENCIALIDAD - El personal que realice la instalación y configuración de los productos ofertados deberá someterse a un estudio de seguridad realizado por la Dirección de Inteligencia de la Policía Nacional, durante la vigencia del contrato. - En virtud del presente estudio previo, el oferente se obliga a no suministrar información que obtenga o conozca con ocasión de la ejecución del presente contrato; así como sobre los lugares a los cuales tenga acceso con ocasión de su desarrollo. El oferente deberá diligenciar el Formulario No. 1 "Acuerdo de confidencialidad". - La Dirección de Inteligencia Policial de la Policía Nacional - DIPOL se reserva el derecho de hacer las verificaciones que considere necesarias en la documentación presentada, con el fin de garantizar la transparencia del proceso de contratación. - NIVEL EDUCATIVO - El personal que realizará la instalación y configuración de los softwares, deberán ostentar el título de tecnólogo de Sistemas, Electrónico y/o a fines, con una experiencia mínima de un (1) año en la configuración e instalación de los softwares solicitados, para lo cual el oferente deberá presentar con la oferta copia del título de tecnología en ingeniería de sistemas, electrónica y/o a fines. - Si es comercializador deberá ser avalado por la casa matriz o distribuidor autorizado, lo cual deberá ser acreditado en la oferta mediante una certificación vigente por una o por todos los ítems solicitados, expedida por la casa matriz o distribuidor donde se especifique que se encuentra autorizado para vender y soportar técnicamente el software ofrecido en Colombia. - La Dirección de Inteligencia Policial de la Policía Nacional – DIPOL podrá solicitar el cambio del personal ofrecido en cualquier momento a partir de la suscripción del contrato y el mismo podrá ser sustituido por el proponente por uno con iguales o mejores capacidades, condiciones y calificaciones a las presentadas en la oferta. - EXPERIENCIA DEL PERSONAL - Con el fin de garantizar la idoneidad del personal encargado las actividades de instalación, configuración de los software de antivirus, congelador de discos, hipervisor de máquina virtual, red privada virtual (VPN) e hipervisor de máquina virtual ofertada, el proponente deberá certificar que este personal cuenta con experiencia en Colombia de haber participado mínimo en un (1) proyecto relacionado con el objeto del presente contrato; para lo cual el oferente debe anexar a la propuesta por cada empleado, una (1) certificación de proyectos en los cuales haya participado, expedidas por el oferente, durante los últimos tres (3) años anteriores a la fecha de apertura del presente proceso.

	- DOCUMENTACIÓN TÉCNICA – ENTREGABLES - El oferente debe entregar los manuales de uso en idioma español. - Toda la documentación debe entregarse en idioma español. - EXPERIENCIA DEL OFERENTE - Con el fin de garantizar la calidad de los bienes a contratar y evitar incumplimientos en la ejecución del futuro contrato, se requiere acreditar experiencia en la venta software similares al objeto del presente estudio previo, tal acreditación será avalada con la presentación de certificaciones que acrediten la participación en contratos suscritos en los últimos tres (03) años (2019.2020,2021) con empresas públicas o privada para lo cual el oferente deberá presentar máximo dos (02) certificaciones expedidas por la entidad que adquirió el software, con concepto favorable de la recepción de los servicios cuya suma o valor individual sea igual o superior al 100% del presupuesto oficial asignado. - REQUERIMIENTOS AMBIENTALES - El contratista deberá entregar los manuales de manera digital con el fin de aportar a la política de cero papeles establecida en directiva presidencial 04/2012. - SISTEMA DE GESTIÓN DE SEGURIDAD Y SALUD EN EL TRABAJO - El contratista aplicará el protocolo de bioseguridad establecido en la Dirección de Inteligencia Policial, teniendo en cuenta lo establecido por el Ministerio de Salud y Protección Social, a través de la Resolución 0000223 del 25/02/2021 "Por medio de la cual se modifica la Resolución 000666 del 24!04/2020 en sentido de sustituir el anexo técnico" y la Resolución 777 del 02/07/.2021 "Por la cual se definen los criterios y condiciones para el desarrollo de las actividades económicas, sociales y del estado y se adopta el protocolo de bioseguridad para la ejecución de estas". - El contratista deberá entregar los documentos que evidencien objetivamente, la afiliación a la Seguridad Social Integral del personal que ejecutará el objeto contractual, (E.P.S., A.F.P., A.R.L., C.C.F.), obligándose a mantener dicha afiliación, durante la totalidad del tiempo necesario para la ejecución de la actividad contratada. - El contratista correrá con los gastos médicos, de hospitalización y procedimientos médicos a que haya a lugar, en caso de que uno de sus funcionarios sufra un accidente laboral durante la ejecución del presente contrato. - En caso de presentarse un accidente de trabajo dentro de las instalaciones de la Dirección de Inteligencia, le corresponde al contratista realizar el respectivo reporte e investigación dentro del tiempo reglamentario, presentará una copia de la documentación al Grupo de Seguridad y Salud en el Trabajo de la Dirección de Inteligencia Policial, según lo establecido en la Resolución 1401 del 14 mayo de 2007 o cualquiera que la modifique, reemplace o sustituya.

