DIRECCIÓN DE INTELIGENCIA POLICIAL

Bogotá D.C., 10 de febrero de 2023

I. ASPECTOS GENERALES DEL ESTUDIO PREVIO.

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

1.1 DESCRIPCIÓN GENERAL DEL OBJETO

ADQUISICIÓN SISTEMA INTELIGENCIA DE AMENAZAS EN LA RED

CLASIFICACIÓN UNSPSC	Segmento	Familia	Clase	Producto
43222500	Difusión de tecnologías de información y telecomunicaciones	Equipos o plataformas y accesorios de redes multimedia o de voz de datos	Equipo de seguridad de Red	
43233200	Difusión de tecnologías de información y telecomunicaciones	Software	Software de seguridad y protección.	

1.2 VALOR ESTIMADO

El valor estimado del presente proceso de contratación es de TRES MIL NOVECIENTOS NOVENTA MILLONES DOSCIENTOS MIL PESOS M/CTE ($ 3.990.200.000,00) EXENTO DE IVA. *

ÍTEM Y/O LOTE	RUBRO Y DESAGREGACIÓN PRESUPUESTAL	UNIDAD	DESCRIPCIÓN	RECURSO	CANTIDAD	VALOR UNITARIO ESTIMADO, INLCUIDO IVA, EXENTO DE IVA O EXCLUIDO DE IVA SEGÚN CORRESPONDA	VALOR TOTAL ESTIMADO INLCUIDO IVA, EXENTO DE IVA O EXCLUIDO DE IVA SEGÚN CORRESPONDA
1	C-1501-0100-22-0-1501037-02	10	DIPOL	SOFTWARE INTELIGENCIA DE AMENAZAS EN LA RED	1	$ 3.940.200.000	$ 3.940.200.000
2	C-1501-0100-22-0-1501037-02	10	DIPOL	SERVIDOR INTELIGENCIA DE AMENAZAS EN LA RED	1	$ 50.000.000	$ 50.000.000
						VALOR TOTAL ESTIMADO	$ 3.990.200.000

Nota aclaratoria: ****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	01/01/23	053	DIPOL	11	INTELIGENCIA DE AMENAZAS EN LA RED	1	$ 4.000.000.000	$ 4.000.000.000
					Total	1	$ 4.000.000.000	$ 4.000.000.000

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), que estén en capacidad de suministrar el objeto de este proceso y cumplan con todos los requisitos exigidos para el mismo.

1.6 IDENTIFICACIÓN DE LA NECESIDAD Y JUSTIFICACIÓN

Con el uso exponencial de la tecnología en la actualidad, los fenómenos delictivos han encontrado en el uso del ciberespacio una oportunidad para converger. La cantidad de delitos informáticos han ido aumentado con el tiempo, impactando entidades públicas y privadas, cuya afectación se ve reflejada en sus usuarios, ante la falta de prestación del servicio y exposición de datos personales. Por otra parte, los ciberdelincuentes, hacen uso del ciberespacio como medio para llevar a cabo conductas delictivas, cuyo fin contempla escenarios desde el hurto por medios digitales, hasta el secuestro de información (ransomware). Ante este panorama, es imperioso que la Dirección de Inteligencia Policial cuente con una capacidad que permitirá la anticipación de estas conductas y así poder salvaguardar los activos críticos de los colombianos. De igual forma, evitar en la medida de las capacidades la impunidad en acciones que atenten contra la fuga de información y/o perdida de datos, ya que podrían generar un impacto negativo en cuanto al manejo y protección de los activos estratégicos de los colombianos.

Es por esto por lo que, se requiere una capacidad que permita al servicio de inteligencia contar con información relacionada con ciberamenazas que se presente en el direccionamiento IP colombiano o que pueda afectar el mismo. La información debe estar compuesta por: URL o direcciones IP maliciosas, perfil de actor, motivaciones, malware asociado junto con el detalle de la amenaza, hash, nombre, actor, vulnerabilidad, sectores afectados e impacto, phishing, comando y control del malware, spammer. La información recolectada servirá de insumo estratégico para coadyuvar a minimizar las infecciones y ataques cibernéticos, que puedan irrumpir en los sistemas o bases de datos que se utilizan en las entidades del Estado Colombiano reduciendo las brechas de seguridad, que puedan facilitar el acceso no autorizado a los servicios web críticos del Estado colombiano. Adicionalmente, permitirá identificar indicadores de compromiso con el propósito de recolectar información que conlleven a la toma de decisiones y creación de estrategias para combatir y minimizar el impacto de los ciberdelincuentes.

Esta recolección de información servirá como insumo para la creación de productos de inteligencia los cuales se difundirán de manera oportuna a los responsables de la ciberseguridad y ciberdefensa del Estado y a las entidades del país categorizadas como infraestructuras críticas que puedan ser objeto de estos ataques informáticos, dado que en Colombia no existe tal tecnología en entidades del estado, la información entregada se enfocará en comandos y control de botnets, malware de zero day, gusanos, troyanos y amenazas avanzadas persistentes (APT).

La Dirección de Inteligencia Policial por medio del ciclo de inteligencia, tiene la función de identificar nuevos fenómenos delictivos, motivo por el cual y ante el incremento del uso del ciberespacio, debe estar en la

vanguardia tecnológica en el proceso de inteligencia de amenazas cibernéticas, con el propósito de contrarrestar las acciones maliciosas que realizan diversos actores en el ciberespacio y de esta forma garantizar la confidencialidad, integridad y disponibilidad de la información de los ciudadanos colombianos, antes que se materialicen los incidentes informáticos.

Alineados al contexto y atendiendo las responsabilidades establecidas en las políticas públicas, como lo son las **Bases del Plan Nacional de Desarrollo 2022-2026 (PND 2022-2026) Colombia potencia mundial de la vida**, en el cual se concreta el inicio de una transición que debe desembocar en la paz total, que no es otra cosa que la búsqueda de una oportunidad para que todos podamos vivir una vida digna, basada en la justicia; es decir, en una cultura de la paz que reconoce el valor excelso de la vida en todas sus formas y que garantiza el cuidado de la causa común.

Uno de sus principales propósitos se denomina **la seguridad humana y justicia social**, el cual dentro de los catalizadores para cumplir con su propósito enuncia textualmente los "***Habilitadores que potencian la seguridad humana y las oportunidades de bienestar",*** que a su vez en su numeral (8), define la necesidad de tener una **"Seguridad digital confiable para la garantía de las libertades, la protección de la dignidad y el desarrollo integral de las personas";** la cual se contempla en su literal (B) la "**Protección de las personas, de las infraestructuras digitales, fortalecimiento de las entidades del Estado y garantía en la prestación de sus servicios en el entorno digital**", con el propósito de diseñar e implementar "*...una estrategia para adelantar las medidas enfocadas a salvaguardar la infraestructura cibernética del país...*" (Planeación, 2022).

De igual forma, dentro del marco del CONPES 3995 "Confianza y Seguridad Digital" CONPES 3995 del 01 de julio de 2020 – Consejo Nacional de Política Económica y Social "*Política Nacional de Confianza y Seguridad Digital*" (Planeación, 2020). El cual tiene como objetivo general, "*Establecer medidas para desarrollar la confianza digital a través de la mejora de la seguridad digital de manera que Colombia sea una sociedad incluyente y competitiva en el futuro digital mediante el fortalecimiento de capacidades y la actualización del marco de gobernanza en seguridad digital, así como con la adopción de modelos con énfasis en nuevas tecnologías.*"

En su objetivo específico **5.3.1. Fortalecer las capacidades en seguridad digital de los ciudadanos, del sector público y del sector privado para aumentar la confianza digital en el país en la cual se define**, el diseño, estructura y presentación el proyecto de implementación del CSIRT del Sector Inteligencia, con el fin que contribuya en la protección de la seguridad digital nacional. Este proyecto buscará principalmente que este CSIRT del sector de inteligencia (i) apoye la toma de decisiones en términos de valoración de los riesgos cibernéticos que se presenten en las entidades del sector y (ii) facilite la difusión de información técnica de alto valor de amenazas al Comité de Seguridad Digital referente a los distintos fenómenos que se generen en el Ciberespacio, acciones que en la actualidad son permanentes dentro de la Junta de Inteligencia Conjunta (JIC).

Asimismo, "el crecimiento que se observa de conductas delictivas en el ciberespacio en un comparado del 2021 al 2022 está por el orden de un 26%. Las conductas delictivas como se observa en la figura 1, tiene incrementos en los nueve (9) delitos definidos en la ley 1273 de 2009" (C4, 2022); sumado a esto incidentes de trascendencia nacional como vulneración de datos de la Fiscalía General de la Nación, Comando General

de las Fuerzas Militares y empresas privadas como Colsanitas (Keralty) enciende una alarma para el Estado, en cuanto a cómo contrarrestar este tipo de conductas de manera preventiva, como ha sido mencionado en diferentes medios nacionales e internacionales ante la ocurrencia de incidentes informáticos.

Figura 1

Estadísticas del Centro de Capacidades para la Ciberseguridad de Colombia C4



Nota. Conductas delictivas en el ciberespacio comparativo 2021 al 2022. (C4, 2022).

Dado lo anterior, el ciclo de Inteligencia puede ser aplicado a los fenómenos delictivos que se presentan en el ciberespacio en pro de identificar, anticipar y contrarrestar las capacidades, intenciones y actividades de los ciberactores. Por tal razón, la Policía Nacional, a través del Servicio de Inteligencia Policial y su grupo Ciberinteligencia cuenta con capacidades de recolección de datos, en el despliegue de actividades de recolección técnica en el ciberespacio que permiten identificar indicadores de compromiso (direcciones IP, hash, urls, entre otros) que son usados por ciberdelincuentes para cometer hechos delictivos. Ante eso y con el fin de mejorar las capacidades la Dirección de Inteligencia Policial debe llevar a cabo la adquisición de un componente que permita realizar inteligencia de amenazas en el ciberespacio, propósito del presente estudio previo, así:

Inteligencia de amenazas en la red: contar con una solución de datos globales integrados en un ambiente web (https) (dashboard live) que permita obtener en tiempo real información de al menos: actividad de actores, malwares activos, alertas de actividades de amenazas y creación de informes de inteligencia a partir de la

información obtenida, para la toma de decisiones y creación de estrategias para contrarrestar los fenómenos delictivos en el ciberespacio. Los datos globales deben proporcionar información que permita identificar posibles ciberataques dirigidos y/o originados con(a) direccionamiento IP Colombiano, como también a nivel internacional, con objetivo de identificar los actores maliciosos que afecten los activos digitales de los ciudadanos.

Con base a lo anterior, la implementación del proceso permitirá la generación de alertas de inteligencia con indicadores de compromiso a las entidades encargadas de la protección del ciberespacio a partir de la recolección de información, con las cuales puedan generar acciones para contrarrestar las campañas de los actores maliciosos y asesorar al gobierno nacional en la creación de estrategias para la protección de los ciudadanos que hacen uso e interactúan en el ciberespacio.

Por otro lado, los lineamientos para la realización de actividades de inteligencia se encuentran descritos en la normatividad vigente, destacándose que de acuerdo con el **artículo 2º de la Ley 1621 de 2013** *"Por medio del cual se expiden normas para fortalecer el marco jurídico que permite a los organismos que llevan a cabo actividades de inteligencia y contrainteligencia cumplir con su misión Constitucional y legal, y se dictan otras disposiciones."*, la función de inteligencia y contrainteligencia enmarca la utilización de medios técnicos para la recolección, procesamiento, análisis y difusión de información, con el objetivo de proteger los derechos humanos, prevenir y combatir amenazas internas o externas, que dentro del contexto del presente proceso se enfoca a ciberamenazas que atenten contra la vigencia del régimen democrático, el régimen constitucional y legal, la seguridad y la defensa nacional, y cumplir los fines enunciados en el artículo 4º de dicha ley.

Además, no se podrá desarrollar una actividad de inteligencia y contrainteligencia por razones de género, raza, origen nacional o familiar, lengua, religión, opinión política o filosófica, pertenencia a una organización sindical o con fines partidistas, entre otros; y en especial, el ejercicio de ésta función estará limitada por el principio de reserva legal y compartimentación que garantiza la protección de los derechos a la honra, al buen nombre, a la intimidad personal y familiar, y al debido proceso.

En tal sentido, las actividades de recolección de información de inteligencia enmarcadas en el presente proceso, serán realizadas por la Dirección de Inteligencia Policial para afrontar las modalidades delictivas que convergen en el ciberespacio y de igual forma en el cumplimiento de los fines establecidos para esta función estatutaria y en completa alineación con el ordenamiento jurídico vigente (Ley Estatutaria 1621 de 2013 Por medio del cual se expiden normas para fortalecer el marco jurídico que permite a los organismos que llevan a cabo actividades de inteligencia y contrainteligencia cumplir con su misión Constitucional y legal, y se dictan otras disposiciones., Decreto 1070 de 2015 Por el cual se establece el Decreto Único Reglamentario del Sector Administrativo de Defensa. y sentencia de constitucionalidad C-540 de 2012).

Tomado de C4, C. d. (20 de 12 de 2022). Conductas delictivas en el ciberespacio. (M. J. Pulido, Entrevistador)

Tomado de Representantes, C. (06 de 02 de 2023). Bases del *Plan Nacional de Desarrollo.* Obtenido de camara.gov.co: https://www.camara.gov.co/sites/default/files/2023-02/P.L.338-2023C%20%28PLAN%20NACIONAL%20DE%20DESARROLLO%29.pdf

ÍTEM	DESCRIPCIÓN	No. CANTIDAD ADQUIRIR	No. NECESIDAD	PORCENTAJE NECESIDAD
1	INTELIGENCIA DE AMENAZAS EN LA RED	1	1	100%

Para la consecución de este tipo de bienes se consideran de características técnicas uniformes y de común utilización, porque sus características técnicas son estándar en el mercado de telecomunicaciones e iguales para diferentes fabricantes del mercado, su utilización es común en todas las redes de comunicación corporativas y cumplen con especificaciones de servicios comunes, ofrecidos por los diferentes fabricantes y su utilización está definida con un propósito específico. Por lo anterior, diferentes oferentes pueden presentar los mismos productos y se requiere obtener el costo más favorable para la Entidad.

Es importante indicar, que con la contratación de los bienes se cumple con lo establecido en la normativa vigente frente a la austeridad del gasto, con base a lo estipulado en la directiva presidencial 08 del 17/09/22 "Directrices de austeridad hacia un gasto público eficiente".

Así mismo se verificó la tienda virtual del estado colombiano https://www.colombiacompra.gov.co/tienda-virtual-del-estado-colombiano, y no se encuentra ningún acuerdo marco de precios, que contemple la adquisición de estos elementos objeto del presente proceso con las especificaciones técnicas requeridas

Mediante comunicación oficial No. GS-2023-000294-OFITE-COTEL-GINTE 10.3, del 13 de enero de 2023, suscrito por el señor teniente coronel OSCAR ANDRES CARDENAS PEÑA, Jefe Oficina de Telemática, informa que el comité evaluador una vez validados los ajustes requeridos, mediante acta No. 025 OFITE-GINTE 2.25 del 12/01/2023, considera viable la adquisición de este componente tecnológico y así fortalecer la parte administrativa y operativa de la Policía Nacional.

Acuerdos internacionales y tratados de libre comercio:

Dando cumplimiento a lo contemplado en la SECCION IV SUBSECCION I acuerdo comerciales y trato Nacional del Decreto 1082 de 2015 (Modificado por Decreto 1676 de 2016), en la página web del Ministerio de Comercio Industria y Turismo se constató que la INTELIGENCIA DE AMENAZAS EN LA RED, por la suma TRES MIL NOVECIENTOS NOVENTA MILLONES DOSCIENTOS MIL PESOS M/CTE ($3.990.200.000,00), SI está cubierto bajo las obligaciones de carácter internacional, esto de acuerdo los criterios se relacionan a continuación según el Manual para el manejo de los Acuerdos Comerciales en Procesos de Contratación:

La mayoría de las Entidades Estatales del nivel nacional están obligadas por los Acuerdos Comerciales. De forma general están incluidos los Ministerios; los Departamentos Administrativos; las Superintendencias; los Establecimientos Públicos; las Unidades Administrativas Especiales; las Ramas Judicial y Legislativa; los Órganos de Control y la Organización Electoral.

La Decisión 439 de 1998 de la Secretaría de la CAN es aplicable a todos los Procesos de Contratación de las Entidades Estatales de nivel nacional, independientemente del valor del Proceso de Contratación.

Adicionalmente, algunas Entidades Estatales deben conceder trato nacional a los bienes y servicios extranjeros, según lo señalado en cada Acuerdo Comercial, sin que tengan que cumplir las demás obligaciones del Acuerdo Comercial.

La Entidad Estatal puede determinar si un Acuerdo Comercial es aplicable siguiendo las siguientes reglas en orden consecutivo:

Regla 1. Si la Entidad Estatal no hace parte de las Entidades Estatales incluidas en el Acuerdo Comercial, el Proceso de Contratación no está cubierto por este y, en consecuencia, no es necesario hacer análisis adicional alguno.

Regla 2. Si la Entidad Estatal está incluida en el Acuerdo Comercial y el presupuesto oficial del Proceso de Contratación es inferior al valor a partir del cual el Acuerdo Comercial es aplicable, el Proceso de Contratación no está cubierto y, en consecuencia, no es necesario hacer análisis adicional alguno.

Regla 3. Si la Entidad Estatal está incluida en el Acuerdo Comercial y el presupuesto oficial del Proceso de Contratación es superior al valor a partir del cual el Acuerdo Comercial es aplicable, la Entidad Estatal debe determinar si hay excepciones aplicables al Proceso de Contratación. Si hay excepciones, el Acuerdo Comercial no es aplicable al Proceso de Contratación. Si no hay excepciones, el Acuerdo Comercial es aplicable al Proceso de Contratación.

Acuerdo comercial		Entidad estatal incluida	Presupuesto del proceso de contratación superior al valor del acuerdo comercial	Exclusión aplicable al proceso de contratación	Proceso de contratación cubierto por el acuerdo comercial
Alianza Pacífico	Chile	SI	SI	NO	SI
	Perú	SI	SI	NO	SI
	México	SI	SI	NO	SI
Canadá y Colombia		SI	SI	NO	SI
Estados Unidos y Colombia		SI	SI	NO	SI
Corea y Colombia		SI	SI	NO	SI
Costa Rica y Colombia		SI	SI	NO	SI
Chile y Colombia		SI	SI	NO	SI
Israel y Colombia		SI	SI	NO	SI
Reino Unido Gran Bretaña E Irlanda Del Norte		SI	SI	NO	SI
Estados Unidos Mexicanos		SI	SI	NO	SI
Acuerdo de libre comercio entre Colombia y los estados AELC (EFTA - Suiza, Liechtenstein, Noruega e Islandia)		SI	SI	NO	SI
Unión Europea		SI	SI	NO	SI

Acuerdo comercial		Entidades generales del nivel nacional / Bienes y Servicios
Alianza Pacífico	Chile	$ 257.061.877 COP
	Perú	$ 488.417.566 COP
	México	$ 257.061.877 COP
Canadá y Colombia		$ 336.138.654 COP
Estados Unidos y Colombia		$ 337.737.809 COP
Corea y Colombia		$ 359.000.000 COP
Costa Rica y Colombia		$ 337.737.809 COP
Chile y Colombia		$ 255.459.239 COP
Israel y Colombia		Sección A Entidades de Nivel Central Bienes: Umbral: 130.000 DEG

	Valor en pesos del umbral = Valor umbral en DEG x TRM del día anterior a la fecha de publicación del aviso de convocatoria x Valor del DEG (USD por DEG)
Reino Unido Gran Bretaña E Irlanda Del Norte	$ 664.194.020 COP
Estados Unidos Mexicanos	$ 391.900.299 COP
Acuerdo de libre comercio entre Colombia y los estados AELC (EFTA - Suiza, Liechtenstein, Noruega e Islandia)	$ 696.380.112 COP
Unión Europea	$ 696.380.112 COP

Fuente: Ministerio de Comercio, Industria y Turismo

https://www.colombiacompra.gov.co/sites/cce_public/files/files_2020/umbrales_2022-2024_actualizada_vf_1.pdf

Nota 1: La información contenida en este documento fue elaborada por el Ministerio de Comercio Industria y Turismo – MINCIT y la Agencia Nacional de Contratación Pública – Colombia Compra Eficiente la pública por su importancia para las entidades públicas y los participantes en la contratación.

Nota 2: Según el Ministerio de Comercio Industria y Turismo – MINCIT el valor de los umbrales tendrá vigencia del 1 de enero del 2022 hasta el 31 de diciembre de 2023, excepto respecto de los Acuerdos Comerciales suscritos con la Unión Europea, México y los Estados AELC cuyos umbrales tendrán vigencia del 1 de enero de 2023 hasta el 31 de diciembre de 2024, y el Acuerdo Comercial suscrito con el Reino Unido de Gran Bretaña e Irlanda del Norte cuyos umbrales tendrán vigencia hasta el 31 de diciembre de 2023.

Nota 3: El Acuerdo Comercial entre Colombia y los países del Triángulo Norte de Centroamérica (El Salvador, Guatemala y Honduras) no se incluye en el presente documento dado que no se establecieron umbrales para su aplicabilidad.

Nota 4: Sin perjuicio de las particulares de la cobertura dispuesta por cada Acuerdo Comercial, por regla general, las entidades del nivel central corresponden a las entidades del sector nacional y las entidades del nivel subcentral corresponden a las entidades del sector territorial. En todo caso, se recuerda que las entidades estatales tienen la obligación de identificar los Acuerdos Comerciales aplicables a sus procesos de contratación.

2. ANTECEDENTES ADMINISTRATIVOS DEL PROCESO

Se consultó en la página **www.colombiacompra.gov.co,** con objeto igual y/o similar al presente estudio previo durante los últimos años celebrados por entidades públicas, encontrándose para la vigencia 2021 y 2022 los siguientes contratos:

UNIDAD CONTRATANTE Y CONTRATISTA	NÚMERO DEL CONTRATO Y FECHA DE SUSCRIPCIÓN	OBJETO	NÚMERO DE PROCESO	ACIERTOS	PROBLEMAS
COMANDO FUERZA AÉREA COLOMBIANA - IA CYBEREXPOSURE PLATFORM	079-00-A-COFAC-GOCOP-2022-28/07/2022	SUSCRIPCION A UN SERVICIO DE CIBERSEGURIDAD DE PROTECCION DIGITAL CON CAPACIDADES DE MEDICION DEL RIESGO	079-00-A-COFAC-GOCOP-2022	EL CONTRATO SE EJECUTÓ SIN CONTRATIEMPOS	NO SE PRESENTARON

		DE EXPOSICIÓN CIBERNÉTICA, MONITOREO DE MARCA Y CIBERINTELIGENCIA DE AMENAZAS			
COMANDO GENERAL DE LAS FUERZAS MILITARES - CCD COMPAÑIA DE CIBERSEGURIDAD Y DEFENSA SAS	207COGFM DIADF 2021- 03/09/2021	ACCESO PLATAFORMAS DE INTELIGENCIA DE AMENAZAS AVANZADAS	203COGFM DIADF 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

B. SELECCIÓN ABREVIADA. Reglada por el numeral 2 del Artículo 2 de la ley 1150 de 2007 y el Capítulo 2, Sección 1, Subsección 2 del Decreto 1082 de 2015, así:

"(...) La Selección abreviada corresponde a la modalidad de selección objetiva prevista para aquellos casos en que por las características del objeto a contratar, las circunstancias de la contratación o la cuantía o destinación del bien, obra o servicio, puedan adelantarse procesos simplificados para garantizar la eficiencia de la gestión contractual..."

En sujeción a la norma anterior, el numeral 2 del capítulo II de la Resolución No. 03049 de 2014, dispone:

"(...) Es una modalidad de selección objetiva prevista para aquellos casos en que por las características del objeto a contratar, las circunstancias de la contratación o la cuantía o destinación del bien, obra o servicio, pueden adelantarse procesos simplificados. Para efectos de esta modalidad de selección, el numeral 2º del artículo 2º de la Ley 1150 de 2007..."

Son causales de esta modalidad:

- **Selección Abreviada para la adquisición de Bienes y Servicios de Características Técnicas Uniformes:**

El literal a) del Numeral 2 del Artículo 2 de la ley 1150 de 2007, manifiesta:

"(...) La adquisición o suministro de bienes y servicios de características técnicas uniformes y de común utilización por parte de las entidades, que corresponden a aquellos que poseen las mismas especificaciones técnicas, con independencia de su diseño o de sus características descriptivas, y comparten patrones de desempeño y calidad objetivamente definidos.

Para la adquisición de estos bienes y servicios las entidades deberán, siempre que el reglamento así lo señale, hacer uso de procedimientos de subasta inversa o de instrumentos de compra por

catálogo derivados de la celebración de acuerdos marco de precios o de procedimientos de adquisición en bolsas de productos…"

Se aclara que las entidades estatales de la rama ejecutiva del poder público del orden nacional, obligadas a aplicar la ley 80 de 1993 y ley 1150 de 2007 o las normas que las modifiquen, aclaren, adicionen o sustituyan, están obligadas a adquirir Bienes y Servicios de características técnicas Uniformes a través de los Acuerdos marco de Precios vigentes.

Así la cosas y de conformidad con el artículo 2.2.1.2.1.2.9. del Decreto 1082 de 2015, Colombia Compra Eficiente deberá publicar el catálogo para Acuerdos Marco de Precios, y las entidades Estatales en la etapa de planeación del proceso de contratación están obligadas a verificar si existe un Acuerdo Marco de Precios vigente, con el cual la Entidad Estatal pueda satisfacer la necesidad identificada. De encontrarse el bien o servicio dentro del catálogo para Acuerdos Marco de Precios, las entidades Estatales enmarcadas dentro del inciso primero del Artículo 2.2.1.2.1.2.7. del Decreto 1082 de 2015, estarán obligas a suscribir el Acuerdo Marco de Precios, en la forma que Colombia Compra Eficiente disponga.

4. CRITERIOS DE SELECCIÓN

4.1. ESPECIFICACIONES TÉCNICAS MÍNIMAS

Las especificaciones técnicas requeridas serán evaluadas como **CUMPLE** o **NO CUMPLE** y están descritas en el presente estudio de conveniencia y oportunidad.

4.1.1. EXPERIENCIA PROPONENTE

La experiencia del proponente está descrita en el Anexo "ESPECIFICACIONES TÉCNICAS MÍNIMAS" del presente estudio previo, las cuales se verificarán como CUMPLE o NO CUMPLE.

El oferente, trátese de personas naturales o jurídicas, nacionales o extranjeras, domiciliadas o con sucursal en Colombia, fabricantes y/o comercializadores y/o distribuidores autorizados en Colombia, en forma individual o conjunta (consorcio, unión temporal o promesas de sociedad), deberán registrar experiencia en el Registro Único de Proponentes del Registro Único Empresarial de la Cámara de Comercio con jurisdicción en su domicilio principal, de conformidad con el Artículo 2.2.1.1.1.5.3., del Decreto 1082 de 2015.

Con el fin de garantizar la calidad de los bienes a adquirir y evitar incumplimientos en la ejecución del futuro contrato, se requiere acreditar experiencia en proyectos similares al objeto del presente estudio previo, según los códigos de clasificación de los bienes, obras o servicios (UNSPSC) en la clasificación 43222500 y/o 43233200, para lo cual el oferente deberá acreditar contratos realizados por valor igual o superior a 1724,13 SMMLV, de procesos adelantados con empresas públicas o privadas. Lo anterior se verificará mediante la presentación del Registro Único de Proponentes (RUP).

EXPERIENCIA ESPECIFICA DE LOS OFERENTES

Con el fin de garantizar la calidad de los productos, bienes y servicios, el cumplimiento en la ejecución del contrato, el oferente deberá presentar máximo tres (3) certificaciones de contratos (certificación por contrato) celebrados y ejecutados durante los últimos tres (3) años (2020 y/o 2021 y/o 2022), con entidades públicas y/o privadas, acreditando que cuenta con experiencia específica, directa y propia en la ejecución de contratos similares al objeto "INTELIGENCIA DE AMENAZAS EN LA RED" y/o "CIBERINTELIGENCIA DE AMENAZAS " y/o "INTELIGENCIA DE AMENAZAS AVANZADAS", que hayan sido ejecutados y terminados, y cuya suma o valor individual sea igual o superior al 50% del presupuesto oficial asignado.

En caso que la empresa haya implementado este tipo de bienes bajo reserva o confidencialidad, se hace necesario que certifiquen su experiencia especifica a través de un documento certificado ante un notario, en el cual se especifiquen los valores de los contratos celebrados y ejecutados durante los últimos tres (3) años (2020 y/o 2021 y/o 2022), el país o países donde ha realizado contratación, así como una comunicación emitida por una entidad del gobierno donde se indique que efectivamente la empresa cuenta con la experiencia, en desarrollo de procesos similares al objeto INTELIGENCIA DE AMENAZAS EN LA RED" y/o "CIBERINTELIGENCIA DE AMENAZAS " y/o "INTELIGENCIA DE AMENAZAS AVANZADAS".

Las certificaciones contendrán como mínimo la siguiente información:

-Entidad contratante
-Contratista
-Objeto del contrato
-Número de contrato (Si registra)
-Valor del contrato
-Fecha de inicio (día, mes y año).
-Fecha de terminación del contrato (día, mes y año)
-Nombre, firma y cargo de la persona que expide la certificación (representante legal o persona autorizada de la empresa que expide la certificación).
-Dirección y teléfono de la empresa que expide la certificación.

En caso de ser oferente extranjero, deberá diligenciar los formularios "CERTIFICACIÓN DE CONTRATOS PARA ACREDITACIÓN DE EXPERIENCIA PROPONENTE EXTRANJERO SIN SUCURSAL O DOMICILIO EN COLOMBIA" y "FORMULARIO EXPERIENCIA DEL PROPONENTE".

Este aspecto se verificará en el Anexo de Especificaciones Técnicas Mínimas.

4.1.2 NIVEL DE EDUCACIÓN O NIVEL ACADÉMICO

El nivel de educación está descrito en el Anexo "ESPECIFICACIONES TÉCNICAS MÍNIMAS" del presente estudio previo, las cuales se verificarán como CUMPLE o NO CUMPLE.

Con el fin de garantizar la idoneidad del personal que se vincula al presente proceso, el proponente deberá acreditar que el mismo cuente con la idoneidad, experiencia general y especifica suficiente, que garantice la calidad de las actividades a desarrollar definidas en las condiciones técnicas del presente proceso. Por consiguiente, el proponente deberá garantizar que para la instalación, implementación y configuración, cuenta con al menos un (1) ingeniero de sistemas y/o telecomunicaciones y/o áreas afines, con postgrado en seguridad de la información y/o seguridad informática y/o ciberinteligencia y/o afines, quien deberá tener el soporte de haber obtenido una o varias de las certificaciones que se relacionan a continuación.

-CISM (Certified Information Security Manager)
-CTIA (Certified Threat Intelligence Analyst)
-GCTI – GIAC Cyber Threat Intelligence
-RCIA – Rocheston Cyberthreat Intelligence Analyst
-CCTIA by the NICCS – Certified Cyber Threat Intelligence Analyst
-CTIP – Certified Threat Intelligence Professional
-Certified Threat Intelligence Analyst - Cyber Intelligence Tradecraft
-CPTIA – CREST Practitioner Threat Intelligence Analyst
-CRTIA – CREST Registered Threat Intelligence Analyst
-CCTIM – CREST Certified Threat Intelligence Manager
-MTIA - Certified Threat Intelligence Analyst
-OSCP - Offensive Security Certified Professional

Nota 1. El oferente deberá adjuntar en su propuesta, la copia verificable de la certificación realizada. No serán tenidas en cuenta certificaciones de asistencia

Nota 2. El oferente deberá adjuntar en su propuesta la copia legible del acta de grado o diploma expedido por entidad educativa reconocida por el Ministerio de Educación.

Nota 3. En caso de ser profesional extranjero deberá presentar certificado de homologación de su título profesional ante el Ministerio de Educación Nacional de Colombia.

Este aspecto se verificará en el Anexo de Especificaciones Técnicas Mínimas.

4.1.3 EXPERIENCIA

No aplica

4.1.4 EXPERIENCIA DEL PERSONAL

La experiencia del personal está descrita en el Anexo "ESPECIFICACIONES TÉCNICAS MÍNIMAS" del presente estudio previo, las cuales se verificarán como CUMPLE o NO CUMPLE.

Es importante para la Dirección de Inteligencia Policial que el personal profesional que integrará el equipo de trabajo cuente con la idoneidad, experiencia general y específica suficiente que

garantice la calidad de las actividades que se desarrollen sobre la infraestructura tecnológica descrita en el pliego de condiciones técnicas. Por consiguiente, el oferente deberá acreditar que durante los años: 2020 y/o 2021 y/o 2022, el profesional que presente en su oferta participó en proyectos relacionados al objeto del presente proceso, en los cuales éste haya tenido que instalar y/o implementar y/o configurar alguno de los sistemas relacionadas a continuación:

-SIEM (Security Information and Event Management)
-OpenCTI
-YETI
-MISP (Malware Information Sharing Platform)
-Sandbox – (Automated Malware Analysis)
-The Hive Project
-Cortex
-Herramientas CTI (Cyber Threat Intelligence)
-El producto ofertado por el oferente en el presente proceso.

Nota1. El oferente debe anexar a la propuesta, máximo tres (3) certificaciones de proyectos en los cuales, el profesional que presente en su oferta haya participado durante los últimos tres (3) años en la instalación y/o implementación y/o configuración de alguno de los sistemas arriba listados, con fechas anteriores a la apertura del presente proceso. Estas deben ser verificables, para lo cual deberá anexar en cada certificación emitida, los datos de contacto de las empresas donde se desarrollaron los proyectos.

Nota 2. El oferente deberá adjuntar en su propuesta copia de la tarjeta profesional que acredita la formación académica e idoneidad en el área específica del conocimiento. Esta no debe tener fecha menor a dos (2) años de expedición.

En caso de realizar cambio del personal implementador, el contratista deberá informar y solicitar al supervisor la aprobación del cambio, anexando la documentación que garantice la igualdad o mejora del perfil presentado en la propuesta.

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 deberá ser sustituido por el contratista por uno con iguales o mejores capacidades, condiciones y calificaciones a las presentadas en la oferta.

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

4.1.7 CONDICIONES TÉCNICAS ADICIONALES DE CALIFICACIÓN Y SU JUSTIFICACIÓN

No aplica.

4.2 EVALUACIÓN ECONÓMICA Y FINANCIERA

4.2.1 EVALUACIÓN ECONÓMICA

Los factores de evaluación económica están establecidos en el sobre No. 2 de la plataforma SECOP II.

4.2.2 FACTORES ADICIONALES DE CALIFICACIÓN Y SU JUSTIFICACIÓN:

No aplica

4.2.3 CRITERIOS DE DESEMPATE

En caso de empate se dará aplicabilidad a lo establecido en el artículo 35 de la ley 2069 del 2020 ARTÍCULO FACTORES DE DESEMPATE. En caso de empate en el puntaje total de dos o más ofertas en los Procesos de Contratación realizados con cargo a recursos públicos, los Procesos de Contratación realizados por las Entidades Estatales indistintamente de su régimen de contratación, así como los celebrados por los Procesos de Contratación de los patrimonios autónomos constituidos por Entidades Estatales, el contratante deberá utilizar las siguientes reglas de forma sucesiva y excluyente para seleccionar al oferente favorecido, respetando en todo caso los compromisos internacionales vigentes.

1. Preferir la oferta de bienes o servicios nacionales frente a la oferta de bienes o servicios extranjeros.

2. Preferir la propuesta de la mujer cabeza de familia, mujeres víctimas de la violencia intrafamiliar o de la persona jurídica en la cual participe o participen mayoritariamente; o, la de un proponente plural constituido por mujeres cabeza de familia, mujeres víctimas de violencia intrafamiliar y/o personas jurídicas en las cuales participe o participen mayoritariamente.

3. Preferir la propuesta presentada por el oferente que acredite en las condiciones establecidas en la ley que por lo menos el diez por ciento (10%) de su nómina está en condición de discapacidad a la que se refiere la Ley 361 de 1997. Si la oferta es presentada por un proponente plural, el integrante del oferente que acredite que el diez por ciento (10%) de su nómina está en condición de discapacidad en los términos del presente numeral, debe tener una participación de por lo menos el veinticinco por ciento (25%) en el consorcio, unión temporal o promesa de sociedad futura y aportar mínimo el veinticinco por ciento (25%) de la experiencia acreditada en la oferta.

4. Preferir la propuesta presentada por el oferente que acredite la vinculación en mayor proporción de personas mayores que no sean beneficiarios de la pensión de vejez, familiar o de sobrevivencia y que hayan cumplido el requisito de edad de pensión establecido en la Ley.

5. Preferir la propuesta presentada por el oferente que acredite, en las condiciones establecidas en la ley, que por lo menos diez por ciento (10%) de su nómina pertenece a población indígena, negra, afrocolombiana, raizal, palanquera, Rrom o gitanas.

6. Preferir la propuesta de personas en proceso de reintegración o reincorporación o de la persona jurídica en la cual participe o participen mayoritariamente; o, la de un proponente plural constituido por personas en proceso de reincorporación, y/o personas jurídicas en las cuales participe o participen mayoritariamente.

7. Preferir la oferta presentada por un proponente plural siempre que:

(a) esté conformado por al menos una madre cabeza de familia y/o una persona en proceso de reincorporación o reintegración, o una persona jurídica en la cual participe o participen mayoritariamente, y, que tenga una participación de por lo menos el veinticinco por ciento (25%) en el proponente plural;

(b) la madre cabeza de familia, la persona en proceso de reincorporación o reintegración, o la persona jurídica aporte mínimo el veinticinco por ciento (25%) de la experiencia acreditada en la oferta; y

(c) ni la madre cabeza de familia o persona en proceso de reincorporación o reintegración, ni la persona jurídica, ni sus accionistas, socios o representantes legales sean empleados, socios o accionistas de los miembros del proponente plural.

8. Preferir la oferta presentada por una MiPymes o cooperativas o asociaciones mutuales; o un proponente plural constituido por Mipymes, cooperativas o asociaciones mutuales.

9. Preferir la oferta presentada por el proponente plural constituido por micro y/o pequeñas empresas, cooperativas o asociaciones mutuales.

10. Preferir al oferente que acredite de acuerdo con sus estados financieros o información contable con corte a 31 de diciembre del año anterior, por lo menos el veinticinco por ciento (25%) del total de pagos realizados a MiPymes, cooperativas o asociaciones mutuales por concepto de proveeduría del oferente, realizados durante el año anterior; o, la oferta presentada por un proponente plural siempre que:

(a) esté conformado por al menos una MIPYME, cooperativa o asociación mutual que tenga una participación de por lo menos el veinticinco por ciento (25%);

(b) la MIPYME, cooperativa o asociación mutual aporte mínimo el veinticinco por ciento (25%) de la experiencia acreditada en la oferta; y

(c) ni la MIPYME, cooperativa o asociación mutual ni sus accionistas, socios o representantes legales sean empleados, socios o accionistas de los miembros del proponente plural.

11. Preferir las empresas reconocidas y establecidas como Sociedad de Beneficio e Interés Colectivo o Sociedad BIC, del segmento MIPYMES.

12. Utilizar un método aleatorio para seleccionar el oferente, método que deberá haber sido previsto previamente en los Documentos del Proceso.

PARÁGRAFO 1. Los factores de desempate serán aplicables en el caso de las cooperativas y asociaciones mutuales que cumplan con los criterios de clasificación empresarial, definidos por el Decreto 957 de 2019, priorizando aquellas que sean micro, pequeñas o medianas.

PARÁGRAFO 2. Para los criterios enunciados que involucren la vinculación de capital humano, el oferente deberá acreditar una antigüedad igual o mayor a un año. Para los casos de constitución inferior a un año se tendrá en cuenta a aquellos trabajadores que hayan estado vinculados desde el momento de constitución de la misma.

PARÁGRAFO 3. El Gobierno Nacional podrá reglamentar la aplicación de factores de desempate en casos en que concurran dos o más de los factores aquí previstos.

(Reglamentado por el Decreto 1860 de 2021)

5. CONDICIONES DEL CONTRATO

5.1. LUGAR DE ENTREGA O LUGAR DE PRESTACIÓN DEL SERVICIO

El objeto del presente proceso a adquirir deberá ser entregado en el Almacén de Telemática 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 forma de ejecución será en forma total, el contratista deberá entregar instalada y configurada la herramienta de acuerdo con las especificaciones técnicas establecidas en el presente estudio previo, dentro del plazo establecido para el presente proceso.

5.3. PLAZO DE EJECUCIÓN

El plazo de ejecución del contrato será hasta el 15 de julio del 2023, previa aprobación de la garantía única, plazo en el cual deberán quedar instaladas y configuradas la totalidad de las especificaciones técnicas mínimas.

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

La supervisión del contrato estará a cargo del Jefe del Área de Producción de Inteligencia de la Dirección de Inteligencia Policial 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 la Resolución No. 00090 del 15 de enero de 2018.