	- El contratista deberá colaborar en las auditorias de cumplimiento al Sistema de Gestión de Seguridad y Salud en el Trabajo, que se realicen en el centro de trabajo donde se encuentre desempeñando las actividades	
CONDICIONES DE CONTRATACIÓN	PLAZO DE EJECUCIÓN	3 meses
	FORMA DE PAGO	Se realizará un (01) solo pago contra entrega total del ítem, en moneda legal colombiana, dentro de los sesenta (60) días calendario siguientes a la radicación de la factura, junto con el recibo a satisfacción del supervisor del contrato y los demás documentos requeridos por la Dirección de Inteligencia policial (cuando los elementos sean de origen extranjero se deberá aportar la declaración de importación), de acuerdo con el derecho a turno y la disponibilidad del Plan Anual de Caja (PAC).
	RIESGOS DE LA CONTRATACIÓN	Ver Tabla 1
	MECANISMOS DE COBERTURA DE LOS RIESGOS	Ver Tabla 2
VALOR OFRECIDO	El cotizante deberá tener en cuenta todos los gastos en los que incurra para la suscripción, legalización y ejecución del contrato, como impuestos, publicaciones, constitución de garantía única, transportes, operarios, etc.	
PLAZO PARA PRESENTAR COTIZACIÓN	El plazo será de hasta tres (3) días hábiles.	

Tabla 1
ESTIMACIÓN, TIPIFICACIÓN, ASIGNACIÓN DE RIESGOS Y DETERMINACIÓN DE GARANTÍAS.

En la definición de los parámetros de mecanismos de cobertura de los riesgos deberán efectuarse dentro de los términos definidos en el Titulo III Capítulo I del Decreto 1082 de 2015.

GARANTIAS DEL PROCESO

ETAPA PRECONTRACTUAL

MECANISMO DE COBERTURA	CLASE DE RIESGO	TIPIFICACION DE LOS RIESGOS	ESTIMACION DEL RIESGO	ASIGNACION DEL RIESGO	VIGENCIA	JUSTIFICACION COBERTURA / VIGENCIA
GARANTIA DE SERIEDAD	RIESGO JURIDICO	LA NO SUSCRIPCION DEL CONTRATO SIN JUSTA CAUSA	DIEZ POR CIENTO (10%) DEL MONTO DEL PRESUPUESTO OFICIAL.	PROPONENTE SELECCIONADO	DESDE LA PRESENTACION DE LA OFERTA Y POR CUATRO (4) MESES MAS.	AMPARA LA NO SUSCRIPCIÓN DEL CONTRATO SIN JUSTA CAUSA POR EL DIEZ POR CIENTO (10%) DEL PRESUPUESTO OFICIAL DESDE LA PRESENTACIÓN DE LA OFERTA Y POR CUATRO (4) MESES MÁS.
	RIESGO JURIDICO	LA NO AMPLIACION DE LA VIGENCIA DE LA GARANTIA DE SERIEDAD DE OFERTA CUANDO EL TERMINO PREVISTO EN LA INVITACION PARA LA ADJUDICACION DEL CONTRATO SE PRORROGUE O CUANDO EL TERMINO PREVISTO PARA LA SUSCRIPCION DEL CONTRATO SE PRORROGUE SIEMPRE Y CUANDO ESAS PRORROGAS NO EXCEDAN UN TERMINO DE CUATRO MESES.				
	RIESGO JURIDICO	LA FALTA DE OTORGAMIENTO POR PARTE DEL PROPONENTE SELECCIONADO DE GARANTIA DE CUMPLIMIENTO EXIGIDA POR LA ENTIDAD PARA AMPARAR EL INCUMPLIMIENTO DE LAS OBLIGACIONES DEL CONTRATO.				
	RIESGO JURIDICO	EL RETIRO DE LA OFERTA DESPUES DE VENCIDO EL TERMINO FIJADO PARA LA PRESENTACION DE LAS OFERTAS.				