5.6. OBLIGACIONES DEL CONTRATISTA

Las obligaciones del contratista están descritas en el Anexo "OBLIGACIONES DEL CONTRATISTA".

5.7. OBLIGACIONES DE LA POLICÍA NACIONAL

Las obligaciones de la Policía Nacional están descritas en el Anexo "OBLIGACIONES DE LA POLICÍA NACIONAL".

6. FORMA Y PROCEDIMIENTO DE ADJUDICACIÓN

La adjudicación del contrato se debe hacer en forma total, esto teniendo en cuenta los aspectos técnicos, jurídicos y económicos.

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

La entidad deberá establecer la distribución del riesgo, de conformidad con lo previsto en el artículo 4º de la ley 1150 de 2007, para lo cual deberá hacer la estimación, tipificación y asignación de los riesgos previsibles involucrados en la contratación, de acuerdo con la naturaleza del Contrato y las actividades involucradas en él. Para estos efectos podrá usar como referencia el "Manual para la Identificación y Cobertura del Riesgo en los Procesos de Contratación (Versión 1)", publicado por la Agencia Nacional de Contratación – Colombia Compra Eficiente.

Como quiera que no se han realizado procesos de contratación con el mismo o similar ese objeto al del presente proceso en los años anteriores, la estimación del riesgo (probabilidad de ocurrencia del siniestro) corresponde a los porcentajes mínimos indicados dentro de la normatividad vigente, el Manual de Contratación para la Policía Nacional y las necesidades de la Institución, los cuales se relacionan en la "ESTIMACIÓN, TIPIFICACIÓN, ASIGNACIÓN DE RIESGOS Y DETERMINACIÓN DE GARANTÍAS" y "ANÁLISIS DEL RIESGO Y LA FORMA DE MITIGARLO" del presente estudio previo.

II ESTUDIO DEL SECTOR

1. ANÁLISIS DE LA DEMANDA

Con el uso exponencial de la tecnología en la actualidad, los fenómenos delictivos han encontrado en el uso del ciberespacio una oportunidad para converger. La cantidad de delitos informáticos han ido aumentado con el tiempo, impactando entidades públicas y privadas, cuya afectación se ve reflejada en sus usuarios, ante la falta de prestación del servicio y exposición de datos personales. Por otra parte, los ciberdelincuentes, hacen uso del ciberespacio como medio para llevar a cabo conductas delictivas, cuyo fin contempla escenarios desde el hurto por medios digitales, hasta el secuestro de información (ransomware). Ante este panorama, es imperioso que la Dirección de Inteligencia Policial cuente con una capacidad que permitirá la anticipación de estas conductas y así poder salvaguardar los activos críticos de los colombianos. De igual forma, evitar en la medida de las capacidades la impunidad en acciones que atenten contra la fuga de información y/o perdida de datos, ya que podrían generar un impacto negativo en cuanto al manejo y protección de los activos estratégicos de los colombianos.

Es por esto por lo que, se requiere una capacidad que permita al servicio de inteligencia contar con información relacionada con ciberamenazas que se presente en el direccionamiento IP colombiano o que pueda afectar el mismo. La información debe estar compuesta por: URL o direcciones IP maliciosas, perfil de actor, motivaciones, malware asociado junto con el detalle de la amenaza, hash, nombre, actor, vulnerabilidad, sectores afectados e impacto, phishing, comando y control del malware, spammer. La información recolectada servirá de insumo estratégico para coadyuvar a minimizar las infecciones y ataques cibernéticos, que puedan irrumpir en los sistemas o bases de datos que se utilizan en las entidades del Estado Colombiano reduciendo las brechas de seguridad, que puedan facilitar el acceso no autorizado a los servicios web críticos del Estado colombiano. Adicionalmente, permitirá identificar indicadores de compromiso con el propósito de recolectar información que conlleven a la toma de decisiones y creación de estrategias para combatir y minimizar el impacto de los ciberdelincuentes.

Esta recolección de información servirá como insumo para la creación de productos de inteligencia los cuales se difundirán de manera oportuna a los responsables de la ciberseguridad y

ciberdefensa del Estado y a las entidades del país categorizadas como infraestructuras críticas que puedan ser objeto de estos ataques informáticos, dado que en Colombia no existe tal tecnología en entidades del estado, la información entregada se enfocará en comandos y control de botnets, malware de zero day, gusanos, troyanos y amenazas avanzadas persistentes (APT).

La Dirección de Inteligencia Policial por medio del ciclo de inteligencia, tiene la función de identificar nuevos fenómenos delictivos, motivo por el cual y ante el incremento del uso del ciberespacio, debe estar en la vanguardia tecnológica en el proceso de inteligencia de amenazas cibernéticas, con el propósito de contrarrestar las acciones maliciosas que realizan diversos actores en el ciberespacio y de esta forma garantizar la confidencialidad, integridad y disponibilidad de la información de los ciudadanos colombianos, antes que se materialicen los incidentes informáticos.

Alineados al contexto y atendiendo las responsabilidades establecidas en las políticas públicas, como lo son las **Bases del Plan Nacional de Desarrollo 2022-2026 (PND 2022-2026) Colombia potencia mundial de la vida**, en el cual se concreta el inicio de una transición que debe desembocar en la paz total, que no es otra cosa que la búsqueda de una oportunidad para que todos podamos vivir una vida digna, basada en la justicia; es decir, en una cultura de la paz que reconoce el valor excelso de la vida en todas sus formas y que garantiza el cuidado de la causa común.

Uno de sus principales propósitos se denomina **la seguridad humana y justicia**, el cual dentro de los catalizadores para cumplir con su propósito enuncia textualmente los "***Habilitadores que potencian la seguridad humana y las oportunidades de bienestar",*** que a su vez en su numeral (8), define la necesidad de tener una **"Seguridad digital confiable para la garantía de las libertades, la protección de la dignidad y el desarrollo integral de las personas";** la cual se contempla en su literal (B) la "**Protección de las personas, de las infraestructuras digitales, fortalecimiento de las entidades del Estado y garantía en la prestación de sus servicios en el entorno digital**", con el propósito de diseñar e implementar "*…una estrategia para adelantar las medidas enfocadas a salvaguardar la infraestructura cibernética del país…"* (Planeación, 2022).

De igual forma, dentro del marco del CONPES 3995 "Confianza y Seguridad Digital" CONPES 3995 del 01 de julio de 2020 – Consejo Nacional de Política Económica y Social "*Política Nacional de Confianza y Seguridad Digital*" (Planeación, 2020). El cual tiene como objetivo general, "*Establecer medidas para desarrollar la confianza digital a través de la mejora de la seguridad digital de manera que Colombia sea una sociedad incluyente y competitiva en el futuro digital mediante el fortalecimiento de capacidades y la actualización del marco de gobernanza en seguridad digital, así como con la adopción de modelos con énfasis en nuevas tecnologías.*"

En su objetivo específico **5.3.1. Fortalecer las capacidades en seguridad digital de los ciudadanos, del sector público y del sector privado para aumentar la confianza digital en el país en la cual se define**, el diseño, estructura y presentación el proyecto de implementación del CSIRT del Sector Inteligencia, con el fin que contribuya en la protección de la seguridad digital nacional. Este proyecto buscará principalmente que este CSIRT del sector de inteligencia (i)

apoye la toma de decisiones en términos de valoración de los riesgos cibernéticos que se presenten en las entidades del sector y (ii) facilite la difusión de información técnica de alto valor de amenazas al Comité de Seguridad Digital referente a los distintos fenómenos que se generen en el Ciberespacio, acciones que en la actualidad son permanentes dentro de la Junta de Inteligencia Conjunta (JIC)

Asimismo, "el crecimiento que se observa de conductas delictivas en el ciberespacio en un comparado del 2021 al 2022 está por el orden de un 26%. Las conductas delictivas como se observa en la figura 1, tiene incrementos en los nueve (9) delitos definidos en la ley 1273 de 2009" (C4, 2022); sumado a esto incidentes de trascendencia nacional como vulneración de datos de la Fiscalía General de la Nación, Comando General de las Fuerzas Militares y empresas privadas como Colsanitas (Keralty) enciende una alarma para el Estado, en cuanto a cómo contrarrestar este tipo de conductas de manera preventiva, como ha sido mencionado en diferentes medios nacionales e internacionales ante la ocurrencia de incidentes informáticos.

Figura 1

Estadísticas del Centro de Capacidades para la Ciberseguridad de Colombia C4



Nota. Conductas delictivas en el ciberespacio comparativo 2021 al 2022. (C4, 2022).

Dado lo anterior, el ciclo de Inteligencia puede ser aplicado a los fenómenos delictivos que se presentan en el ciberespacio en pro de identificar, anticipar y contrarrestar las capacidades, intenciones y actividades de los ciberactores. Por tal razón, la Policía Nacional, a través del Servicio de Inteligencia Policial y su grupo Ciberinteligencia cuenta con capacidades de recolección de datos, en el despliegue de actividades de recolección técnica en el ciberespacio

que permiten identificar indicadores de compromiso (direcciones IP, hash, urls, entre otros) que son usados por ciberdelincuentes para cometer hechos delictivos. Ante eso y con el fin de mejorar las capacidades la Dirección de Inteligencia Policial debe llevar a cabo la adquisición de un componente que permita realizar inteligencia de amenazas en el ciberespacio, propósito del presente estudio previo, así:

Inteligencia de amenazas en la red: contar con una solución de datos globales integrados en un ambiente web (https) (dashboard live) que permita obtener en tiempo real información de al menos: actividad de actores, malwares activos, alertas de actividades de amenazas y creación de informes de inteligencia a partir de la información obtenida, para la toma de decisiones y creación de estrategias para contrarrestar los fenómenos delictivos en el ciberespacio. Los datos globales deben proporcionar información que permita identificar posibles ciberataques dirigidos y/o originados con(a) direccionamiento IP Colombiano, como también a nivel internacional, con objetivo de identificar los actores maliciosos que afecten los activos digitales de los ciudadanos.

Con base a lo anterior, la implementación del proceso permitirá la generación de alertas de inteligencia con indicadores de compromiso a las entidades encargadas de la protección del ciberespacio a partir de la recolección de información, con las cuales puedan generar acciones para contrarrestar las campañas de los actores maliciosos y asesorar al gobierno nacional en la creación de estrategias para la protección de los ciudadanos que hacen uso e interactúan en el ciberespacio.

Por otro lado, los lineamientos para la realización de actividades de inteligencia se encuentran descritos en la normatividad vigente, destacándose que de acuerdo con el **artículo 2° de la Ley 1621 de 2013** *"Por medio del cual se expiden normas para fortalecer el marco jurídico que permite a los organismos que llevan a cabo actividades de inteligencia y contrainteligencia cumplir con su misión Constitucional y legal, y se dictan otras disposiciones."*, la función de inteligencia y contrainteligencia enmarca la utilización de medios técnicos para la recolección, procesamiento, análisis y difusión de información, con el objetivo de proteger los derechos humanos, prevenir y combatir amenazas internas o externas, que dentro del contexto del presente proceso se enfoca a ciberamenazas que atenten contra la vigencia del régimen democrático, el régimen constitucional y legal, la seguridad y la defensa nacional, y cumplir los fines enunciados en el artículo 4° de dicha ley.

Además, no se podrá desarrollar una actividad de inteligencia y contrainteligencia por razones de género, raza, origen nacional o familiar, lengua, religión, opinión política o filosófica, pertenencia a una organización sindical o con fines partidistas, entre otros; y en especial, el ejercicio de ésta función estará limitada por el principio de reserva legal y compartimentación que garantiza la protección de los derechos a la honra, al buen nombre, a la intimidad personal y familiar, y al debido proceso.

En tal sentido, las actividades de recolección de información de inteligencia enmarcadas en el presente proceso, serán realizadas por la Dirección de Inteligencia Policial para afrontar las modalidades delictivas que convergen en el ciberespacio y de igual forma en el cumplimiento de

los fines establecidos para esta función estatutaria y en completa alineación con el ordenamiento jurídico vigente (Ley Estatutaria 1621 de 2013 Por medio del cual se expiden normas para fortalecer el marco jurídico que permite a los organismos que llevan a cabo actividades de inteligencia y contrainteligencia cumplir con su misión Constitucional y legal, y se dictan otras disposiciones., Decreto 1070 de 2015 Por el cual se establece el Decreto Único Reglamentario del Sector Administrativo de Defensa. y sentencia de constitucionalidad C-540 de 2012).

Tomado de C4, C. d. (20 de 12 de 2022). Conductas delictivas en el ciberespacio. (M. J. Pulido, Entrevistador)

Tomado de Representantes, C. (06 de 02 de 2023). Bases del *Plan Nacional de Desarrollo.* Obtenido de camara.gov.co: https://www.camara.gov.co/sites/default/files/2023-02/P.L.338-2023C%20%28PLAN%20NACIONAL%20DE%20DESARROLLO%29.pdf

ÍTEM	DESCRIPCIÓN	No. CANTIDAD ADQUIRIR	No. NECESIDAD	PORCENTAJE NECESIDAD
1	INTELIGENCIA DE AMENAZAS EN LA RED	1	1	100%

Para la consecución de este tipo de bienes se consideran de características técnicas uniformes y de común utilización, porque sus características técnicas son estándar en el mercado de telecomunicaciones e iguales para diferentes fabricantes del mercado, su utilización es común en todas las redes de comunicación corporativas y cumplen con especificaciones de servicios comunes, ofrecidos por los diferentes fabricantes y su utilización está definida con un propósito específico. Por lo anterior, diferentes oferentes pueden presentar los mismos productos y se requiere obtener el costo más favorable para la Entidad.

Es importante indicar, que con la contratación de los bienes se cumple con lo establecido en la normativa vigente frente a la austeridad del gasto, con base a lo estipulado en la directiva presidencial 08 del 17/09/22 "Directrices de austeridad hacia un gasto público eficiente".

Se consultó en la página www.colombiacompra.gov.co, con objeto igual y/o similar al presente estudio previo durante las vigencias 2019, 2020, 2021 y 2022 celebrados por la Policía Nacional para lo cual no se encontraron procesos, sin embargo, se relaciona un contrato similar realizado por la Fuerza Aérea Colombiana en la vigencia 2019, así:

DESCRIPCIÓN	VIGENCIA
	2019
MODALIDAD DE SELECCIÓN DEL CONTRATISTA	SELECCIÓN ABREVIADA menor cuantía
NÚMERO Y OBJETO DEL CONTRATO	079-00-A-COFAC-GOCOP-2022 SUSCRIPCION A UN SERVICIO DE CIBERSEGURIDAD DE PROTECCION DIGITAL CON CAPACIDADES DE MEDICION DEL RIESGO DE EXPOSICIÓN CIBERNÉTICA, MONITOREO DE MARCA Y CIBERINTELIGENCIA DE AMENAZAS
CANTIDAD DEL BIEN, OBRA O SERVICIO	20
AUTORIZACIONES PERMISOS Y LICENCIAS REQUERIDAS PARA SU EJECUCIÓN	NO APLICA
VALOR DEL CONTRATO	$846'612.335,2 en pesos colombianos
FORMA DE PAGO- CONDICIONES DE PAGO ESTABLECIDAS	Un pago con cargo al PAC diciembre 2022 posterior al recibo a satisfacción del 100% de los servicios por parte del supervisor inicio de la suscripción del servicio, presentación de la factura del contrato, y después de agotados todos los trámites administrativos a que haya lugar. 1. El pago al Contratista se realizará previa presentación de la facturación, el acta de recibo a satisfacción suscrito por el Supervisor del Contrato y demás trámites administrativos a que haya lugar. Por lo tanto, la Entidad no se

DESCRIPCIÓN	VIGENCIA 2019
	hace responsable por las demoras presentadas en el trámite para el pago al Contratista cuando ellas fueren ocasionadas por encontrarse incompleta la documentación de soporte o no ajustarse a cualquiera de las condiciones establecidas en el Contrato. 2. Para la realización de los pagos por parte del Ministerio de Defensa ± Fuerza Aérea Colombiana se requiere la acreditación, por parte del revisor fiscal o del representante legal (según aplique), de que el contratista se encuentra al día en el pago de los aportes al Sistema de Seguridad Social Integral y Parafiscales, cuando a ello haya lugar, dentro de los últimos seis (06) meses. Cuando de conformidad con lo establecido en el artículo 114-1 del Estatuto Tributario, las personas jurídicas o las personas naturales empleadoras se encuentren exentas de realizar los aportes al SENA e ICBF deberán presentar certificación en donde se manifieste dicha situación la cual se entenderá prestada bajo la gravedad del juramento. 3. La Entidad hará las retenciones a que haya lugar sobre cada pago, de acuerdo con las disposiciones legales vigentes sobre la materia.
PRESUPUESTO CON CARGO AL CUAL SE HAN SIDO EJECUTADOS	RECURSO 10
OFERENTES QUE HAN PARTICIPADO EN EL PROCESO	CSL, WEXLER S.A.S, AXON TECH S.A.S, NOVOPANGEA, PROCEWATERHOUSECOOPERS AG S.A.S
COMPORTAMIENTO DE LOS CONTRATISTAS E IMPOSICIÓN DE SANCIONES	SIN INCONVENIENTES
LUGARES DE ENTREGA ACORDADOS	DATACENTER ubicado en el Comando Aéreo de Transporte Militar, Puerta 6 Aeropuerto Internacional el Dorado, Bogotá D.C.
GARANTÍAS EXIGIDAS Y SINIESTROS	CUMPLIMIENTO DEL CONTRATO CALIDAD DE LOS BIENES
VIGENCIA DEL CONTRATO (PLAZO DE EJECUCIÓN)	Desde el perfeccionamiento del contrato y suscripción del acta de inicio hasta el 30 de septiembre de 2022.
LINK O NUMERO DE PROCESO	079-00-A-COFAC-GOCOP-2022

2. ANÁLISIS DEL MERCADO

DESCRIPCIÓN DEL MERCADO

La inteligencia de amenazas es el proceso de identificar y analizar ciberamenazas. El término "inteligencia de amenazas" puede hacer referencia a los datos reunidos sobre una potencial amenaza o al proceso de recopilar, procesar y analizar esos datos para comprender mejor las amenazas. (kaspersky, s.f.)

La inteligencia de amenazas consiste en revisar los datos, examinarlos en contexto para detectar problemas e implementar soluciones específicas para el problema encontrado. (kaspersky, s.f.)

Gracias a la tecnología digital, el mundo actual está más interconectado que nunca; sin embargo, esta mayor conectividad también ha traído aparejado un mayor riesgo de ciberataques, como vulneraciones de seguridad, robo de datos y malware. Un aspecto clave de la ciberseguridad es la inteligencia de amenazas. (kaspersky, s.f.)

Por tal razón en importante entender ¿Qué es la inteligencia de amenazas?, la definición de la inteligencia de amenazas suele confundirse con otros términos de ciberseguridad. Lo más habitual es que las personas confundan "datos de amenazas" con "inteligencia de amenazas" (kaspersky, s.f.), pero son dos conceptos diferentes:

Los datos de amenazas son una lista de posibles amenazas. Y la inteligencia de amenazas se centra en cuestiones más globales: examina los datos y el contexto más general para elaborar una narrativa que aporte información para la toma de decisiones. (kaspersky, s.f.)

Básicamente, la inteligencia de amenazas permite que las organizaciones tomen decisiones sobre la seguridad más rápido y con más información. Fomenta las acciones proactivas, en lugar de las reactivas, en la lucha contra los ciberataques. (kaspersky, s.f.)

La inteligencia de amenazas se vuelve importante y una "parte fundamental de cualquier ecosistema de ciberseguridad" (kaspersky, s.f.). Dado que, puede:

- ✓ "**Evitar la pérdida de datos:** con un programa CTI bien estructurado, las organizaciones pueden detectar las ciberamenazas y prevenir las filtraciones de datos con información confidencial" (kaspersky, s.f.).
- ✓ "**Proporcionar orientación sobre medidas de seguridad:** al identificar y analizar las amenazas, el programa CTI detecta los patrones que utilizan los hackers y ayuda a las organizaciones a implementar medidas de seguridad para protegerse contra ataques futuros" (kaspersky, s.f.).
- ✓ "**Informar a otras personas:** los hackers son cada vez más inteligentes. Para mantenerse informados, los expertos en ciberseguridad comparten las tácticas que conocen con otras personas de su comunidad para crear una base de conocimientos colectiva y luchar contra los delitos cibernéticos"(kaspersky, s.f.).