ETAPA CONTRACTUAL

MECANISMO DE COBERTURA	CLASE DE RIESGO	TIPIFICACION DE LOS RIESGOS	ESTIMACION DEL RIESGO	ASIGNACION DEL RIESGO	VIGENCIA	JUSTIFICACION COBERTURA / VIGENCIA
GARANTIA UNICA	RIESGO JURIDICO	INCUMPLIMIENTO DEL CONTRATO	VEINTE POR CIENTO (20%) DEL VALOR DEL CONTRATO	CONTRATISTA	VIGENTE POR UN TERMINO IGUAL AL PLAZO DE EJECUCIÓN DEL CONTRATO Y (4) CUATRO MESES MAS.	AMPARA EL RIESGO DE INCUMPLIMIENTO DURANTE EL PLAZO DE EJECUCIÓN Y LIQUIDACION DEL CONTRATO LA ESTIMACION DEL RIESGO CUBRE EL 20% DEL VALOR DEL CONTRATO COMO QUIERA QUE SE PRETENDE EL PAGO PARCIAL O DEFINITIVO DE LOS PERJUICIOS QUE CAUSE A LA ENTIDAD EN LOS MISMOS TERMINOS DE LA CLAUSULA PENAL PECUNIARIA.
GARANTÍA ÚNICA	RIESGO OPERATIVO	CALIDAD DE LOS ELEMENTOS	CINCUENTA POR CIENTO (50%) DEL VALOR DEL CONTRATO	CONTRATISTA	VIGENTE POR UN TERMINO IGUAL AL PLAZO DE EJECUCIÓN DEL CONTRATO Y UN (01) AÑO MÁS	AMPARA EL RIESGO DE MALA CALIDAD DE LOS BIENES DURANTE EL PLAZO DE EJECUCIÓN Y EL TIEMPO QUE CUBRE LA GARANTÍA TÉCNICA. LA ESTIMACIÓN DEL RIESGO CUBRE EL CINCUENTA POR CIENTO (50%) DEL VALOR DEL CONTRATO LO QUE CUBRIRÍA EL PERJUICIO ADMINISTRATIVO POR LA POSIBLE PÉRDIDA DE LOS RECURSOS, LOS GASTOS OCASIONADOS POR EL PROCESO Y LA NO ENTREGA DE LOS BIENES REQUERIDOS.

CLAUSULAS SANCIONATORIAS

MULTA	RIESGO JURIDICO	LA NO CONSTITUCION DENTRO DEL TERMINO Y EN LA FORMA PREVISTA EN EL CONTRATO O EN ALGUNO DE SUS MODIFICATORIOS LA POLIZA DE GARANTIA UNICA	MULTA CUYO VALOR SE LIQUIDARÁ CON BASE EN UN CERO PUNTO DOS (0.2%) DEL VALOR DEL CONTRATO	CONTRATISTA	LA MULTA SE APLICARÁ POR CADA DIA DE RETARDO Y HASTA POR DIEZ (10) DIAS	CUANDO EL CONTRATISTA NO CONSTITUYA DENTRO DEL TERMINO Y EN LA FORMA PREVISTA EN EL CONTRATO O EN ALGUNO DE SUS MODIFICATORIOS, A POLIZA DE GARANTIA UNICA

MULTA	RIESGO JURIDICO	INCUMPLIMIENTO PARCIAL	MULTAS CUYO VALOR SE LIQUIDARÁ CON BASE EN UN CERO PUNTO CINCO (0.5%) DEL VALOR DEJADO DE CUMPLIR O ENTREGAR	CONTRATISTA	LA MULTA SE APLICARÁ POR CADA DIA DE RETARDO HASTA POR UN PLAZO DE QUINCE (15) DIAS CALENDARIO QUE SE DESCONTARÁ DEL SALDO QUE LE ADEUDE LA ENTIDAD. ESTA SANCION SE IMPONDRA MEDIANTE ACTO ADMINISTRATIVO MOTIVADO EN EL QUE SE EXPRESARA LAS CAUSAS QUE DIERON LUGAR A ELLA	AMPARA LA MORA O INCUMPLIMIENTO PARCIAL DE ALGUNA OBLIGACION DERIVADA DEL CONTRATO POR CAUSAS IMPUTABLES AL CONTRATISTA
CLAUSULA PENAL PECUNIARIA	RIESGO JURIDICO	INCUMPLIMIENTO TOTAL DECLARATORIA DE CADUCIDAD	VEINTE POR CIENTO (20%) DEL VALOR TOTAL DEL CONTRATO	CONTRATISTA	EL VEINTE POR CIENTO (20%) DEL VALOR TOTAL DEL CONTRATO CUANDO SE TRATE DE INCUMPLIMIENTO TOTAL DEL CONTRATO Y PROPORCIONAL AL INCUMPLIMIENTO PARCIAL DEL CONTRATO	AMPARA EL INCUMPLIMIENTO PARCIAL O DEFINITIVO DEL CONTRATO POR PARTE DEL CONTRATISTA, SE BUSCA EL PAGO PARCIAL Y DEFINITIVO DE LOS PERJUICIOS QUE SE CAUSEN A LA ENTIDAD

ANÁLISIS DE RIESGO DEL PROCESO

GARANTÍA TÉCNICA	RIESGO OPERATIVO	DAÑOS DE LOS ELEMENTOS Y DESPERFECTOS CON LOS MISMOS	VALOR DESPERFECTOS Y/O COMPONENTES DE LOS ELEMENTOS	CONTRATISTA	VIGENTE POR UN TÉRMINO IGUAL A LA VIGENCIA DEL CONTRATO Y UN (1) AÑO MÁS A PARTIR DEL RECIBO A SATISFACCIÓN PARA TODOS LOS COMPONENTES DEL SISTEMA.	AMPARA EL CORRECTO FUNCIONAMIENTO DE LOS SOFTWARES DESDE EL MOMENTO DE SU ENTREGA Y HASTA POR EL PERIODO ESTIPULADO EN LAS ESPECIFICACIONES TÉCNICAS.

Tabla 2

ANALISIS DEL RIESGO Y LA FORMA DE MITIGARLO

No.	Clase	Fuente	Etapa	Tipo	Descripción	Consecuencia de la Ocurrencia del Evento		Probabilidad	Impacto	Calificación Total	Prioridad	¿A quién se le asigna el riesgo?	Tratamiento controles a ser implementados	Impacto después del tratamiento			¿Afecta el equilibrio económico del contrato?	Persona responsable por implementar el tratamiento	Fecha estimada en que se inicia el tratamiento	Fecha estimada en que se complementa el tratamiento	Monitoreo y Revisión	
														Probabilidad	Impacto	Calificación						
1	General	Externo	Ejecución	Social o político	Calidad del Producto	Deficiencia en la calidad de los productos	Que no se firme el contrato y se tenga que iniciar un nuevo proceso	1	3	3	Alto	Entidad Estatal	Garantía de seriedad	1	1	Bajo	3	No	No	Entidad Estatal	Desde la presentación de la oferta	3 meses después de la presentación de la oferta	Una vez
2	General	Externo	Contratación	Social o político	La no ampliación de la vigencia de la garantía	Que los elementos adquiridos queden sin cobertura el contrato		1	2	5	Medio	Entidad Estatal	Garantía de seriedad	1	1	Bajo	2	No	No	Entidad Estatal	Desde la presentación de la oferta	3 meses después de la presentación de la oferta	Una vez
3	General	Externo	Contratación	Social o político	Garantía que ampare el incumplimiento de las obligaciones del contrato	No se cumple lo contratado		1	2	5	Medio	Entidad Estatal	Garantía de seriedad	1	1	Bajo	2	No	No	Entidad Estatal	Desde la presentación de la oferta	3 meses después de la presentación de la oferta	Una vez
4	General	Externo	Contratación	Social o político	Retiro de la oferta después del término para presentación	No se firme el contrato		1	3	4	Medio	Entidad Estatal	Garantía de seriedad	1	1	Bajo	2	No	No	Entidad Estatal	Desde la presentación de la oferta	3 meses después de la presentación de la oferta	Una vez
5	General	Externo	Ejecución	Social o político	Incumplimiento del contrato	No se cumple lo contratado		2	4	6	Alto	Contratista	Garantía única	2	1	Bajo	3	No	No	Entidad Estatal	Desde la firma del contrato o	2 meses mas	Frecuente
6	General	Externo	Ejecución	Social o político	Incumplimiento del contrato	Demoras en la entrega de los elementos		2	3	5	Alto	Contratista	Garantía única	2	1	Bajo	3	No	No	Supervisor del Contrato	Desde la firma del contrato o	3 meses después de la presentación de la oferta	Una vez
7	General	Externo	Ejecución	Social o político	Incumplimiento del contrato	No se cumple con lo contratado	Calidad deficiente de los productos	2	3	6	Alto	Contratista	Garantía única	2	1	Bajo	3	No	No	Supervisor del Contrato	Desde la firma del contrato o	3 meses después de la presentación de la oferta	Una vez
8	General	Externo	Ejecución	Social o político	Calidad del Producto	Deficiencia en la calidad de los productos	Que no se firme el contrato y se tenga que iniciar un nuevo proceso	1	3	6	Alto	Entidad Estatal	Garantía de seriedad	1	1	Bajo	3	No	No	Entidad Estatal	Desde la firma del contrato o	3 meses después de la presentación de la oferta	Una vez