Tipos de inteligencia de amenazas

"La inteligencia de amenazas de ciberseguridad suele dividirse en tres categorías: estratégica, táctica y operativa" (kaspersky, s.f.). Veamos una por una:

Inteligencia de amenazas estratégica:

Suele ser un análisis de alto nivel pensado para un público no técnico; por ejemplo, el comité de dirección de una entidad pública o privada. Abarca temas de ciberseguridad que pueden afectar las decisiones empresariales más globales y tiene en cuenta las tendencias y las motivaciones generales. La inteligencia de amenazas estratégica a menudo se basa en códigos abiertos (es decir, a los que cualquier persona tiene acceso), como informes de los medios de comunicación, documentos técnicos e investigaciones. (kaspersky, s.f.)

Inteligencia de amenazas táctica:

Se centra en el futuro inmediato y está pensada para un público más técnico. Identifica indicadores de compromiso (IOC, por sus siglas en inglés) simples para que los equipos de TI puedan buscar y eliminar amenazas específicas en una red. Los IOC incluyen elementos como direcciones IP no válidas, nombres de dominios maliciosos conocidos, tráfico inusual, alertas de inicio de sesión o un aumento en las solicitudes de archivos/descargas. La inteligencia táctica es la forma de inteligencia más sencilla de generar y suele estar automatizada. En general, tiene una vida útil corta, ya que muchos IOC se vuelven obsoletos al poco tiempo. (kaspersky, s.f.)

Inteligencia de amenazas operativa:

Detrás de cada ciberataque, hay un "quién", un "por qué" y un "cómo". La inteligencia de amenazas operativa está pensada para responder estas preguntas mediante el estudio de los ciberataques anteriores y sacando conclusiones sobre la intención, el momento y la sofisticación. La inteligencia de amenazas operativas requiere más recursos que la inteligencia táctica y tiene una vida útil más larga. Esto es así porque los ciberatacantes no pueden cambiar sus tácticas, técnicas y procedimientos (conocidos como TTP) con la misma facilidad con que cambian sus herramientas, como un tipo de malware específico. (kaspersky, s.f.)

Ciclo de vida de la inteligencia de ciberamenazas

"Los expertos en ciberseguridad utilizan el concepto de un ciclo de vida en relación con la inteligencia de amenazas. Un ejemplo típico de un ciclo de vida de ciberamenazas incluye estas etapas: dirección, recopilación, procesamiento, análisis y difusión" (kaspersky, s.f.).

Tomado de kaspersky. (s.f.). *¿Qué es la inteligencia de amenazas? Definición y explicación*. Obtenido de kaspersky: https://latam.kaspersky.com/resource-center/definitions/threat-intelligence

DIRECTORIO DE SECOP II

https://community.secop.gov.co/Directory/CompanyProfiles/Network/Index

Consultado el directorio del SECOP II de las empresas del segmento: Software de seguridad y protección, equipo informático y accesorios, Software, bajo el código UNSPSC 43222500, se encuentran inscritas 888 firmas de origen colombiano, 01 de Japón y 01 de Brasil.

Consultado el directorio del SECOP II de las empresas del segmento: Software de seguridad y protección, equipo informático y accesorios, Software, bajo el código UNSPSC 43233200, se encuentran inscritas 955 firmas de origen colombiano, 01 Eslovaquia, 01 de Japón, 01 Costa Rica y 01 Argentina.

Consulta realizada el 11/01/2023.

Visión general del mercado

El mercado de servicios de seguridad de inteligencia de amenazas se valoró en USD 1863,48 millones en 2020 y se espera que alcance los USD 3829,77 millones para 2026, a una tasa compuesta anual del 12,9 % durante el período de pronóstico 2021 - 2026. Los servicios de inteligencia de amenazas se nutren de proveedores de servicios de seguridad que evolucionan sus capacidades de detección de amenazas para abordar el encuentro de detección de amenazas persistentes avanzadas (APT), ataques no identificados previamente, malware avanzado y otras amenazas. Las amenazas persistentes avanzadas son una nueva clase de malware. Sin embargo, en realidad, las amenazas persistentes avanzadas son una combinación de malware,

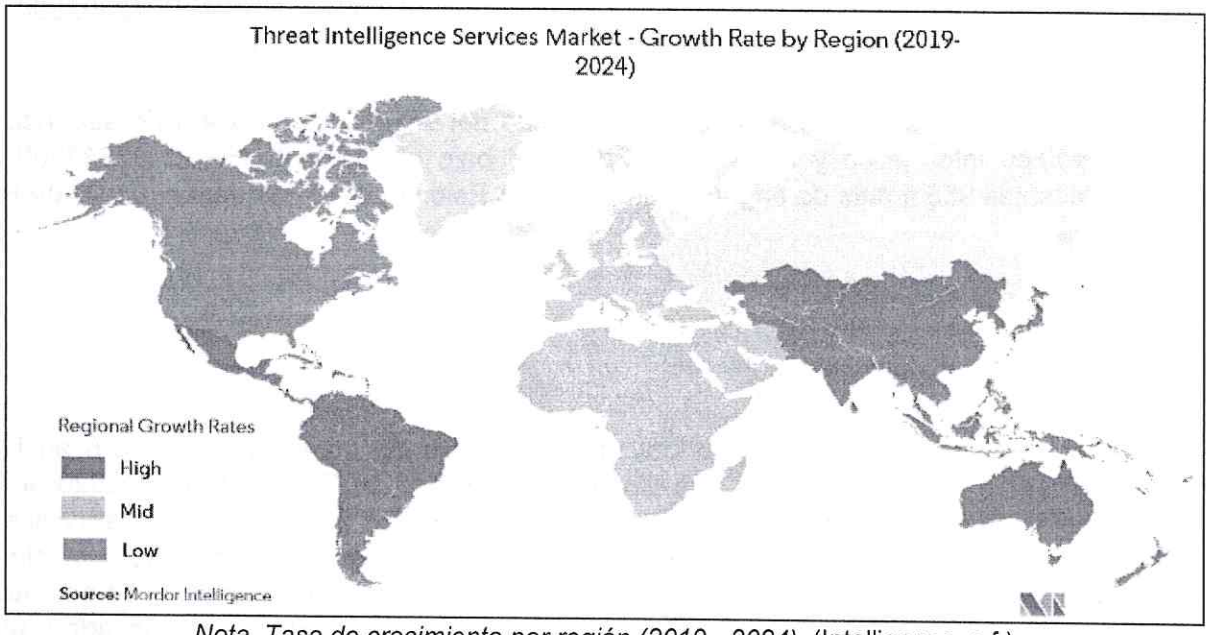
sistemas de entrega (como el phishing) y exfiltración de datos. La mayoría de los ataques de amenazas son desconocidos, de bajo objetivo, lentos y adaptables. (Intelligence, s.f.)

Las fuentes naturales para cuantificar el crimen son las estadísticas registradas por la policía. Sin embargo, en el contexto del delito cibernético, algunas limitaciones y advertencias ponen en duda las estadísticas registradas por la policía. La falta de consenso sobre lo que constituye un delito cibernético es uno de ellos. Como definición autorizada que falta, algunos delitos pueden clasificarse como cibernéticos cuando en realidad no lo son, mientras que otros pueden estar ocultos dentro de otras estadísticas delictivas. Por ejemplo, en Alemania, solo 64.426 de los 14,7 millones de incidentes de ciberdelincuencia estimados (0,4 %) llegaron a las estadísticas registradas por la policía en 2013. En los Estados Unidos, solo el 8 % de las víctimas de robo de identidad declararon haber presentado una denuncia. (Intelligence, s.f.)

En el sector de TI de EE. UU., se estimó que, en los últimos tres años la adopción de BYOD experimentó un aumento del 44,42 %, lo que representa la necesidad de adoptar servicios de inteligencia de amenazas. Además, el país cuenta con una sólida base de proveedores de servicios de inteligencia de amenazas, lo que se suma al crecimiento del mercado. Algunos de ellos incluyen Juniper Networks Inc., IBM Corporation, Cisco Systems Inc., FireEye y Symantec Corporation, entre otros. (Intelligence, s.f.)

Figura 3

Mercado de servicios de inteligencia de amenazas



Nota. Tasa de crecimiento por región (2019 - 2024). (Intelligence, s.f.)

Panorama competitivo

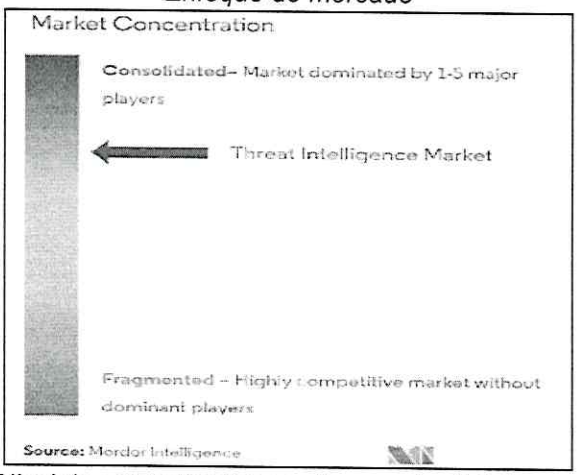
El mercado de inteligencia de amenazas es altamente competitivo y consta de varios jugadores importantes. En términos de cuota de mercado, pocos de los principales actores dominan actualmente el mercado. Estos jugadores importantes con acciones prominentes en el mercado se están enfocando en expandir su base de clientes en países extranjeros. Estas empresas están aprovechando las iniciativas estratégicas de colaboración para aumentar su cuota de mercado y su rentabilidad. Las empresas que operan en el mercado también se están asociando con nuevas empresas que trabajan en el mercado de inteligencia de amenazas para fortalecer las capacidades de sus productos. Sin embargo, para el caso de Colombia estas grandes casas matriz entregan la contratación a pequeños comercializadores locales. (Intelligence, s.f.)

Principales actores

- ✓ Redes de enebro, inc.
- ✓ Dell inc.
- ✓ Check Point Software Technologies Ltd.
- ✓ Fireeye, inc.
- ✓ Corporación IBM
- ✓ Google Inc
- ✓ Kasperky

Figura 3

Enfoque de mercado



Nota. Nivel de competidores en el mercado. (Intelligence, s.f.)

Tomado de: Intelligence, M. (s.f.). Mordor Intelligence. Obtenido de MERCADO DE SERVICIOS DE SEGURIDAD DE INTELIGENCIA DE AMENAZAS: CRECIMIENTO, TENDENCIAS, IMPACTO DE COVID-19 Y PRONÓSTICOS (2023 - 2028): https://www.mordorintelligence.com/es/industry-reports/threat-intelligence-security-services-market

3. ANÁLISIS DE LA OFERTA

IDENTIFICACIÓN DEL PROVEEDOR: Todas las personas naturales o jurídicas, nacionales o extranjeras, con apoderado o representante legal en Colombia, domiciliadas o con sucursal en Colombia, en forma individual o conjunta (consorcio o unión temporal), que tengan dentro de su objeto social o actividad la fabricación y/o comercialización y/o distribución autorizada por la casa fabricante de los bienes objeto del presente proceso, siempre y cuando cumplan con todos los requisitos exigidos para el mismo y se encuentren registradas en el SECOP II.

Para la identificación de proveedores se tomó contacto con las empresas que se relacionan a continuación:

- MNEMO COLOMBIA S.A.S Nit: 900396176-1
  Julian Andres Embus Ipia
  Teléfonos: 316 6604958
  Correo: r.rojasarias@mnemo.com; ja.embusipia@mnemo.com

- HISPASEC SISTEMAS S.L
  Francisco Collantes
  Teléfonos: +34 690 374417
  Correo: fcollantes@hispasec.com

- DATASEC S.A.S. Nit: 901223827-1
  Raiza Benítez
  Teléfonos: 320 3805020
  Correo: raiza.benitez@stssa-com.co

- INFRAESTRUCTURAS SEGURAS S.A.S.- NIT: 901188624-1
  Ramiro Merchán P.
  Teléfono 3153883821
  Correo: informacion@iseguras.com.co

4. MONEDA A CONTRATAR

La contratación se efectuará en moneda legal colombiana (pesos colombianos).

INDICADORES FINANCIEROS Y DE CAPACIDAD ORGANIZACIONAL

No	INDICADOR	CRITERIO DE SELECCIÓN
1	Liquidez	I L < 1.5 Excluyente
2	Nivel de Endeudamiento	I E > 0.65 Excluyente
3	Razón cobertura de interés	R C I < 2 Excluyente
4	Rentabilidad sobre Activo	R A < 0.08 Excluyente
5	Rentabilidad sobre Patrimonio	R P < 0.10 Excluyente

Para el caso de los Consorcios o Uniones Temporales la verificación financiera se realizará así:

Nota 1: para todos los indicadores de la capacidad financiera se obtendrá de la sumatoria de los valores de cada uno de los integrantes de la unión temporal o consorcio, afectada de manera proporcional al porcentaje de participación en la sociedad.

El proponente debe cumplir los porcentajes mínimos para todos y cada uno de los indicadores financieros que se establecen en el presente numeral. La Dirección de Inteligencia Policial ha establecido estos mínimos de tal forma que resultan proporcionales al objeto a realizar y a las características del contrato.

Si el oferente presenta gastos de interés en cero (0) serán habilitados, teniendo en cuenta que no tiene obligaciones financieras por cumplir y los proponentes que presenten una utilidad operacional negativa NO cumplirán con el indicador solicitado, al mostrar rendimientos negativos.

NOTA: Para efecto de verificar los indicadores financieros el proponente deberá aportar el Registro Único de Proponentes actualizado y en firme, de acuerdo a lo establecido con la parte 2 título 1 capítulo 1 sección 1 subsección 5 del Decreto 1082 de 2015.

En caso que el RUP se encuentre en el plazo de firmeza el oferente podrá participar en el proceso, pero en tal evento, el RUP debe estar en firme al momento previo de realización de la subasta en las modalidades de selección que admiten dicho procedimiento.

La anterior información se verificará con el registro único de proponentes RUP y se tendrá en cuenta los parámetros establecidos en el decreto 1041 del 21 de junio del 2022.

5. ANÁLISIS DE PRECIOS

5.1. PRECIOS REFERENCIA SECOP (OTRAS ENTIDADES)

ENTIDAD CONTRATANTE Y CONTRATISTA	OBJETO	NÚMERO DEL CONTRATO Y FECHA DE SUSCRIPCIÓN	NÚMERO DE PROCESO	VALOR
COMANDO FUERZA AÉREA COLOMBIANA - IA CYBEREXPOSURE PLATFORM	SUSCRIPCION A UN SERVICIO DE CIBERSEGURIDAD DE PROTECCION DIGITAL CON CAPACIDADES DE MEDICION DEL RIESGO DE EXPOSICIÓN CIBERNÉTICA, MONITOREO DE MARCA Y CIBERINTELIGENCIA DE AMENAZAS	CO1.PCCNTR.3798377 28/07/2022	079-00-A-COFAC-GOCOP-2022	$ 846.612.335,2
https://community.secop.gov.co/Public/Tendering/ContractDetailView/Index?UniqueIdentifier=CO1.PCCNTR.3798377&AwardContractDetailId=777801&IsFromMarketplace=False&IsFromContractNotice=True&isModal=true&asPopupView=true#GenericContractInformation				
COMANDO GENERAL DE LAS FUERZAS MILITARES - CCD COMPAÑIA DE CIBERSEGURIDAD Y DEFENSA SAS	ACCESO PLATAFORMAS DE INTELIGENCIA DE AMENAZAS AVANZADAS	CONTRATO 207COGFM DIADF 2021 3/09/2021	203COGFM DIADF 2021	$ 350.000.000
https://community.secop.gov.co/Public/Tendering/ContractDetailView/Index?UniqueIdentifier=CO1.PCCNTR.2778596&AwardContractDetailId=1465938&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

Se realizó consulta en la página www.colombiacompra.gov.co, para los años 2020, 2021 y 2022, y no se encontraron publicaciones de contratos en la Policía Nacional, con objeto igual o similar al requerido en el presente estudio previo.

- **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

Se verifico en plataformas de grandes marcas, pero no se encontraron precios al respecto, ya que la capacidad a adquirir está relacionada con bienes y servicios exclusivos que solo son comercializadas a la medida del comprador, por esta razón no se pueden adquirir a través de un catálogo.

De igual forma se procedió a verificar en el portal institucional de Colombia Compra, en el acuerdo marco de precios que contempla la venta de software (https://www.colombiacompra.gov.co/tienda-virtual-del-estado-colombiano/tecnologia/software-por-catalogo), en el cual no se encontraron bienes y servicios iguales o similares al objeto del presente proceso.

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

5.4. PRECIOS DE MERCADO

El 18/01/2023 a las 10:46 AM horas se publicó en el SECOP II el proceso de SOLICITUD DE COTIZACIÓN DIPOL-2023 002, con el fin de estructurar el estudio de mercado para el presente proceso, el 20/01/2023 a las 12:00 p.m., fue la fecha límite para responder a la solicitud de información obteniendo 05 cotizaciones por parte de los oferentes, es de resaltar que según la dinámica y forma de uso de la plataforma del SECOP II 1116 empresas estaban en la posibilidad de interesarse al proceso y cotizar, como se relaciona a continuación:

ÍTEM	DESCRIPCIÓN	MNEMO COLOMBIA S.A.S	INFRAESTRUCTURAS SEGURAS S.A.S	DATASEC S.A.S.	MENOR VALOR COTIZADO
1	SOFTWARE INTELIGENCIA DE AMENAZAS EN LA RED	$ 3.940.200.000	$ 4.359.000.000	$ 3.950.000.000	$ 3.940.200.000
2	SERVIDOR INTELIGENCIA DE AMENAZAS EN LA RED	$ 59.800.000	$ 61.000.000	$ 50.000.000	$ 50.000.000
	VALOR TOTAL	$ 4.000.000.000	$ 4.420.000.000	$ 4.000.000.000	$ 3.990.200.000

Nota 1: las cotizaciones relacionadas en el análisis de mercado se obtuvieron a través de una invitación a cotizar publicada en SECOP II.

Nota 2: se toma como referencia el menor valor del mercado, toda vez que representa el valor más favorable para la Entidad y que cumplen con las condiciones técnicas requeridas en el presente estudio previo.

Nota 3: los elementos de acuerdo a su utilización, desde el componente técnico se encuentran catalogados por la Oficina de Telemática en el numeral 3 literal n) Equipos, software y demás implementos de sistemas y comunicaciones para uso de las Fuerzas Militares y la Policía Nacional, del artículo 188 de la Ley 1819 del 29/12/2016, el cual modificó el artículo 477 del Estatuto Tributario, son bienes que no causan el impuesto sobre las ventas.