Monitoreo y Revisión	
¿Como se realiza el monitoreo?	Periodicidad ¿Cuando?
Seguimiento a la calidad de los producto s, por medio del seguimiento contractual	Una vez
Verificación de la calidad de los productos que serán entregados e instalados	Una vez
Seguimiento Proceso o Contractual	Frecuente
Revisar as Verificar firma del contrato cas	Una vez
Verificar firma del contrato	Una vez
Verificar firma del contrato	Una vez

1 Sobre único

1.1 Lista de artículos — Incluya el precio como lo indique la Entidad Estatal

Incluya el precio como lo indique la Entidad Estatal
99.900.000,00

Ref. Artículo	Código UNSPSC	Descripción	Cantidad	Unidad	Precio unitario estimado	Precio unitario	Incluya el precio como lo indique la Entidad Estatal
1	43231500	SOFTWARE DE HIPERVISOR DE MAQUINA VIRTUAL	30,00	UN	1.773.333,34	1.720.000,00	51.600.000,00
2	43232800	SOFTWARE VPN	70,00	UN	450.000,00	450.000,00	31.500.000,00
3	43232800	SOFTWARE DE CONGELADOR DE DISCO	70,00	UN	180.000,00	180.000,00	12.600.000,00
4	43233200	SOFTWARE PAQUETE ANTIVIRUS	70,00	UN	60.000,00	60.000,00	4.200.000,00

1 Sobre único

1.1 Lista de artículos — Incluya el precio como lo indique la Entidad Estatal

Incluya el precio como lo indique la Entidad Estatal
99.995.950,40

Ref. Artículo	Código UNSPSC	Descripción	Cantidad	Unidad	Precio unitario estimado	Precio unitario	Incluya el precio como lo indique la Entidad Estatal
1	43231500	SOFTWARE DE HIPERVISOR DE MAQUINA VIRTUAL	30,00	UN	1.773.333,34	1.723.263,54	51.697.906,20
2	43232800	SOFTWARE VPN	70,00	UN	450.000,00	449.981,78	31.498.724,60
3	43232800	SOFTWARE DE CONGELADOR DE DISCO	70,00	UN	180.000,00	179.992,71	12.599.489,70
4	43233200	SOFTWARE PAQUETE ANTIVIRUS	70,00	UN	60.000,00	59.997,57	4.199.829,90

1 Sobre único

1.1 Lista de artículos — Incluya el precio como lo indique la Entidad Estatal

Incluya el precio como lo indique la Entidad Estatal
139.870.270,00

Ref. Artículo	Código UNSPSC	Descripción	Cantidad	Unidad	Precio unitario estimado	Precio unitario	Incluya el precio como lo indique la Entidad Estatal
1	43231500	SOFTWARE DE HIPERVISOR DE MAQUINA VIRTUAL	30,00	UN	1.773.333,34	1.712.365,00	51.370.950,00
2	43232800	SOFTWARE VPN	70,00	UN	450.000,00	439.807,00	30.786.490,00
3	43232800	SOFTWARE DE CONGELADOR DE DISCO	70,00	UN	180.000,00	452.845,00	31.699.150,00
4	43233200	SOFTWARE PAQUETE ANTIVIRUS	70,00	UN	60.000,00	371.624,00	26.013.680,00