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

Proceso : INTELIGENCIA DE AMENAZAS EN LA RED - SOLICITUD COTIZACIÓN DIPOL-2023 002 (id:CO1.BDOS.3784141)

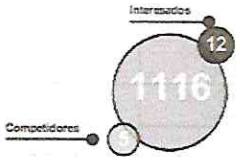
Solicitud de información a los Proveedores
SOLICITUD COTIZACIÓN DIPOL-2023 002 [En análisis]

Unidad de contratación GRUPO CONTRATOS DIPOL

INTELIGENCIA DE AMENAZAS EN LA RED

(Zona horaria (UTC-05:00) Bogotá, Lima, Quito)
Fecha de presentación de ofertas 20/01/2023 12:00 PM - **Fecha de publicación** 18/01/2023 10:48 AM

PROVEEDORES



LÍNEA DE TIEMPO

Fecha de publicación de concurso	Presentación de ofertas	Plazo para solicitar aclaraciones
18/01/2023	20/01/2023	20/01/2023

LISTA DE OFERTAS

Opciones

Referencia de oferta	Entidad	Presentada	Oferta
Oferta Procibernetica Dipol 2023	PROCIBERNETICA S.A.	20/01/2023 11:53 AM	5.500.000.000
PROPUESTA TECNICA VIRUS TOTAL HISPASEC SISTEMAS	HISPASEC SISTEMAS SL	20/01/2023 6:05 AM	753.453
EM-Datasec-Dipol-2	DATASEC S.A.S.	19/01/2023 11:23 AM	4.000.000.000
Oferta ISEGURAS PONAL	ISEGURAS	18/01/2023 4:48 PM	4.420.000.000
OFERTA DIPOL INTELIGENCIA DE AMENAZAS	MNEMO COLOMBIA SAS	18/01/2023 3:05 PM	4.000.000.000

5.5 ANÁLISIS DEL VALOR ESTIMADO

ÍTEM	DESCRIPCIÓN	PRECIO SECOP	PRECIOS DE CATÁLOGO	PRECIOS HISTÓRICOS PROYECTADOS	PRECIOS DE MERCADO	VALOR ESTIMADO
1	SOFTWARE INTELIGENCIA DE AMENAZAS EN LA RED	NO APLICA	NO APLICA	NO APLICA	$ 3.940.200.000	$ 3.940.200.000
2	SERVIDOR INTELIGENCIA DE AMENAZAS EN LA RED	NO APLICA	NO APLICA	NO APLICA	$ 50.000.000	$ 50.000.000
	VALOR TOTAL				$ 3.990.200.000	$ 3.990.200.000

Para el estudio previo no se tuvo en cuenta precios históricos, ni precios del SECOP y catalogo web; debido a que varían factores importantes como: especificaciones técnicas mínimas requeridas, cantidad, capacidad de equipo, la fluctuación del dólar el cual encarecen los de productos tecnológicos

- **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 para el presente proceso de contratación es TRES MIL NOVECIENTOS NOVENTA MILLONES DOSCIENTOS MIL PESOS ($3.990.200.000,00) EXENTO DE IVA, discriminado de la siguiente manera:

ÍTEM Y/O LOTE	RUBRO Y DESAGREGACIÓN PRESUPUESTAL	RECURSO	UNIDAD DE DESTINO	DESCRIPCIÓN	CANTIDAD	VALOR UNITARIO ESTIMADO, INLCUIDO IVA, EXENTO DE IVA O EXCLUIDO DE IVA SEGÚN CORRESPONDA	VALOR TOTAL ESTIMADO INLCUIDO IVA, EXENTO DE IVA O EXCLUIDO DE IVA SEGÚN CORRESPONDA
1	C-1501-0100-22-0-1501037-02	10	DIPOL	SOFTWARE INTELIGENCIA DE AMENAZAS EN LA RED	1	$ 3.940.200.000	$ 3.940.200.000
2	C-1501-0100-22-0-1501037-02	10	DIPOL	SERVIDOR INTELIGENCIA DE AMENAZAS EN LA RED	1	$ 50.000.000	$ 50.000.000
						VALOR TOTAL ESTIMADO	$ 3.990.200.000

Nota aclaratoria: ****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%***

Intendente **DIEGO FERNANDO PINTO PRADA**
Estructurador Estudio Previo

Mayor **JOHN ALBEIRO GUEVARA PULIDO**
Estructurador Estudio Previo

Teniente Coronel **OSCAR OCHOA SÁNCHEZ**
Jefe unidad dueña de la necesidad

Revisado por: IT. Diego pinto Prada/DIPOL-ARPIN
MY. John Guevara Pulido/DIPOL-ARPIN
TC. Oscar Ochoa Sánchez /DIPOL-ARPIN
TC. Marco Alexander Millán Sánchez/ DIPOL-SUDIR

Documentos Anexos al Estudio Previo:

Los documentos seleccionados en la siguiente lista, aplican para el proceso de Selección Abreviada con Subasta Inversa cuyo objeto es INTELIGENCIA DE AMENAZAS EN LA RED.

Aplica	Anexos
☐	Certificación de la necesidad (APLICA)
☐	Especificaciones técnicas mínimas (APLICA)
☐	Constancia de idoneidad y experiencia (NO APLICA)
☐	Estimación, tipificación, asignación de riesgos y determinación de garantías (APLICA)
☐	Análisis del riesgo y forma de mitigarlo. (APLICA)
☐	Ficha técnica (APLICA)
☐	Obligaciones de la policía nacional (APLICA)
☐	Obligaciones del contratista (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 (APLICA)
☐	Certificación de contratos para acreditación de experiencia proponente extranjero sin sucursal o domicilio en Colombia (APLICA)
☐	Clasificación proponente extranjero (APLICA)
☐	Acuerdo de confidencialidad (APLICA)
☐	Sistema de gestión de la seguridad y salud en el trabajo (APLICA)
☐	Compromiso anticorrupción(APLICA)
☐	Capacidad financiera
☐	Certificación de compromiso del fabricante y/o oferente
☐	Certificación de la capacidad técnica
☐	Personal, experiencia y tiempos de dedicación mínimos
☐	Carta de compromiso postventa

Otros documentos adjuntos al Estudio Previo

- ☐ Certificación plan de adquisición de compras No. 053 del 01/01/2023
- ☐ Comunicación oficial No. GS-2023-000294-OFITE-COTEL-GINTE 10.3, del 13 de enero de 2023, Acta No. 025 OFITE-GINTE 2.25 del 12/01/2023,
- ☐ Acta - 003 - DIPOL - PLANE - 2.21 que trata del mantenimiento del sistema de gestión ambiental y asesoramiento a los estructuradores de los estudios previos frente a la inclusión de las cláusulas ambientales.
- ☐ Acta 003 – DIPOL – GUTAH – 33.10 que trata del comité para la estructuración de las cláusulas del sistema de gestión de seguridad y salud en el trabajo a tener en cuenta en la estructuración de los estudios previos de la dirección de inteligencia policial
- ☐ Acta 003 – DIPOL – TELEM – 2.25 que trata de la mesa técnica asesora para requerimientos tecnológicos de la dirección de inteligencia No2, con el fin de estudiar la viabilidad de los proyectos "MANTENIMIENTOS VIDRIOS INTELIGENTES Y PERSIANA, ADQUISICIÓN INTELIGENCIA DE AMENAZAS EN LA RED, SOPORTE, MANTENIMIENTO PGP, SOPORTE Y ACUTALIZACIÓN, MANTENIMIENTO DLP"
- ☐ Solicitud de Cotizaciones
- ☐ Cotizaciones
- ☐ Justificación del margen mínimo

En mi calidad de Almacenista de Telemática de la Dirección de Inteligencia Policial, manifiesto con la suscripción de esta CERTIFICACIÓN que consultado el Inventario de Bienes del almacén de telemática de la DIRECCIÓN DE INTELIGENCIA POLICIAL no se cuenta con el software de Inteligencia de amenazas en la red, por lo cual se hace necesario adquirir el software 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	CANTIDAD ADQUIRIR	DÉFICIT %
1	1011257	No aplica	Software Inteligencia de amenazas en la red	1	0	1	100%
2	1044967	No aplica	Hardware Inteligencia de amenazas en la red	1	0	1	100%

Intendente **CESAR ARMANDO RUIZ QUIÑONEZ**
Almacenista de Telemática DIPOL

ÍTEM	REQUERIMIENTO MÍNIMO	CUMPLE	NO CUMPLE
1.	**SOFTWARE INTELIGENCIA DE AMENAZAS EN LA RED**		
1.1	Contar con una solución de datos globales integrados en un ambiente web (https) (dashboard live) que permita obtener en tiempo real información de al menos: la actividad de actores, malwares activos, alertas de actividades de amenazas e informes analizados por inteligencia. Los datos globales deben proporcionar información que permita identificar posibles ciberataques dirigidos y/o originados con (a) direccionamiento IP Colombiano. Los datos, aunque en primera medida deben estar enfocados al direccionamiento IP Colombiano también deberá traer en su dashboard, información relacionada con ciberamenazas que se presente de otros direccionamientos IP pero que puedan afectar el direccionamiento IP colombiano. La información debe ser recopilada de los centros de ciberinteligencia del oferente y esta debe tener como mínimo, lo siguiente: • URL o direcciones IP maliciosas Origen • Perfil de actor • Motivaciones, malware asociado • Descarga de malware (junto con el detalle de la amenaza, hash, nombre, actor, vulnerabilidad, impacto.) • Phishing • Comando y control • Spammer El oferente debe estar referenciado como referente en servicios de inteligencia de ciberamenazas, para lo cual debe presentar los soportes e informes que lo acrediten. En caso de ser líder del sector, se aceptan estudios de Forrester o Gartner, en los cuales debe estar claramente definido "inteligencia de ciberamenazas en la red" o similares. Junto con la propuesta se deberá anexar un documento emitido por casa matriz, en el cual se observe la correlación entre indicadores de compromiso del direccionamiento IP colombiano y que permita la descarga de archivos sospechosos, así como el cumplimiento de las demás especificaciones técnicas solicitadas en el presente proceso. Lo anterior deberá ser soportado con un acceso web que evidencie lo descrito en el documento.		
1.1.1	El oferente debe hacer entrega de un certificado de casa matriz en el que se certifique que la herramienta ofertada para la inteligencia de amenazas cumple con todos los requerimientos técnicos solicitados. Por lo anterior, el oferente debe especificar la marca de la herramienta a ofrecer, así: Marca: Especificar por el oferente		
1.2	El sistema deberá permitir realizar búsquedas de las ciberamenazas mínimo con los siguientes parámetros, así:		

	• Máscaras y URL Maliciosas • Hashes MD5 • Direcciones IP El sistema debe en detalle entregar información referente a **Reputación de IP**: conjunto de direcciones IP con un contexto que cubre hosts sospechosos y malintencionados **Direcciones URL maliciosas**: conjunto de direcciones URL formado por enlaces y sitios web malintencionados. En los cuales se pueda buscar en registros enmascarados y no enmascarados. **Direcciones URL de phishing:** conjunto de direcciones URL identificadas por la ciberinteligencia de la casa matriz como sitios de phishing. En los cuales se pueda buscar en registros enmascarados y no enmascarados. **Direcciones URL de C&C de malware**: conjunto de direcciones URL de servidores de comando y control (C&C) y objetos malintencionados relacionados. **Hashes de malware móvil:** conjunto de hashes de archivos para detectar objetos malintencionados que infectan plataformas móviles. **Fuente de datos sobre malware:** conjunto de hashes de troyanos con su contexto correspondiente para detectar troyanos para dispositivos móviles que cargan cobros a los usuarios móviles y que además permiten a un atacante robar, eliminar y responder mensajes. **Direcciones URL de C&C móviles de botnets:** conjunto de direcciones URL con contexto que contempla servidores C&C móviles de botnets. **Investigaciones Manuales:** La interfaz web debe permitir búsquedas y descargas manuales, para realizar análisis profundo de muestras y obtener indicadores adicionales, por medio de otras herramientas. Adicionalmente el oferente debe tener foros, redes sociales y contenido web, en los que se traten temáticas en tendencia de CTI.		
1.3	El sistema ofertado debe tener como mínimo lo siguiente, esto con el fin de contar con la mayor cantidad de información relacionada con ciber inteligencia que permita anticiparse a la posible materialización de amenazas en el direccionamiento IP Colombiano o con relación a este, así: • Una red de seguridad propia de identificación de amenazas, de la cual el oferente debe anexar un soporte con la cantidad de fuentes de las cuales recopilan información. Esto se debe anexar junto con la oferta • Partners de seguridad, enumerar en la propuesta cuales son. • Identificación de C&C o Botnets		

1.4	El sistema debe garantizar la confiabilidad de la inteligencia de amenazas, entregando siempre un contexto (detalle de la amenaza, hash, nombre, actor, vulnerabilidad, sectores afectados, impacto.) y permitir la definición de un puntaje (score) producido por algoritmos machine learning para transmitir la confianza de un indicador es benigno o malicioso. En donde 0 se considera benigno de alta confianza y 100 es maliciosos de alta confianza, según la escala de medición.		
1.5	La inteligencia de amenazas en la red se debe generar automáticamente y en tiempo real. Este debe tener como insumo de hallazgos a nivel mundial (mínimo en 100 países, esto debe ser soportado con una certificación de la casa matriz), información recopilada de la red de identificación de amenazas de la casa matriz que se presente en la oferta.		
1.6	El sistema debe entregar unos datos enriquecidos con el fin de dar más contexto a la inteligencia de amenazas relacionadas con: • Whois • DNS • GeoIP • Hosting • Atributos de archivos • Datos estadísticos y de comportamiento • Cadenas de descarga El sistema de inteligencia de amenazas debe contar con una infraestructura altamente tolerable a fallas, garantizar disponibilidades del sitio web de 99,99% al año.		
1.7	El sistema de inteligencia de amenazas debe utilizar técnicas de Threat Hunting, que hace referencia al proceso de búsqueda iterativa y *proactiva* a través de las redes para detectar y aislar amenazas avanzadas capaces de evadir las soluciones de seguridad existentes.		
1.8	El sistema de inteligencia de amenazas debe permitir crear reglas YARA de forma automática y configurar alertas que permitan la detección en tiempo real, de comportamientos que coincidan con dichas reglas. De igual forma debe permitir exportar las reglas YARA, para ser integradas en herramientas en herramientas SANDBOX propias. Adicionalmente debe permitir personalizar los reportes emitidos por la herramienta. De igual forma además que se cuenta con un acceso a nivel web, este debe permitir tener acceso a través de API, para integrar de forma programática todo el conjunto de datos y automatizar flujos de trabajo, como también el enriquecimiento de alertas basados en los indicadores de compromiso identificados, desplegables a herramientas perimetrales (SIEM, Firewall, SOAR, entre otros).		
1.9	El sistema de inteligencia de amenazas debe contar con un proceso de inspección y afinamiento el cual debe utilizar técnicas de preprocesamiento, como criterios estadísticos, sistemas de sandboxes, motores de heurística, herramientas de similitud y perfiles de comportamiento con entornos colaborativos.		

1.10	El sistema de inteligencia de amenazas deberá permitir realizar búsquedas históricas hasta de un año atrás, de igual forma deberá poder definir etiquetas o registros sobre cada una de las alertas enviadas, donde se evidencia, hora, fecha, comentario y usuario que realizó la gestión de la alerta de ciberinteligencia.		
1.11	El Sistema debe estar actualizado y configurado para detectar tácticas y técnicas enumeradas en el marco MITRE ATTACK, de igual forma los insumos de información deberán poderse categorizar en amenazas estratégicas, operacionales o tácticas.		
1.12	El sistema debe contar con correlación avanzada que involucre técnicas de analítica y/o *data science* para determinar tendencias o patrones anormales en el direccionamiento IP Colombiano. Adicionalmente, el sistema debe permitir configurar alertas de acuerdo con la necesidad del administrador, por ejemplo (alertas sobre direcciones IP específicas, dominios específicos, cyber crime, hacktivismo, entre otros). La herramienta debe mapear visualmente la correlación entre los indicadores de amenaza (archivos, URLs, dominios, IPs, entre otros. No se aceptan soluciones que requieran previamente un listado de archivos, URLs, dominios o IPs para su funcionamiento.		
1.13	El Sistema deberá permitir consumo de inteligencia de amenazas de fuentes públicas y por suscripción		
1.14	La interfaz web del Sistema debe contar con una interfaz Web GUI compatible con navegadores estándares tales como Chrome, EDGE, Firefox/Mozilla, entre otros.		
1.15	El sistema deberá permitir el acceso a diferentes tipos de reportes a través de la consola basada en GUI, sin uso de SQL por parte del usuario.		
1.16	El sistema debe contar con lo siguiente: • Acceso a la fuente de datos INTELX- IntelligenceX, la cual permita realizar búsquedas con un motor de búsqueda sobre archivos de datos global, alimentado desde múltiples fuentes, inclusive la dark web, durante todo el periodo de mantenimiento y soporte • Acceso a la fuente de datos Shodan, incluyendo la capacidad de búsqueda por vulnerabilidad, monitoreo y escaneo de hasta 65.000 direcciones IP, durante todo el periodo de mantenimiento y soporte • Debe tener selectores de búsqueda específicos como email, dominios, URL, dirección IP, entre otros. • Debe permitir realizar consulta de datos expuestos por cibercriminales, producto de ciberataques a los sistemas informáticos de las entidades. • Debe permitir identificar cuentas gubernamentales comprometidas en las filtraciones de datos llevadas a cabo por ciberdelincuentes, entre otras capacidades. • En caso de que la funcionalidad integrada sea descontinuada, se debe establecer junto con el supervisor del contrato las opciones para ser reemplazada.		
1.17	El sistema de inteligencia de amenazas debe contar adicionalmente con las siguientes características. • Realizar solicitudes de análisis de archivos con un conjunto de, al menos, 70		

	motores antivirus distintos, y recuperación de los resultados de dichos análisis. Estos resultados deben incluir información sobre el análisis propiamente dicho, como el archivo analizado o la fecha, y sobre cada motor antivirus utilizado (nombre del motor, versión, fecha de actualización de firmas, alias o nombre de la amenaza identificada). • Permitir la descarga de los archivos almacenados en el repositorio en base a su hash (MD5, SHA1 o SHA256) para que se puedan realizar procesamientos o análisis personalizados de los mismos. • Permitir consultas de información del comportamiento de archivos en entornos aislados con base a su hash (MD5, SHA1 o SHA256). • Permitir la realización de búsquedas de archivos con base a diferentes propiedades de los mismos (nombre, contenido, tamaño, cabeceras, tipo de fichero, firma digital, etc.), las detecciones de los antivirus, características estáticas, patrones de comportamiento y otros metadatos. • Contar con filtros de selección como país desde donde se adjuntó el archivo sospechoso, rango de fechas, cantidad de interacción con dominios o direcciones IP, palabras, entre otros, con el fin de identificar amenazas de forma específica.		
2	**SERVIDOR INTELIGENCIA DE AMENAZAS EN LA RED**		
2.1	El contratista debe entregar un servidor de aplicación con las siguientes características:		
2.2	Cantidad: uno (01)		
2.3	Marca: Especificar por el oferente		
2.4	Modelo: Especificar		
2.5	Tipo: Rack		
2.6	Año de fabricación: Mínimo 2021 última versión (todos los componentes del presente ítem).		
2.7	Software: Como sistema operativo debe incluir herramienta de virtualización, que permita la creación y gestión de máquinas virtuales, debidamente licenciado.		
2.8	Fuente de poder: 2 (dos) como mínimo, debe incluir cables de energía.		
2.9	Cantidad de procesadores mínima: 2(dos) como mínimo		
2.10	Tipo de procesador: Especificar		
2.11	Cantidad de núcleos por procesador: 12 (doce) como mínimo		
2.12	Frecuencia base procesador: 3Ghz como mínimo		
2.13	Memoria mínima procesador: 18 MB		
2.14	Memoria RAM: mínimo 128 GB tipo DDR4		
2.15	Almacenamiento: Mínimo 2 TB en SSD en RAID1 y mínimo 8 en HD en RAID 5		
2.16	Conectividad: 01 tarjeta de red de 10Gbps para conexión a la red LAN por fibra; 01 tarjeta de red de 1Gbps para administración. Debe incluir un cable de fibra y cable UTP.		
2.17	El oferente debe entregar la ficha técnica del servidor de aplicación ofertado.		
3	**SOPORTE Y MANTENIMIENTO**		

3.1	El contratista se compromete con la suscripción del presente documento a otorgar y mantener una garantía de fábrica de los bienes y servicios durante mínimo tres (03) años, a partir del recibo a satisfacción. Igualmente, para el cambio o restitución en caso de cualquier novedad, una vez instalados los bienes y servicios el tiempo de respuesta para algún inconveniente técnico será de 24 horas y para el cambio de un equipo por garantía debe ser máximo de tres (3) días hábiles, sin costo alguno para la Policía Nacional.		
3.2	El contratista deberá garantizar la correcta entrega y puesta en funcionamiento de cada uno de los elementos y servicios.		
3.3	El servicio de soporte telefónico debe 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.		
3.4	En caso de existir urgencia respecto a incidentes que involucren las soluciones ofertadas, el proveedor deberá proporcionar en caso de necesitarlo apoyo de casa matriz (presencial o virtual) hasta solucionar el incidente.		
3.5	Horario de atención de 7X24, para la atención de casos durante el periodo de garantía.		
3.6	El contratista deberá poner a disposición de la Policía Nacional, de manera permanente, los siguientes medios para el reporte de casos con fabricante: • Mesa de servicio o autoservicio con acceso vía web. • Número telefónico. • Correo electrónico.		
3.7	El sistema debe funcionar y contar con un soporte como también actualizaciones por un periodo mínimo de 3 años para todos sus componentes, contados a partir de la recepción del contrato por parte del supervisor.		
4	**TRANSFERENCIA DE CONOCIMIENTO**		
4.1	El contratista deberá realizar un entrenamiento para 10 funcionarios, los cuales deberán tener una duración de 48 horas. Entrenamiento con certificado de asistencia, brindado por el contratista con instructor en sitio con perfil idóneo para permitir la adquisición de conocimientos y habilidades referentes al manejo de las herramientas explicando su funcionalidad. Adicionalmente se deberán tratar las siguientes temáticas en la transferencia de conocimiento: • Entender claramente la inteligencia cibernética y la importancia de la capacidad de inteligencia de amenazas cibernéticas (CTI) • Explicar los conceptos del modelo de amenazas y por qué los usamos. • Indicar los conceptos básicos de la composición del malware. • Aplicar conocimientos en el manejo de las herramientas adquiridas. • Ejemplos de investigaciones CTI con las herramientas adquiridas y toma de notas detalladas del caso con sus aspectos relevantes.		
4.2	Todos los costos para el desarrollo de la transferencia de conocimiento estarán a cargo del contratista. Los entrenamientos deberán dictarse por entidades acreditadas y/o personal calificado con experiencia en los bienes o servicios ofrecidos.		

4.3	Se debe entregar certificación a cada asistente que participe en el curso.		
5	**AUDITORIAS**		
5.1	Con el fin de cumplir con protocolos de seguridad de la información, todo el sistema debe ser auditado con mínimo los siguientes registros: • IP del equipo que realiza las transacciones • fecha y hora legal • tipo de transacción • descripción de la transacción • nombre de usuario		
6	**ASPECTOS AMBIENTALES**		
6.1	El contratista deberá entregar los manuales de manera digital con el fin de aportar a la política cero papel establecida en directiva presidencial 04/2012.		
6.2	Desarrollar y cumplir, durante la vigencia y ejecución del objeto del contrato, con las buenas prácticas ambientales con relación al ahorro y uso eficiente del agua y la energía, así como el manejo integral de residuos (no peligrosos y peligrosos), establecidas por la Dirección y el marco del mantenimiento del Sistema de Gestión Ambiental en las instalaciones del contratante; que contribuyan al cumplimiento de la política ambiental y objetivos ambientales institucionales.		
7	**EXPERIENCIA DE PERSONAL IMPLEMENTADOR**		
7.1	Con el fin de garantizar la idoneidad del personal que se vincula al presente proceso, el proponente deberá acreditar que el mismo cuente con la idoneidad, experiencia general y especifica suficiente, que garantice la calidad de las actividades a desarrollar definidas en las condiciones técnicas del presente proceso. Por consiguiente, el proponente deberá garantizar que, para la instalación, implementación y configuración, cuenta con al menos un (1) ingeniero de sistemas y/o telecomunicaciones y/o áreas afines, con postgrado en seguridad de la información y/o seguridad informática y/o ciberinteligencia y/o afines, quien deberá tener el soporte de haber obtenido una o varias de las certificaciones que se relacionan a continuación. -CISM (Certified Information Security Manager) -CTIA (Certified Threat Intelligence Analyst) -GCTI – GIAC Cyber Threat Intelligence -RCIA – Rocheston Cyberthreat Intelligence Analyst -CCTIA by the NICCS – Certified Cyber Threat Intelligence Analyst -CTIP – Certified Threat Intelligence Professional -Certified Threat Intelligence Analyst - Cyber Intelligence Tradecraft -CPTIA – CREST Practitioner Threat Intelligence Analyst -CRTIA – CREST Registered Threat Intelligence Analyst -CCTIM – CREST Certified Threat Intelligence Manager -MTIA - Certified Threat Intelligence Analyst -OSCP - Offensive Security Certified Professional Nota 1. El oferente deberá adjuntar en su propuesta, la copia verificable de la certificación realizada. No serán tenidas en cuenta certificaciones de asistencia Nota 2. El oferente deberá adjuntar en su propuesta la copia legible del acta de grado o diploma expedido por entidad educativa reconocida por el Ministerio de Educación.		

	Nota 3. En caso de ser profesional extranjero deberá presentar certificado de homologación de su título profesional ante el Ministerio de Educación Nacional de Colombia.		
7.2	Es importante para la Dirección de Inteligencia Policial que el personal profesional que integrará el equipo de trabajo cuente con la idoneidad, experiencia general y específica suficiente que garantice la calidad de las actividades que se desarrollen sobre la infraestructura tecnológica descrita en el pliego de condiciones técnicas. Por consiguiente, el oferente deberá acreditar que durante los años: 2020 y/o 2021 y/o 2022, el profesional que presente en su oferta participó en proyectos relacionados al objeto del presente proceso, en los cuales éste haya tenido que instalar y/o implementar y/o configurar alguno de los sistemas relacionadas a continuación: -SIEM (Security Information and Event Management) -OpenCTI -YETI -MISP (Malware Information Sharing Platform) -Sandbox – (Automated Malware Analysis) -The Hive Project -Cortex -Herramientas CTI (Cyber Threat Intelligence) -El producto ofertado por el oferente en el presente proceso. Nota1. El oferente debe anexar a la propuesta, máximo tres (3) certificaciones de proyectos en los cuales, el profesional que presente en su oferta haya participado durante los últimos tres (3) años en la instalación y/o implementación y/o configuración de alguno de los sistemas arriba listados, con fechas anteriores a la apertura del presente proceso. Estas deben ser verificables, para lo cual deberá anexar en cada certificación emitida, los datos de contacto de las empresas donde se desarrollaron los proyectos. Nota 2. El oferente deberá adjuntar en su propuesta copia de la tarjeta profesional que acredita la formación académica e idoneidad en el área específica del conocimiento. Esta no debe tener fecha menor a dos (2) años de expedición.		
7.3	En caso de realizar cambio del personal implementador, el contratista deberá informar y solicitar al supervisor la aprobación del cambio, anexando la documentación que garantice la igualdad o mejora del perfil presentado en la propuesta.		
7.4	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 deberá ser sustituido por el contratista por uno con iguales o mejores capacidades, condiciones y calificaciones a las presentadas en la oferta.		
8	**DOCUMENTACIÓN TÉCNICA – ENTREGABLES**		
8.1	Se debe entregar totalmente documentada la metodología de implementación y configuración de los bienes y servicios ofertados siguiendo las recomendaciones de mejores prácticas de la casa matriz.		
8.2	Toda la documentación debe entregarse en idioma español y/o inglés.		
8.3	Para el acta de inicio del contrato se debe anexar el cronograma detallado de actividades, indicando actividad, tiempo y responsables de la ejecución del contrato.		

8.4	Manual de procedimientos de administración y operación de los bienes y servicio implementados		
9	**EXPERIENCIA DEL OFERENTE**		
9.1	El oferente, trátese de personas naturales o jurídicas, nacionales o extranjeras, domiciliadas o con sucursal en Colombia, fabricantes y/o comercializadores y/o distribuidores autorizados en Colombia, en forma individual o conjunta (consorcio, unión temporal o promesas de sociedad), deberán registrar experiencia en el Registro Único de Proponentes del Registro Único Empresarial de la Cámara de Comercio con jurisdicción en su domicilio principal, de conformidad con el Artículo 2.2.1.1.1.5.3., del Decreto 1082 de 2015. Con el fin de garantizar la calidad de los bienes a adquirir y evitar incumplimientos en la ejecución del futuro contrato, se requiere acreditar experiencia en proyectos similares al objeto del presente estudio previo, según los códigos de clasificación de los bienes, obras o servicios (UNSPSC) en la clasificación 43222500 y/o 43233200, para lo cual el oferente deberá acreditar contratos realizados por valor igual o superior a 1724,13 SMMLV, de procesos adelantados con empresas públicas o privadas. Lo anterior se verificará mediante la presentación del Registro Único de Proponentes (RUP).		
9.2	Con el fin de garantizar la calidad de los productos, bienes y servicios, el cumplimiento en la ejecución del contrato, el oferente deberá presentar máximo tres (3) certificaciones de contratos (certificación por contrato) celebrados y ejecutados durante los últimos tres (3) años (2020 y/o 2021 y/o 2022), con entidades públicas y/o privadas, acreditando que cuenta con experiencia específica, directa y propia en la ejecución de contratos similares al objeto "INTELIGENCIA DE AMENAZAS EN LA RED" y/o "CIBERINTELIGENCIA DE AMENAZAS " y/o "INTELIGENCIA DE AMENAZAS AVANZADAS", que hayan sido ejecutados y terminados, y cuya suma o valor individual sea igual o superior al 50% del presupuesto oficial asignado. En caso que la empresa haya implementado este tipo de bienes bajo reserva o confidencialidad, se hace necesario que certifiquen su experiencia especifica a través de un documento certificado ante un notario, en el cual se especifiquen los valores de los contratos celebrados y ejecutados durante los últimos tres (3) años (2020 y/o 2021 y/o 2022), el país o países donde ha realizado contratación, así como una comunicación emitida por una entidad del gobierno donde se indique que efectivamente la empresa cuenta con la experiencia, en desarrollo de procesos similares al objeto INTELIGENCIA DE AMENAZAS EN LA RED" y/o "CIBERINTELIGENCIA DE AMENAZAS " y/o "INTELIGENCIA DE AMENAZAS AVANZADAS". Las certificaciones contendrán como mínimo la siguiente información: -Entidad contratante -Contratista -Objeto del contrato -Número de contrato (Si registra) -Valor del contrato -Fecha de inicio (día, mes y año). -Fecha de terminación del contrato (día, mes y año) -Nombre, firma y cargo de la persona que expide la certificación (representante legal o		

	persona autorizada de la empresa que expide la certificación). -Dirección y teléfono de la empresa que expide la certificación. En caso de ser oferente extranjero, deberá diligenciar los formularios "CERTIFICACIÓN DE CONTRATOS PARA ACREDITACIÓN DE EXPERIENCIA PROPONENTE EXTRANJERO SIN SUCURSAL O DOMICILIO EN COLOMBIA" y "FORMULARIO EXPERIENCIA DEL PROPONENTE".		
9.3	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.		
9.4	Los contratos certificados deben estar registrados en el RUP.		
10	**CONFIDENCIALIDAD DE LA INFORMACIÓN**		
10.1	El contratista deberá entregar al supervisor del contrato una vez adjudicado el contrato la documentación requerida del personal que hará parte del proyecto e implementación de la nueva solución.		
10.2	Si la Policía Nacional, considera pertinente someter a estudio de seguridad al personal que prestará los servicios, el contratista permitirá y facilitará todos los medios que la Entidad le solicite para este fin.		
10.3	El Contratista se obliga a no suministrar información que obtenga o conozca con ocasión de la ejecución del presente contrato y que se encuentra marcada como confidencial; así como sobre los lugares a los cuales tenga acceso con ocasión de su servicio y sea revelada información marcada como confidencial. El contratista deberá firmar un acuerdo de confidencialidad y no revelación de la información.		
11	**SISTEMA DE GESTIÓN DE SEGURIDAD Y SALUD EN EL TRABAJO**		
11.1	El contratista deberá entregar al supervisor del contrato el documento firmado por el representante legal el cual indique el número de trabajadores permanentes y el nivel de riesgo de su principal actividad económica, lo anterior como consideración a la Resolución 0312 del 13 de febrero del 2019 del Ministerio de Trabajo "Por la cual se definen los Estándares Mínimos del Sistema de Gestión de SST", en cumplimiento al art. 1 la presente Resolución tiene por objeto establecer los Estándares Mínimos del SG-SST para las personas naturales y jurídicas señaladas en el art. 2 aplica a los empleadores públicos y privados, a los contratantes del personal bajo modalidad de contrato civil, comercial o administrativo, a los trabajadores dependientes e independientes, a las organizaciones de economía solidaria y del sector cooperativo a las agremiaciones u asociaciones que afilian trabajadores independientes al sistema de seguridad social integral, a las empresas de servicios temporales, a los estudiantes afiliados al Sistema General de Riesgos Laborales y los trabajadores en misión; a las administradoras de riesgos laborales; a la Policía Nacional en lo que corresponde a su personal no uniformado y al personal civil de las Fuerzas Militares; quienes deben implementar los Estándares Mínimos del Sistema de Gestión de SST en el marco del Sistema de Garantía de Calidad del Sistema General de Riesgos Laborales.		
11.2	El contratista deberá entregar al supervisor del contrato 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.		
11.3	El contratista deberá cumplir con los protocolos establecidos por el Ministerio de Salud y Protección Social en atención a la Resolución 1238 del 21/07/2022 "Por medio de la cual se dictan medidas para prevención, promoción y conservación de la salud con ocasión de infecciones respiratorias, incluidas las originadas por la COVID-19".		
11.4	El contratista deberá garantizar que el personal que desarrolla las tareas durante la ejecución del contrato cuente con los debidos Elementos de Protección Personal EPP, acorde a los peligros y riesgos relacionados la actividad contratada.		
11.5	El contratista garantizará que el personal que desarrolle la tarea durante la ejecución del contrato, se encuentre con la debida identificación de la empresa.		
11.6	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 supervisor del contrato, con el fin de que este haga llegar la copia al Grupo de Seguridad y Salud en el Trabajo de la Dirección de Inteligencia Policial, según lo establecido en la Resolución 1401 del 14/05/2007 del Ministerio de Trabajo y Protección Social "Por la cual se reglamenta la investigación de incidentes y accidentes de trabajo" o cualquiera que la modifique, reemplace o sustituya.		
11.7	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.		
11.8	En caso de que se desarrolle en la Dirección de Inteligencia Policial una auditoría del SG-SST durante la ejecución del contrato, el contratista deberá suministrar al supervisor del contrato la documentación requerida del objeto contractual.		

Intendente **DIEGO FERNANDO PINTO PRADA**
Estructurador estudio previo

Mayor **JOHN ALBEIRO GUEVARA PULIDO**
Estructurador Estudio Previo

Teniente Coronel **OSCAR OCHOA SÁNCHEZ**
Jefe unidad dueña de la necesidad

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.	OFERENTES	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 CUATRO (4) 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 TRES (03) AÑOS 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

Intendente **DIEGO FERNANDO PINTO PRADA**
Estructurador estudio previo

Mayor **JOHN ALBEIRO GUEVARA PULIDO**
Estructurador Estudio Previo

Teniente Coronel **OSCAR OCHOA SANCHEZ**
Jefe unidad dueña de la necesidad

ELABORACION DE ESTUDIOS PREVIOS PARA CONTRATOS

ANÁLISIS DEL RIESGO Y LA FORMA DE MITIGARLO

POLICÍA NACIONAL

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	Calificación total						¿Cómo se realiza el monitoreo?	Periodicidad ¿Cuándo?
1	GENERAL	EXTERNO	CONTRATACIÓN	ECONÓMICO	FLUCTUACIÓN EN EL PRECIO DEL DÓLAR SOBRE LA TASA REPRESENTATIVA DEL MERCADO	SOBRECOSTO EN LA ADQUISICIÓN, CON OCASIÓN DE LA IMPORTACIÓN DE BIENES	2	3	5	MEDIO	CONTRATISTA	EL CONTRATISTA EN SU OFERTA ECONÓMICA DEBERÁ CONTEMPLAR LAS VARIACIONES DE LA TASA REPRESENTATIVA DEL MERCADO, POR CUANTO EL PRESUPUESTO OFICIAL ASIGNADO, ES EN PESOS COLOMBIANOS	1	1	2	BAJO	SI	SI	CONTRATISTA	A PARTIR DE LA PRESENTACIÓN DE LA OFERTA	FINALIZACIÓN DEL CONTRATO	RECIBIDO SATISFACCIÓN	ACTA DE RECIBO SATISFACCIÓN
2	ESPECIFICO	EXTERNO	SELECCIÓN	OPERACIONAL	FALSEDAD EN LOS DOCUMENTOS QUE CONFORMAN LA OFERTA	DECLARATORIA DESIERTO DEL PROCESO DE CONTRATACIÓN	1	4	5	MEDIO	ENTIDAD	EVITAR EL RIESGO/VERIFICACIÓN ESTRICTA DE LOS DOCUMENTOS QUE CONFORMA LA OFERTA, POR PARTE DEL COMITÉ EVALUADOR	1	1	2	BAJO	SI	NO	INTEGRANTES DE LOS COMITÉS EVALUADORES (JURÍDICO, ECONÓMICO Y TÉCNICO)	DE ACUERDO A LA CRONOLOGÍA DEL PROCESO	DE ACUERDO A LA CRONOLOGÍA DEL PROCESO	EVALUACIONES	DE ACUERDO A LA CRONOLOGÍA DEL PROCESO
3	ESPECIFICO	EXTERNO	SELECCIÓN	OPERACIONAL	NO CUMPLIMIENTO DE LOS REQUISITOS HABILITANTES POR NINGÚN OFERENTE	DECLARATORIA DESIERTO DEL PROCESO DE CONTRATACIÓN	2	3	5	MEDIO	ENTIDAD	ESTABLECER ADECUADAMENTE LAS ESPECIFICACIONES TÉCNICAS EN EL ESTUDIO PREVIO	1	2	3	BAJO	SI	NO	ESTRUCTURADOR DEL ESTUDIO PREVIO	ELABORACIÓN DEL ESTUDIO PREVIO	ELABORACIÓN DEL ESTUDIO PREVIO	ESTUDIO PREVIO	EN LA APROBACIÓN DEL ESTUDIO PREVIO
4	GENERAL	EXTERNO	EJECUCIÓN	JURIDICO	QUE EL PERSONAL QUE REALICE EL PROCEDIMIENTO DE INSTALACIÓN NO SEA IDÓNEO PARA LA EJECUCIÓN DEL PROCESO	INSTALACIÓN Y/O FUNCIONAMIENTO NO ADECUADO DE LOS EQUIPOS	2	3	5	MEDIO	ENTIDAD	EL CONTRATISTA DEBERÁ GARANTIZAR DESDE LA PRESENTACIÓN DE LA OFERTA QUE CUENTA CON PERSONAL EXPERTO E IDÓNEO PARA EJECUTAR EL CONTRATO	1	1	2	BAJO	SI	SI	SUPERVISOR DEL CONTRATO	A PARTIR DE LA APROBACIÓN DE LA GARANTÍA ÚNICA	TERMINACIÓN DEL CONTRATO	INFORME AL ORDENADOR DEL GASTO	PERMANENTE

5	ESPECIFICO	EXTERNO	EJECUCIÓN	OPERACIONAL	QUE SE REALICE LA INSTALACIÓN DE LOS EQUIPOS Y NO SE DE CUMPLIMIENTO AL PROCEDIMIENTO TÉCNICO ESTABLECIDO POR CADA FABRICANTE	FALLA EN EL SISTEMA DE ALMACENAMIENTO	4	3	7	ALTO	CONTRATISTA	REDUCIR LA PROBABILIDAD DE OCURRENCIA, EL CONTRATISTA DURANTE LA EJECUCIÓN DEL CONTRATO DEBERÁ GARANTIZAR EL CUMPLIMIENTO AL PROCEDIMIENTO TÉCNICO ESTABLECIDO POR CADA FABRICANTE.	1	1	2	BAJO	SI	SI	SUPERVISOR DEL CONTRATO Y CONTRATISTA	INICIO DEL CONTRATO	TERMINACIÓN DEL CONTRATO	INFORME AL ORDENADOR DEL GASTO	PERMANENTE
6	ESPECIFICO	EXTERNO	EJECUCIÓN	OPERACIONAL	QUE EL PERSONAL REALICE TRABAJOS DE INSTALACIÓN, MANTENIMIENTO Y/O REPARACIÓN SIN EL DEBIDO CRONOGRAMA	NO SE REALICE LA INSTALACIÓN Y/O CONFIGURACIÓN A TODOS LOS EQUIPOS CONTEMPLADOS EN EL PRESENTE PROCESO	3	2	5	MEDIO	CONTRATISTA	REDUCIR LA PROBABILIDAD DE OCURRENCIA, EL SUPERVISOR DEL CONTRATO SOLICITARA AL CONTRATISTA UN CRONOGRAMA DE ACTIVIDADES	1	1	2	BAJO	SI	NO	SUPERVISOR DEL CONTRATO	INICIO DEL CONTRATO	TERMINACIÓN DEL CONTRATO	CUMPLIMIENTO ESPECIFICACIONES TÉCNICAS DEL ESTUDIO PREVIO	CRONOGRAMA DE TRABAJO

NOTA: Con la presentación de la oferta, el oferente acepta y aprueba los riesgos propuestos por la Policía Nacional, así como el análisis realizado por la Entidad para su mitigación y gestión, de igual forma corresponde al estructurador del estudio previo, analizar los riesgos a los cuales se expone la entidad y el oferente frente a la ejecución del contrato, por cuanto cada proyecto es único en los factores ambientales, económicos, políticos, sociales y tecnológicos.

Intendente **DIEGO FERNANDO PINTO PRADA**
Estructurador estudio previo

Mayor **JOHN ALBEIRO GUEVARA PULIDO**
Estructurador Estudio Previo

Teniente Coronel **OSCAR OCHOA SANCHEZ**
Jefe unidad dueña de la necesidad

FIRMA (firma del dueño de la necesidad y de quien o quienes realizan el análisis del riesgo y la forma de mitigarlo)

FICHA TÉCNICA DE PRODUCTO

DENOMINACIÓN DE BIEN O SERVICIO

INTELIGENCIA DE AMENAZAS EN LA RED

DENOMINACIÓN TÉCNICA DEL BIEN O SERVICIO

INTELIGENCIA DE AMENAZAS EN LA RED

UNIDAD DE MEDIDA

UNIDAD

DESCRIPCIÓN GENERAL

ÍTEM	REQUERIMIENTO MÍNIMO
1.	**SOFTWARE INTELIGENCIA DE AMENAZAS EN LA RED**
1.1	Contar con una solución de datos globales integrados en un ambiente web (https) (dashboard live) que permita obtener en tiempo real información de al menos: la actividad de actores, malwares activos, alertas de actividades de amenazas e informes analizados por inteligencia. Los datos globales deben proporcionar información que permita identificar posibles ciberataques dirigidos y/o originados con (a) direccionamiento IP Colombiano. Los datos, aunque en primera medida deben estar enfocados al direccionamiento IP Colombiano también deberá traer en su dashboard, información relacionada con ciberamenazas que se presente de otros direccionamientos IP pero que puedan afectar el direccionamiento IP colombiano. La información debe ser recopilada de los centros de ciberinteligencia del oferente y esta debe tener como mínimo, lo siguiente: • URL o direcciones IP maliciosas Origen • Perfil de actor • Motivaciones, malware asociado • Descarga de malware (junto con el detalle de la amenaza, hash, nombre, actor, vulnerabilidad, impacto.) • Phishing • Comando y control • Spammer El oferente debe estar referenciado como referente en servicios de inteligencia de ciberamenazas, para lo cual debe presentar los soportes e informes que lo acrediten. En caso de ser líder del sector, se aceptan estudios de Forrester o Gartner, en los cuales debe estar claramente definido "inteligencia de ciberamenazas en la red" o similares. Junto con la propuesta se deberá anexar un documento emitido por casa matriz, en el cual se observe la correlación entre indicadores de compromiso del direccionamiento IP colombiano y que permita la descarga de archivos sospechosos, así como el cumplimiento de las demás especificaciones técnicas solicitadas en el presente proceso. Lo anterior deberá ser soportado con un acceso web que evidencie lo descrito en el documento.
1.1.1	El oferente debe hacer entrega de un certificado de casa matriz en el que se certifique que la herramienta ofertada para la inteligencia de amenazas cumple con todos los requerimientos técnicos solicitados. Por lo anterior, el oferente debe especificar la marca de la herramienta a ofrecer, así: Marca: Especificar por el oferente

1.2	El sistema deberá permitir realizar búsquedas de las ciberamenazas mínimo con los siguientes parámetros, así: • Máscaras y URL Maliciosas • Hashes MD5 • Direcciones IP El sistema debe en detalle entregar información referente a **Reputación de IP**: conjunto de direcciones IP con un contexto que cubre hosts sospechosos y malintencionados **Direcciones URL maliciosas**: conjunto de direcciones URL formado por enlaces y sitios web malintencionados. En los cuales se pueda buscar en registros enmascarados y no enmascarados. **Direcciones URL de phishing:** conjunto de direcciones URL identificadas por la ciberinteligencia de la casa matriz como sitios de phishing. En los cuales se pueda buscar en registros enmascarados y no enmascarados. **Direcciones URL de C&C de malware**: conjunto de direcciones URL de servidores de comando y control (C&C) y objetos malintencionados relacionados. **Hashes de malware móvil:** conjunto de hashes de archivos para detectar objetos malintencionados que infectan plataformas móviles. **Fuente de datos sobre malware:** conjunto de hashes de troyanos con su contexto correspondiente para detectar troyanos para dispositivos móviles que cargan cobros a los usuarios móviles y que además permiten a un atacante robar, eliminar y responder mensajes. **Direcciones URL de C&C móviles de botnets:** conjunto de direcciones URL con contexto que contempla servidores C&C móviles de botnets. **Investigaciones Manuales:** La interfaz web debe permitir búsquedas y descargas manuales, para realizar análisis profundo de muestras y obtener indicadores adicionales, por medio de otras herramientas. Adicionalmente el oferente debe tener foros, redes sociales y contenido web, en los que se traten temáticas en tendencia de CTI.
1.3	El sistema ofertado debe tener como mínimo lo siguiente, esto con el fin de contar con la mayor cantidad de información relacionada con ciber inteligencia que permita anticiparse a la posible materialización de amenazas en el direccionamiento IP Colombiano o con relación a este, así: • Una red de seguridad propia de identificación de amenazas, de la cual el oferente debe anexar un soporte con la cantidad de fuentes de las cuales recopilan información. Esto se debe anexar junto con la oferta • Partners de seguridad, enumerar en la propuesta cuales son. • Identificación de C&C o Botnets
1.4	El sistema debe garantizar la confiabilidad de la inteligencia de amenazas, entregando siempre un contexto (detalle de la amenaza, hash, nombre, actor, vulnerabilidad, sectores afectados, impacto.) y permitir la definición de un puntaje (score) producido por algoritmos machine learning para transmitir la confianza de un indicador es benigno o malicioso. En donde 0 se considera benigno de alta confianza y 100 es maliciosos de alta confianza, según la escala de medición.
1.5	La inteligencia de amenazas en la red se debe generar automáticamente y en tiempo real. Este debe tener como insumo de hallazgos a nivel mundial (mínimo en 100 países, esto debe ser soportado con una certificación de la casa matriz), información recopilada de la red de identificación de amenazas de la casa matriz que se presente en la oferta.

1.6	El sistema debe entregar unos datos enriquecidos con el fin de dar más contexto a la inteligencia de amenazas relacionadas con: • Whois • DNS • GeoIP • Hosting • Atributos de archivos • Datos estadísticos y de comportamiento • Cadenas de descarga El sistema de inteligencia de amenazas debe contar con una infraestructura altamente tolerable a fallas, garantizar disponibilidades del sitio web de 99,99% al año.
1.7	El sistema de inteligencia de amenazas debe utilizar técnicas de Threat Hunting, que hace referencia al proceso de búsqueda iterativa y *proactiva* a través de las redes para detectar y aislar amenazas avanzadas capaces de evadir las soluciones de seguridad existentes.
1.8	El sistema de inteligencia de amenazas debe permitir crear reglas YARA de forma automática y configurar alertas que permitan la detección en tiempo real, de comportamientos que coincidan con dichas reglas. De igual forma debe permitir exportar las reglas YARA, para ser integradas en herramientas en herramientas SANDBOX propias. Adicionalmente debe permitir personalizar los reportes emitidos por la herramienta. De igual forma además que se cuenta con un acceso a nivel web, este debe permitir tener acceso a través de API, para integrar de forma programática todo el conjunto de datos y automatizar flujos de trabajo, como también el enriquecimiento de alertas basados en los indicadores de compromiso identificados, desplegables a herramientas perimetrales (SIEM, Firewall, SOAR, entre otros).
1.9	El sistema de inteligencia de amenazas debe contar con un proceso de inspección y afinamiento el cual debe utilizar técnicas de preprocesamiento, como criterios estadísticos, sistemas de sandboxes, motores de heurística, herramientas de similitud y perfiles de comportamiento con entornos colaborativos.
1.10	El sistema de inteligencia de amenazas deberá permitir realizar búsquedas históricas hasta de un año atrás, de igual forma deberá poder definir etiquetas o registros sobre cada una de las alertas enviadas, donde se evidencia, hora, fecha, comentario y usuario que realizó la gestión de la alerta de ciberinteligencia.
1.11	El Sistema debe estar actualizado y configurado para detectar tácticas y técnicas enumeradas en el marco MITRE ATTACK, de igual forma los insumos de información deberán poderse categorizar en amenazas estratégicas, operacionales o tácticas.
1.12	El sistema debe contar con correlación avanzada que involucre técnicas de analítica y/o *data science* para determinar tendencias o patrones anormales en el direccionamiento IP Colombiano. Adicionalmente, el sistema debe permitir configurar alertas de acuerdo con la necesidad del administrador, por ejemplo (alertas sobre direcciones IP específicas, dominios específicos, cyber crime, hacktivismo, entre otros). La herramienta debe mapear visualmente la correlación entre los indicadores de amenaza (archivos, URLs, dominios, IPs, entre otros. No se aceptan soluciones que requieran previamente un listado de archivos, URLs, dominios o IPs para su funcionamiento.
1.13	El Sistema deberá permitir consumo de inteligencia de amenazas de fuentes públicas y por suscripción
1.14	La interfaz web del Sistema debe contar con una interfaz Web GUI compatible con navegadores estándares tales como Chrome, EDGE, Firefox/Mozilla, entre otros.

1.15	El sistema deberá permitir el acceso a diferentes tipos de reportes a través de la consola basada en GUI, sin uso de SQL por parte del usuario.
1.16	El sistema debe contar con lo siguiente: • Acceso a la fuente de datos INTELX- IntelligenceX, la cual permita realizar búsquedas con un motor de búsqueda sobre archivos de datos global, alimentado desde múltiples fuentes, inclusive la dark web, durante todo el periodo de mantenimiento y soporte • Acceso a la fuente de datos Shodan, incluyendo la capacidad de búsqueda por vulnerabilidad, monitoreo y escaneo de hasta 65.000 direcciones IP, durante todo el periodo de mantenimiento y soporte • Debe tener selectores de búsqueda específicos como email, dominios, URL, dirección IP, entre otros. • Debe permitir realizar consulta de datos expuestos por cibercriminales, producto de ciberataques a los sistemas informáticos de las entidades. • Debe permitir identificar cuentas gubernamentales comprometidas en las filtraciones de datos llevadas a cabo por ciberdelincuentes, entre otras capacidades. • En caso de que la funcionalidad integrada sea descontinuada, se debe establecer junto con el supervisor del contrato las opciones para ser reemplazada.
1.17	El sistema de inteligencia de amenazas debe contar adicionalmente con las siguientes características. • Realizar solicitudes de análisis de archivos con un conjunto de, al menos, 70 motores antivirus distintos, y recuperación de los resultados de dichos análisis. Estos resultados deben incluir información sobre el análisis propiamente dicho, como el archivo analizado o la fecha, y sobre cada motor antivirus utilizado (nombre del motor, versión, fecha de actualización de firmas, alias o nombre de la amenaza identificada). • Permitir la descarga de los archivos almacenados en el repositorio en base a su hash (MD5, SHA1 o SHA256) para que se puedan realizar procesamientos o análisis personalizados de los mismos. • Permitir consultas de información del comportamiento de archivos en entornos aislados con base a su hash (MD5, SHA1 o SHA256). • Permitir la realización de búsquedas de archivos con base a diferentes propiedades de los mismos (nombre, contenido, tamaño, cabeceras, tipo de fichero, firma digital, etc.), las detecciones de los antivirus, características estáticas, patrones de comportamiento y otros metadatos. • Contar con filtros de selección como país desde donde se adjuntó el archivo sospechoso, rango de fechas, cantidad de interacción con dominios o direcciones IP, palabras, entre otros, con el fin de identificar amenazas de forma específica.
2	**SERVIDOR INTELIGENCIA DE AMENAZAS EN LA RED**
2.1	El contratista debe entregar un servidor de aplicación con las siguientes características:
2.2	Cantidad: uno (01)
2.3	Marca: Especificar por el oferente
2.4	Modelo: Especificar
2.5	Tipo: Rack
2.6	Año de fabricación: Mínimo 2021 última versión (todos los componentes del presente ítem).
2.7	Software: Como sistema operativo debe incluir herramienta de virtualización, que permita la creación y gestión de máquinas virtuales, debidamente licenciado.
2.8	Fuente de poder: 2 (dos) como mínimo, debe incluir cables de energía.
2.9	Cantidad de procesadores mínima: 2(dos) como mínimo
2.10	Tipo de procesador: Especificar
2.11	Cantidad de núcleos por procesador: 12 (doce) como mínimo
2.12	Frecuencia base procesador: 3Ghz como mínimo

2.13	Memoria mínima procesador: 18 MB
2.14	Memoria RAM: mínimo 128 GB tipo DDR4
2.15	Almacenamiento: Mínimo 2 TB en SSD en RAID1 y mínimo 8 en HD en RAID 5
2.16	Conectividad: 01 tarjeta de red de 10Gbps para conexión a la red LAN por fibra; 01 tarjeta de red de 1Gbps para administración. Debe incluir un cable de fibra y cable UTP.
2.17	El oferente debe entregar la ficha técnica del servidor de aplicación ofertado.
3	**SOPORTE Y MANTENIMIENTO**
3.1	El contratista se compromete con la suscripción del presente documento a otorgar y mantener una garantía de fábrica de los bienes y servicios durante mínimo tres (03) años, a partir del recibo a satisfacción. Igualmente, para el cambio o restitución en caso de cualquier novedad, una vez instalados los bienes y servicios el tiempo de respuesta para algún inconveniente técnico será de 24 horas y para el cambio de un equipo por garantía debe ser máximo de tres (3) días hábiles, sin costo alguno para la Policía Nacional.
3.2	El contratista deberá garantizar la correcta entrega y puesta en funcionamiento de cada uno de los elementos y servicios.
3.3	El servicio de soporte telefónico debe 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.
3.4	En caso de existir urgencia respecto a incidentes que involucren las soluciones ofertadas, el proveedor deberá proporcionar en caso de necesitarlo apoyo de casa matriz (presencial o virtual) hasta solucionar el incidente.
3.5	Horario de atención de 7X24, para la atención de casos durante el periodo de garantía.
3.6	El contratista deberá poner a disposición de la Policía Nacional, de manera permanente, los siguientes medios para el reporte de casos con fabricante: • Mesa de servicio o autoservicio con acceso vía web. • Número telefónico. • Correo electrónico.
3.7	El sistema debe funcionar y contar con un soporte como también actualizaciones por un periodo mínimo de 3 años para todos sus componentes, contados a partir de la recepción del contrato por parte del supervisor.
4	**TRANSFERENCIA DE CONOCIMIENTO**
4.1	El contratista deberá realizar un entrenamiento para 10 funcionarios, los cuales deberán tener una duración de 48 horas. Entrenamiento con certificado de asistencia, brindado por el contratista con instructor en sitio con perfil idóneo para permitir la adquisición de conocimientos y habilidades referentes al manejo de las herramientas explicando su funcionalidad. Adicionalmente se deberán tratar las siguientes temáticas en la transferencia de conocimiento: • Entender claramente la inteligencia cibernética y la importancia de la capacidad de inteligencia de amenazas cibernéticas (CTI) • Explicar los conceptos del modelo de amenazas y por qué los usamos. • Indicar los conceptos básicos de la composición del malware. • Aplicar conocimientos en el manejo de las herramientas adquiridas. • Ejemplos de investigaciones CTI con las herramientas adquiridas y toma de notas detalladas del caso con sus aspectos relevantes.
4.2	Todos los costos para el desarrollo de la transferencia de conocimiento estarán a cargo del contratista. Los entrenamientos deberán dictarse por entidades acreditadas y/o personal calificado con experiencia en los bienes o servicios ofrecidos.
4.3	Se debe entregar certificación a cada asistente que participe en el curso.

5	**AUDITORIAS**
5.1	Con el fin de cumplir con protocolos de seguridad de la información, todo el sistema debe ser auditado con mínimo los siguientes registros: • IP del equipo que realiza las transacciones • fecha y hora legal • tipo de transacción • descripción de la transacción • nombre de usuario

Intendente **DIEGO FERNANDO PINTO PRADA**
Estructurador estudio previo

Mayor **JOHN ALBEIRO GUEVARA PULIDO**
Estructurador Estudio Previo

Teniente Coronel **OSCAR OCHOA SANCHEZ**
Jefe unidad dueña de la necesidad

1. Poner a disposición del **CONTRATISTA** los bienes y lugares que se requieran para la ejecución y entrega del objeto contratado.

2. Una vez se surta el proceso de contratación estatal, asignar un supervisor, a través de quien la **POLICÍA NACIONAL** mantendrá la interlocución permanente y directa con el **CONTRATISTA**.

3. Ejercer el control sobre el cumplimiento del contrato a través del supervisor designado para el efecto, exigiéndole la ejecución idónea y oportuna del objeto a contratar.

4. Recibir a satisfacción los bienes y/o servicios que sean entregados por el **CONTRATISTA,** cuando estos cumplan con las condiciones establecidas y en especial las especificaciones u obligaciones técnicas contenidas en el anexo técnico.

5. Adelantar las gestiones necesarias para el reconocimiento y cobro de las sanciones pecuniarias y garantías a que hubiere lugar, para lo cual el supervisor dará aviso oportuno a la POLICÍA NACIONAL, sobre la ocurrencia de hechos constitutivos de mora o incumplimiento**.**

6. Pagar al **CONTRATISTA** en la forma pactada y con sujeción a las disponibilidades presupuestales y de PAC previstas para el efecto.

7. Tramitar diligentemente las apropiaciones presupuestales que requiera para solventar las prestaciones patrimoniales que hayan surgido a su cargo como consecuencia de la suscripción del contrato.

8. Solicitar y recibir información técnica respecto del bien o servicio y demás del **CONTRATISTA** en desarrollo del objeto del contractual.

9. Incluir aquellas obligaciones propias de cada proceso que coadyuven al cumplimiento de las obligaciones contractuales.

10. Rechazar los bienes y/o servicios cuando no cumplan con los requerimientos técnicos exigidos.

NOTA: además de las propias de su condición, deberá indicarse aquellas que correspondan a actividades o trámites a cargo de la administración, a partir de los cuales, el contratista estará obligado al cumplimiento de sus obligaciones contractuales.

En los procesos que se adelantan bajo el amparo de un Acuerdo Marco de Precios, deberá citarse la cláusula correspondiente a las obligaciones de la Entidad Compradora, contenida en la minuta del respectivo acuerdo marco.

1. Cumplir con el objeto contractual.

2. Obrar con lealtad y buena fe en las distintas etapas contractuales, evitando dilaciones y trabas.

3. Responder en los plazos que la **POLICÍA NACIONAL** establezca en cada caso, los requerimientos de aclaración o de información que le formule.

4. Cumplir cabalmente con sus obligaciones, frente al Sistema de Seguridad Social Integral y parafiscales (Cajas de Compensación Familiar, Sena e ICBF), por cuanto el cumplimiento de esta obligación es requisito indispensable para la realización de cualquier pago.

5. Constituir en debida forma y aportar al Grupo Contractual y Seguimiento de la Dirección de Inteligencia Policial o quien haga sus veces, dentro de los tres (3) días hábiles siguientes a la suscripción del contrato, la Garantía Única.

6. Guardar la confidencialidad de toda la información que le sea entregada y que se encuentre bajo su custodia o que por cualquier otra circunstancia deba conocer o manipular y responderá civil, penal y disciplinariamente por los perjuicios de su divulgación y/o utilización indebida que por sí o por un tercero se cause a la administración o a terceros.

7. No acceder a peticiones o amenazas, de quienes actuando por fuera de la ley pretendan obligarlo a hacer u omitir algún acto o hecho, el CONTRATISTA deberá Informar de tal evento a la Dirección de Inteligencia Policial de la Policía Nacional y a las autoridades competentes para que se adopte las medidas necesarias.

8. Mantener activa la cuenta corriente o de ahorros reportada para los pagos con el fin de evitar traumatismos en el proceso de ejecución del contrato.

9. Restituir a LA POLICÍA NACIONAL los elementos que haya colocado a su disposición para el desarrollo del objeto contractual, cuando se lo requiera o al finalizar el contrato, en caso de que se hayan suministrado.

10. CATALOGACIÓN. - EL CONTRATISTA deberá proporcionar la información necesaria para denominar, clasificar, identificar y numerar los artículos de abastecimiento relacionados y/o incluidos en el objeto del contrato, dentro del plazo y en las condiciones señaladas por el Supervisor, quien acreditará el cumplimiento de la presente cláusula, mediante un certificado en que conste la entrega total de la información requerida. La presente certificación será necesaria para la liquidación del contrato. Entendiéndose no finalizada la entrega de los bienes objeto del contrato, en tanto no se cumplan las obligaciones de la cláusula de catalogación.

11. Incluir todas aquellas obligaciones que el contratista debe cumplir con el fin de alinear la actividad contractual a las buenas prácticas en materia ambiental. Tener además en cuenta lo establecido en la resolución 03049 del 2014, *"Por medio del cual se adopta el Manual de Contratación de la Policía Nacional"*, actualizada, modificada y complementada por las Resoluciones Nos. 00090 del 2018 apéndice 1 y apéndice 2 del 2020.

12. Así mismo incluir las obligaciones en materia de Seguridad y Salud en el Trabajo y los lineamientos del gobierno nacional en el tema del COVID.

13. Para la facturación de los bienes o servicios contratados, se debe tener en cuenta los lineamientos y parámetros contemplados en la circular externa 016 del 09 de marzo de 2021 establecidos por el Ministerio de Hacienda y Crédito Público, por medio del cual se implementa el modelo de recepción de facturas de venta, notas débito y/o notas crédito, la cual es de obligatorio cumplimiento, de acuerdo con la Directiva Presidencial 09 del 17 de septiembre de 2020 "*Lineamientos para el Pago de Proveedores del Estado*" y la Resolución No. 000042 del 05 de mayo de 2020, "*Por la cual se desarrollan los sistemas de facturación, los proveedores tecnológicos*" y el registro de la factura electrónica de venta.

14. Las demás obligaciones del CONTRATISTA contenidas en el artículo 5º de la Ley 80 de 1993, así mismo, será civil y penalmente responsable por sus acciones u omisiones en la actuación contractual.

NOTA: se deben precisar claramente las obligaciones que con ocasión del contrato deberá cumplir el contratista, que sean relevantes en su cumplimiento. Para su concreción podrán usarse verbos como: realizar, entregar, ejecutar, suministrar, atender, etc. Así mismo actualizar los lineamientos relacionados con la normatividad cuando se generen cambios.

En los procesos que se adelantan bajo el amparo de un Acuerdo Marco de Precios, deberá indicarse la cláusula correspondiente a las obligaciones del proveedor en la operación secundaria, contenida en la minuta del respectivo acuerdo marco.

En el caso de servicios de mantenimiento de bienes inmuebles, se debe relacionar y referenciar las obligaciones contractuales contempladas en el modelo indicado por la dependencia institucional competente, conforme lo establecido en la guía *"Lineamientos para el mantenimiento de bienes inmuebles en la Policía Nacional"*.

ELABORACION DE ESTUDIOS PREVIOS PARA CONTRATOS	POLICÍA NACIONAL
FORMULARIO EXPERIENCIA DEL PROPONENTE	

Ciudad, seleccionar la fecha.

Señores.
POLICÍA NACIONAL – DILIGENCIAR LA UNIDAD A LA QUE PRESENTA LA OFERTA
Ciudad.

Referencia: experiencia del proponente del proceso de Elegir la modalidad de contratación., Número Diligenciar el número del proceso cuyo objeto es: Transcribir el objeto del proceso

RELACIÓN DE CONTRATOS CON LOS QUE CUMPLE EXPERIENCIA REGISTRADA EN EL RUP- EXPERIENCIA DEL PROPONENTE.

CONSECUTIVO	ENTIDAD CONTRATANTE	FECHA DE INICIO DD/MM/AA	FECHA DE TERMINACIÓN DD/MM/AA	MODALIDAD *			% PART	VALOR CONTRATO EXPRESADO EN SALARIOS MÍNIMOS (SMMLV)	FOLIO EN QUE SE ENCUENTRA LA CERTIFICACIÓN PRESENTADA EN LA OFERTA	FOLIO EN QUE SE ENCUENTRA REGISTRADA LA EXPERIENCIA EN EL RUP.
				I	UT	C				
1	Nombre del contratante	DD/MM/AA	DD/MM/AA	☐	☐	☐	%	00	00	00
2	Nombre del contratante	DD/MM/AA	DD/MM/AA	☐	☐	☐	%	00	00	00
3	Nombre del contratante	DD/MM/AA	DD/MM/AA	☐	☐	☐	%	00	00	00
4	Nombre del contratante	DD/MM/AA	DD/MM/AA	☐	☐	☐	%	00	00	00
5	Nombre del contratante	DD/MM/AA	DD/MM/AA	☐	☐	☐	%	00	00	00
TOTAL								00		

*** I: INDIVIDUAL, UT: UNIÓN TEMPORAL, C: CONSORCIO**

Nota: el diligenciamineto del presente formulario se hará conforme a las condiciones establacidas en el pliego de condiciones definitivo publicado por la entidad

_____
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

Ciudad, seleccionar la fecha.

Señores.
POLICÍA NACIONAL – DILIGENCIAR LA UNIDAD A LA QUE PRESENTA LA OFERTA
Ciudad.

Referencia: Certificación de contratos para acreditación de experiencia proponente extranjero sin sucursal o domicilio en Colombia, del proceso de Elegir la modalidad de contratación., Número Diligenciar el número del proceso cuyo objeto es: Transcribir el objeto del proceso

Contratos relacionados con la actividad de estudios en Moneda del País de Origen (A)	Contratos relacionados con la actividad estudios y diseños convertidos a Moneda Legal Colombiana (B)	Participación porcentual del proponente en el contratista plural (C)	Valor en Pesos Colombianos de los contratos ejecutados (valor del contrato ponderado por la participación) (D) (B * C) = D
Contrato	contrato	contrato	contrato
Contrato	contrato	contrato	contrato
Contrato	contrato	contrato	contrato
Contrato	contrato	contrato	contrato
Contrato	contrato	contrato	contrato
Total		Contrato	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

_____
Firma del Contador público y/o Revisor fiscal
Nombre: Diligenciar el nombre completo del proponente
Identificación (C.C ☐ C.E. ☐) Diligenciar el documento de identificación del representante legal
Cargo: Diligenciar cargo
Número de la Tarjeta Profesional: Diligenciar el número de la tarjeta profesional

NOTA: los representantes de los integrantes del Oferente plural deben suscribir cada uno el presente documento

Ciudad, seleccionar la fecha.

Señores.
POLICÍA NACIONAL – DILIGENCIAR LA UNIDAD A LA QUE PRESENTA LA OFERTA
Ciudad.

Referencia: Clasificación del proponente extranjero de Elegir la modalidad de contratación., Número Diligenciar el número del proceso cuyo objeto es: Transcribir el objeto del proceso

El suscrito declaro bajo gravedad de juramento acorde a la actividad comercial desarrollada, o al objeto social de la empresa que represento, que me encuentro facultado para ejercer las actividades comerciales propias a cada actividad, especialidad y grupo descrito en el pliego de condiciones "Clasificación en el Registro Único de Proponentes", así

SEGMENTO	FAMILIAS	CLASES
Segmento	Familia	Clases

Autorizo a la Unidad Ejecutora de la Policía Nacional para verificar la información suministrada.

Atentamente,

_____
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

Ciudad, seleccionar la fecha

Señores.
POLICÍA NACIONAL – DILIGENCIAR LA UNIDAD A LA QUE PRESENTA LA OFERTA
Ciudad.

Referencia: Acuerdo de confidencialidad del proceso de Elegir la modalidad de contratación., Número Diligenciar el número del proceso cuyo objeto es: Transcribir el objeto del proceso

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 Elegir la modalidad de contratación, para la celebración de un contrato estatal para. Transcribir el objeto del proceso.

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

Ciudad, seleccionar la fecha

Señores.
POLICÍA NACIONAL – DILIGENCIAR LA UNIDAD A LA QUE PRESENTA LA OFERTA
Ciudad.

Referencia: presentación sistema de gestión de la seguridad y salud en el trabajo para el proceso de Elegir la modalidad de contratación. Número Diligenciar el número del proceso cuyo objeto es: Transcribir el objeto del proceso

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

Ciudad, seleccionar la fecha.

Señores.
POLICÍA NACIONAL – DILIGENCIAR LA UNIDAD A LA QUE PRESENTA LA OFERTA
Ciudad.

Referencia: Compromiso anticorrupción del proceso de Elegir la modalidad de contratación., Número Diligenciar el número del proceso cuyo objeto es: Transcribir el objeto del proceso

El (los) suscrito(s) a saber Nombre del representante legal de la sociedad, asociación, persona jurídica, consorcio, unión temporal .: domiciliado en Domicilio 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 - DILIGENCIAR LA UNIDAD A LA QUE PRESENTA LA OFERTA, 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 - DILIGENCIAR LA UNIDAD A LA QUE PRESENTA LA OFERTA 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.

Ciudad, seleccionar la fecha.

Señores.
POLICÍA NACIONAL – DILIGENCIAR LA UNIDAD A LA QUE PRESENTA LA OFERTA
Ciudad.

Referencia: Cuadro de capacidad financiera del proceso de Elegir la modalidad de contratación., Número Diligenciar el número del proceso cuyo objeto es: Transcribir el objeto del proceso

La solicitud de las vigencias a tener en cuenta, se realizará de acuerdo a las normas vigentes, debiéndose realizar los ajustes acordes a la misma, por el estructurador del estudio previo, cuando se generen cambios

PROPONENTE	ACTIVO CORRIENTE	ACTIVO TOTAL	PASIVO CORRIENTE	PASIVO TOTAL
	$ 20XX-000.000.000,00	$ 20XX-000.000.000,00	$ 20XX-000.000.000,00	$ 20XX-000.000.000,00
	$ 20XX-000.000.000,00	$ 20XX-000.000.000,00	$ 20XX-000.000.000,00	$ 20XX-000.000.000,00
	$ 20XX-000.000.000,00	$ 20XX-000.000.000,00	$ 20XX-000.000.000,00	$ 20XX-000.000.000,00

PROPONENTE	UTILIDAD OPERACIONAL	GASTOS DE INTERESES	PATRIMONIO
	$ 20XX-000.000.000,00	$ 20XX-000.000.000,00	$ 20XX-000.000.000,00
	$ 20XX-000.000.000,00	$ 20XX-000.000.000,00	$ 20XX-000.000.000,00
	$ 20XX-000.000.000,00	$ 20XX-000.000.000,00	$ 20XX-000.000.000,00

Para el diligenciamiento del siguiente cuadro, en el caso de proponentes extranjeros, deberán realizar la conversión de la moneda según corresponda al pais, a dólares y posteriormente a pesos colombianos.

Proponente	Liquidez	Nivel de endeudamiento	Capital de trabajo	Razón de cobertura de intereses	Rentabilidad del patrimonio	Rentabilidad del activo
Nombre del proponente	Activo corriente sobre pasivo corriente	Pasivo total sobre activo total	Activo corriente menos pasivo corriente	Utilidad operacional dividida por los gastos de intereses	Utilidad operacional dividida por el patrimonio	Utilidad operacional dividida por el activo total
RESULTADO	%	%	%	%	%	%

Declaramos bajo la gravedad de juramento, comprometiendo nuestra responsabilidad personal y comprometiendo la responsabilidad institucional de las personas jurídicas que representamos, que la información antes consignada es totalmente cierta, corresponde única y exclusivamente a la entidad que representamos.

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

_____

Firma del Contador público y/o Revisor fiscal
Nombre: Diligenciar el nombre completo del proponente
Identificación (C.C ☐ C.E. ☐) Diligenciar el documento de identificación del representante legal
Cargo: Diligenciar cargo

JUSTIFICACIÓN DEL MARGEN MÍNIMO (LANCE)

1 FORMA DE ADJUDICAR.

La adjudicación del presente proceso de selección se efectuará por ítem, grupo o en forma total.

2 PROCEDIMIENTO DE ADJUDICACIÓN – SUBASTA

Teniendo en cuenta que el proceso de selección es "selección abreviada - bienes y servicios de características técnicas uniformes", La adjudicación se realizara por subasta inversa electrónica a través de la plataforma del SECOP II.

El porcentaje base para la puja será el siguiente:

DESCRIPCIÓN	PRESUPUESTO OFICIAL	PORCENTAJE LANCE MÍNIMO
ADQUISICION SISTEMA INTELIGENCIA DE AMENAZAS EN LA RED	$ 3.990.200.000,00	4%

**** 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***

JUSTIFICACIÓN MARGEN MÍNIMO

1. El valor del precio de cada lance deberá hacerse en forma total al precio base.
2. El valor mínimo del lance inicial deberá ser del 4%, en adelante de acuerdo a la estrategia comercial de cada oferente.
3. El oferente deberá hacer lances, en menor precio, con el fin de mejorar el valor unitario de su oferta.
4. En caso de empate se dará aplicabilidad a lo establecido en el artículo 35 de la ley 2069 del 2020 y demás normas vigentes.

DESARROLLO DE LA PUJA

La puja se desarrollará de acuerdo a los parámetros y criterios establecidos por Colombia compra eficiente a través de la plataforma del SECOP II.

Proceso : INTELIGENCIA DE AMENAZAS EN LA RED - SOLICITUD COTIZACIÓN DIPOL-2023 002 (id.CO1.BDOS.3784141)

Solicitud de información a los Proveedores
SOLICITUD COTIZACIÓN DIPOL-2023 002 (En análisis)

Unidad de contratación GRUPO CONTRATOS DIPOL

INTELIGENCIA DE AMENAZAS EN LA RED

(Zona horaria (UTC-05:00) Bogotá, Lima, Quito)
Fecha de presentación de ofertas 20/01/2023 12:00 PM - **Fecha de publicación** 18/01/2023 10:46 AM

PROVEEDORES



LÍNEA DE TIEMPO

Fecha de publicación de concurso	Presentación de ofertas	Plazo para solicitar aclaraciones
18/01/2023	20/01/2023	20/01/2023

LISTA DE OFERTAS

Opciones

Referencia de oferta	Entidad	Presentada	Oferta
Oferta Procibernetica Dipol 2023	PROCIBERNETICA S.A.	20/01/2023 11:53 AM	5.500.000.000
PROPUESTA TECNICA VIRUS TOTAL HISPASEC SISTEMAS	HISPASEC SISTEMAS SL	20/01/2023 6:05 AM	753.453
EM-Datasec-Dipol-2	DATASEC S.A.S.	19/01/2023 11:23 AM	4.000.000.000
Oferta ISEGURAS PONAL	ISEGURAS	18/01/2023 4:48 PM	4.420.000.000
OFERTA DIPOL INTELIGENCIA DE AMENAZAS	MNEMO COLOMBIA SAS	18/01/2023 3:05 PM	4.000.000.000

EVALUACIÓN ECONÓMICA

Nuevo | Opciones

EVALUACIÓN

Opciones

OBSERVACIONES AL PLIEGO DE CONDICIONES — Contestar

No tiene ninguna observación a los documentos del proceso

MENSAJES — Crear

Sin mensajes

TAREAS — Crear

Sin tareas

MODIFICACIONES / ADENDAS — Crear

No tiene ninguna modificación

PROVEEDORES SUSCRITOS

HISPASEC SISTEMAS SL
Comentarios HISPASEC SISTEMAS
19/01/2023 6:51 AM

PROCIBERNETICA S.A.
19/01/2023 11:06 AM

NEWSAT SAS
20/01/2023 8:41 AM

Multisoftware Transaccional S.A.S
Comentarios MULTISOFT SAS, Interesado en participar.
20/01/2023 8:03 AM

DATASEC S.A.S.
19/01/2023 11:19 AM

Ver más »

ADMINISTRACIÓN DE EQUIPOS

Las modificaciones serán aplicadas sólo en este proceso

Equipo: SOLICITUD COTIZACIONES / 18/01/2023 10:28 AM (UTC-5 horas)((UTC-05:00) Bogotá, Lima, Quito)

EVENTOS DEL PROCESO

El proceso CO1.BDOS.3784141 ha cambiado de Solicitud información publicada a En análisis.
Sistema
20/01/2023 12:12 PM

El proceso CO1.REQ.3879806cambiado de estado Solicitud Información publicada a En análisis.
Sistema
20/01/2023 12:12 PM

Oportunidad CO1.OPDOS.15750904 fue consultado por el Proveedor HISPASEC SISTEMAS SL.
HISPASEC SISTEMAS SL
20/01/2023 12:05 PM

Oportunidad CO1.OPDOS.15750904 fue consultado por el Proveedor HISPASEC SISTEMAS SL.
HISPASEC SISTEMAS SL
20/01/2023 12:04 PM

Oportunidad CO1.OPDOS.15754812 fue consultado por el Proveedor PROCIBERNETICA S.A.
PROCIBERNETICA S.A.
20/01/2023 11:53 AM

Ver más »

Información general

Información general

Nombre de la oferta OFERTA DIPOL INTELIGENCIA DE AMENAZAS
Número del proceso SOLICITUD COTIZACIÓN DIPOL-2023 002
Tipo Total
Estado Información en evaluación
Proveedor MNEMO COLOMBIA SAS
COLOMBIA, Bogotá
Número de documento 900396176
Responsable Humberto de Jesus Velez Castro

Sobres

Nombre del sobre	Situación de llegada	Estado	Fecha y hora de entrega
Oferta de estimación	Dentro del plazo	Abierto	23 horas de tiempo transcurrido *(18/01/2023 3:05:06 PM(UTC-05:00) Bogotá, Lima, Quito)*

Cuestionario

1 Sobre único

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

							Precio total estimado	Incluya el precio como lo indique la Entidad Estatal
							0,00	4,000,000,000,00
Ref. Artículo	Código UNSPSC	Descripción	Cantidad	Unidad	Precio unitario estimado	Precio unitario	Precio total estimado	Incluya el precio como lo indique la Entidad Estatal
1	43233200	Software de Inteligencia de Amenazas en la red	1,00	UN		3,940,200,000,00	0,00	3,940,200,000,00
1	43222500	Hardware de Inteligencia de Amenazas en la red	1,00	UN		59,800,000,00	0,00	59,800,000,00

Anexos

Anexos

#	Nombre del documento			Solicitud de confidencialidad	Confidencial
☐	Sobre único (PDF)	Descargar	Detalle	No	☐
☐	Solicitud cotización 180123 -Final.docx	Descargar	Detalle	No	☐

Notas

Evaluación

Evaluación de ofertas

⚠ **La configuración de evaluación no se definió para la solicitud. Con el fin de ser capaz de crear una única evaluación a esta oferta se debería haber definido antes de la publicación de la solicitud.**

Evaluación de proveedores

Evaluación de proveedores

Información general

Información general

Nombre de la oferta Oferta ISEGURAS PONAL
Número del proceso SOLICITUD COTIZACIÓN DIPOL-2023 002
Tipo Total
Estado Información en evaluación
Proveedor ISEGURAS
COLOMBIA, Bogotá
Número de documento 901188624
Responsable Javier Fernando Merchán García

Sobres

Nombre del sobre	Situación de llegada	Estado	Fecha y hora de entrega
Oferta de estimación	Dentro del plazo	Abierto	22 horas de tiempo transcurrido *(18/01/2023 4:48:34 PM(UTC-05:00) Bogotá, Lima, Quito)*

Cuestionario

1 Sobre único

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

							Precio total estimado	Incluya el precio como lo indique la Entidad Estatal
							0,00	4,420,000,000,00
	Ref. Artículo	Código UNSPSC	Descripción	Cantidad	Unidad	Precio unitario estimado	Precio unitario	Precio total estimado	Incluya el precio como lo indique la Entidad Estatal
	1	43233200	Software de Inteligencia de Amenazas en la red	1,00	UN	4,359,000,000,00	0,00	4,359,000,000,00
	1	43222500	Hardware de Inteligencia de Amenazas en la red	1,00	UN	61,000,000,00	0,00	61,000,000,00

Anexos

Anexos

	#	Nombre del documento			Solicitud de confidencialidad	Confidencial
☐		Sobre único (PDF)	Descargar	Detalle	No	☐
☐		Solicitud cotización 180123-Infraestructuras.docx	Descargar	Detalle	No	☐

Notas

Evaluación

Evaluación de ofertas

⚠ **La configuración de evaluación no se definió para la solicitud. Con el fin de ser capaz de crear una única evaluación a esta oferta se debería haber definido antes de la publicación de la solicitud.**

Evaluación de proveedores

Evaluación de proveedores

Información general

Información general

Nombre de la oferta EM-Datasec-Dipol-2
Número del proceso SOLICITUD COTIZACIÓN DIPOL-2023 002
Tipo Total
Estado Información en evaluación
Proveedor DATASEC S.A.S.
Número de documento 901223827
Responsable DATASEC

Sobres

Nombre del sobre	Situación de llegada	Estado	Fecha y hora de entrega
Oferta de estimación	Dentro del plazo	Abierto	3 horas de tiempo transcurrido *(19/01/2023 11:23:09 AM(UTC-05:00) Bogotá, Lima, Quito)*

Cuestionario

1 Sobre único

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

							Precio total estimado	Incluya el precio como lo indique la Entidad Estatal
							0,00	4,000,000,000,00
	Ref. Artículo	Código UNSPSC	Descripción	Cantidad	Unidad	Precio unitario estimado	Precio unitario	Precio total estimado	Incluya el precio como lo indique la Entidad Estatal
	1	43233200	Software de Inteligencia de Amenazas en la red	1,00	UN		3,950,000,000,00	0,00	3,950,000,000,00
	1	43222500	Hardware de Inteligencia de Amenazas en la red	1,00	UN		50,000,000,00	0,00	50,000,000,00

Anexos

Anexos

	#	Nombre del documento			Solicitud de confidencialidad	Confidencial
☐		Sobre único (PDF)	Descargar	Detalle	No	☐
☐		Solicitud cotización 180123.pdf	Descargar	Detalle	No	☐

Notas

Evaluación

Evaluación de ofertas

⚠ **La configuración de evaluación no se definió para la solicitud. Con el fin de ser capaz de crear una única evaluación a esta oferta se debería haber definido antes de la publicación de la solicitud.**

Evaluación de proveedores

Evaluación de proveedores